ACLI Commands Reference for Avaya Virtual Services Platform 9000

Introduction

This guides describes the Avaya Command Line Interface (ACLI) commands for the configuration of various features in the Avaya Virtual Services Platform 9000 for the 4.0 release.

This document provides two different ways of navigating ACLI command documentation.

- alphabetically Each command is listed corresponding to the first letter of the command.
- command mode Each command mode page has a list of commands that are available in that mode. Each page is organized alphabetically for those commands in that mode.

Use the 'find-in-page' function of the browser to search for a command based on the page you are viewing. Most browsers launch 'find' using CTRL+F.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

License types

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING,

DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: avaya.com/support/Copyright/.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All other trademarks are the property of their respective owners.

Technical support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: avaya.com/support.

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Documentation support

For the most current versions of documentation, see the Avaya Support Web site: avaya.com/support.

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

Alphabetized list of commands

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

- A - 44 commands
- B - 39 commands
- C - 52 commands
- D - 18 commands
- E - 23 commands
- F - 15 commands
- G - 2 commands
- H - 5 commands
- I - 382 commands
- L - 46 commands
- M - 53 commands
- N - 38 commands
- O - 2 commands
- P - 20 commands
- Q - 9 commands
- R - 53 commands
- S - 524 commands
- T - 35 commands
- U - 5 commands
- V - 30 commands
- W - 1 commands

©Avaya Inc. 2015 All Rights Reserved.

Command mode index

The following command modes are available. Select the command mode to see a list of commands available in that mode.

- Application Configuration
- BGP Router Configuration
- GigabitEthernet Interface Configuration
- Global Configuration
- IS-IS Router Configuration
- Loopback Interface Configuration
- mgmtEthernet Interface Configuration
- MLT Interface Configuration
- OSPF Router Configuration
- Privileged EXEC
- RIP Router Configuration
- Route-Map Configuration
- User EXEC
- VLAN Interface Configuration
- VRF Router Configuration
- VRRP Router Configuration

Back to top

©Avaya Inc. 2015 All Rights Reserved.

Commands starting with A organized alphabetically

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

- accept adv-rtr (for OSPF)
- accept adv-rtr (for the GRT)
- accept (for the GRT)
- accept i-sid (for the GRT)
- accept isid-list (for the GRT)
- accept route-map
- access-diffserv
- access-policy
- access-policy <1-65535> accesslevel
- access-policy <1-65535> access-strict
- access-policy <1-65535> enable
- access-policy <1-65535> ftp
- access-policy <1-65535> host
- access-policy <1-65535> http
- access-policy <1-65535> mode
- access-policy <1-65535> name
- access-policy <1-65535> network
- access-policy <1-65535> precedence
- access-policy <1-65535> rlogin
- access-policy <1-65535> snmp-group
- access-policy <1-65535> snmpv3
- access-policy <1-65535> ssh
- access-policy <1-65535> telnet
- access-policy <1-65535> tftp
- access-policy <1-65535> username
- access-policy by-mac
- action
- aggregate-address
- application
- area
- area range
- area virtual-link
- area virtual-link message-digest-key
- as-boundary-router enable
- attribute
- auto-negotiate enable (on an Ethernet port)
- auto-negotiate (for the management port)
- auto-negotiation-advertisements
- auto-peer-restart enable
- auto-recover-delay
- auto-recover-port
- auto-summary
- autotopology
- auto-vlink

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

Commands starting with B organized alphabetically

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

- backup
- bad-lsa-ignore enable
- banner
- bgp aggregation
- bgp always-compare-med
- bgp client-to-client reflection
- bgp cluster-id
- bgp confederation
- bgp default local-preference<0-2147483647>
- bgp deterministic-med enable
- bgp multiple-paths <1-8>
- boot
- boot config choice
- boot config delay
- boot config flags block-snmp
- boot config flags debug-config
- boot config flags debugmode
- boot config flags fabric-profile
- boot config flags factorydefaults
- boot config flags ftpd
- boot config flags ha-cpu
- boot config flags hsecure
- boot config flags logging
- boot config flags reboot
- boot config flags rlogind
- boot config flags savetostandby
- boot config flags spanning-tree-mode
- boot config flags sshd
- boot config flags telnetd
- boot config flags tftpd
- boot config flags trace-logging
- boot config flags verify-config
- boot config host
- boot config linecard-compatibility-mode
- boot config logfile
- boot config master
- boot config multicast
- boot config sio console
- brouter

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

©Avaya Inc. 2015 All Rights Reserved.

Commands starting with C organized alphabetically

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

- cd
- cfm cmac enable
- cfm cmac level <0-7>
- cfm cmac mepid <1-8191>
- cfm maintenance-association
- cfm maintenance-domain
- cfm maintenance-endpoint
- cfm spbm enable
- cfm spbm level <0-7>
- cfm spbm mepid <1-8191>
- clear alarm
- clear filter acl
- clear ip arp interface
- clear ip dhcp-relay
- clear ip ipfix hash-stats
- clear ip ipfix stats
- clear ip mroute stats
- clear ip route
- clear ipv6 dcache
- clear ipv6 neighbor-cache
- clear ipv6 route static
- clear ipv6 statistics
- clear ipv6 vrrp
- clear ip vrrp
- clear isis lsdb
- clear isis spbm drop-stats
- clear isis stats
- clear khi
- clear lacp
- clear logging
- clear mac-address-table
- clear mac-address-table dynamic
- clear mlt
- clear qos
- clear radius statistics
- clear slpp
- clear-stats
- clear telnet
- clear trace
- clilog
- cli password
- cli timeout
- clock set
- clock time-zone
- !(command number)
- comp-bestpath-med-confed
- configure
- copy
- cp

cp-limit (for an MLT)
- cp-limit (for a port)
- csnp-interval

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

Commands starting with D organized alphabetically

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

- debug-file remove
- debug ip pim
- debug-screen
- default-cost
- default-information
- default-metric (for BGP)
- default-metric (for RIP)
- default-vlan-id
- delete
- dir
- disable
- domain
- dos-chkdsk
- dos-format
- dsapssap
- dump ar
- duplex
- duplex (for the management port)

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

Commands starting with E organized alphabetically

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

- eapol enable
- eapol init
- eapol max-request
- eapol quiet-interval
- eapol re-authenticate
- eapol re-authentication
- eapol server-timeout
- eapol sess-manage enable
- eapol sess-manage-mode
- eapol sess-manage-open-immediate
- eapol status
- eapol supplicant-timeout
- eapol traffic-control
- eapol transmit-interval
- editing
- enable
- enable-diffserv
- enable (for a route policy)
- encapsulation dot1q
- end
- exception dump
- exit
- extflash-stop

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

©Avaya Inc. 2015 All Rights Reserved.

Commands starting with F organized alphabetically

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

- fabric statistics
- filter acl
- filter acl ace
- filter acl ace action
- filter acl ace arp
- filter acl ace ethernet
- filter acl ace ip
- filter acl ace protocol
- filter acl enable
- filter acl log buffer-wrap
- filter acl port
- filter acl set
- filter acl vlan
- flap-dampening
- flight-recorder

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

©Avaya Inc. 2015 All Rights Reserved.

Commands starting with G organized alphabetically

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

- global-debug mask
- grep

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

Commands starting with H organized alphabetically

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

- hash-calc getEcmpRoute
- hash-calc getmltindex traffic-type
- help
- high-secure enable
- host-route

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

Commands starting with I organized alphabetically

- ibgp-report-import-rt
- ignore-illegal-rtrid
- interface GigabitEthernet
- interface Loopback
- interface mgmtEthernet
- interface mlt
- interface vlan
- ip address (for the management port)
- ip address (loopback)
- ip address (on a VLAN)
- ip alternative-route (globally)
- ip alternative-route (on a VRF)
- ip area (loopback)
- ip arp
- ip arp (for a VRF)
- ip arp multicast-mac-flooding
- ip arp-proxy enable (for a port)
- ip arp-proxy enable (for a VLAN)
- ip arp-response (for a port)
- ip arp-response (for a VLAN)
- ip arp static-mcast
- ip as-list
- ip as-list (for a VRF)
- ip bgp
- ip bgp aggregate-address
- ip bgp aggregation
- ip bgp always-compare-med
- ip bgp apply redistribute
- ip bgp auto-peer-restart enable
- ip bgp auto-summary
- ip bgp debug-screen
- ip bgp default-information
- ip bgp default local-preference
- ip bgp default-metric
- ip bgp deterministic-med enable
- ip bgp enable
- ip bgp flap-dampening
- ip bgp global-debug mask
- ip bgp ibgp-report-import-rt enable
- ip bgp ignore-illegal-rtrid enable
- ip bgp in-route-map
- ip bgp multiple-paths <1-8>
- ip bgp neighbor
- ip bgp neighbor password
- ip bgp network
- ip bgp no-med-path-is-worst enable
- ip bgp out-route-map WORD<0-256>
- ip bgp quick-start enable
- ip bgp redistribute

ip bgp restart-bgp
- ip bgp router-id {A.B.C.D}
- ip bgp stats-clear-counters
- ip bgp synchronization
- ip bgp traps enable
- ip community-list
- ip dhcp-relay (for an MLT)
- ip dhcp-relay (for a port)
- ip dhcp-relay (for a VLAN)
- ip dhcp-relay fwd-path
- ip dhcp-relay fwd-path enable
- ip dhcp-relay fwd-path (for a port)
- ip dhcp-relay fwd-path mode
- ip dhcp-relay fwd-path mode (for a port)
- ip dhcp-relay (loopback)
- ip directed-broadcast (for a port)
- ip directed-broadcast (for a VLAN)
- ip domain-name
- ip ecmp
- ip ecmp pathlist-apply
- ip extcommunity-list
- ip forward-protocol udp
- ip forward-protocol udp broadcastmask
- ip forward-protocol udp maxttl
- ip forward-protocol udp (on a VLAN)
- ip forward-protocol udp portfwd
- ip forward-protocol udp portfwdlist
- ip forward-protocol udp portfwdlist (on a VLAN)
- ip icmp
- ip igmp access-list (for a port)
- ip igmp access-list (for a VLAN)
- ip igmp access-list mode (for a port)
- ip igmp access-list mode (for a VLAN)
- ip igmp flush port
- ip igmp flush vlan
- ip igmp (for an port)
- ip igmp (for a VLAN)
- ip igmp generate-log (for a VRF)
- ip igmp generate-trap (for a VRF)
- ip igmp (globally)
- ip igmp igmpv3-explicit-host-tracking (for an Ethernet port)
- ip igmp igmpv3-explicit-host-tracking (for a VLAN)
- ip igmp immediate-leave (for an Ethernet port)
- ip igmp immediate-leave (for a VLAN)
- ip igmp immediate-leave-members
- ip igmp immediate-leave-mode (for a VRF)
- ip igmp mrdisc
- ip igmp snoop-querier
- ip igmp snoop-querier-addr
- ip igmp ssm dynamic-learning (for a VRF)
- ip igmp ssm group-range (for a VRF)
- ip igmp ssm-map (for a VRF)
- ip igmp static-group
- ip igmp stream-limit (for a port)
- ip igmp stream-limit (for a VLAN)
- ip igmp stream-limit-group
- ip ipfix collector
- ip ipfix enable
- ip ipfix flush
- ip ipfix (on a port)
- ip ipfix slot
- ip irdp
- ip irdp address (for a port)
- ip irdp address (for a VLAN)
- ip irdp holdtime (for a port)

- ip irdp holdtime (for a VLAN)
- ip irdp maxadvertinterval (for a port)
- ip irdp maxadvertinterval (for a VLAN)
- ip irdp minadvertinterval (for a port)
- ip irdp minadvertinterval (for a VLAN)
- ip irdp multicast (for a port)
- ip irdp multicast (for a VLAN)
- ip irdp preference (for a port)
- ip irdp preference (for a VLAN)
- ip isid-list (for a VRF)
- ip isid-list (for the GRT)
- ip max-routes-trap enable
- ip more-specific-non-local-route
- ip mroute (for a port)
- ip mroute resource-usage egress-threshold
- ip mroute resource-usage (for a VRF)
- ip mroute resource-usage log-msg trap-msg
- ip mroute static-source-group
- ip mroute stats enable
- ip mroute stream-limit (globally)
- ip name-server
- ip ospf advertise-when-down enable (for a port)
- ip ospf advertise-when-down enable (for a VLAN)
- ip ospf apply accept
- ip ospf apply accept adv-rtr
- ip ospf apply redistribute
- ip ospf area (for a port)
- ip ospf area (for a VLAN)
- ip ospf authentication-key WORD<0-8> (for a port)
- ip ospf authentication-key WORD<0-8> (for a VLAN)
- ip ospf authentication-type <none|message-digest|simple> (for a port)
- ip ospf authentication-type <none|message-digest|simple> (for a VLAN)
- ip ospf cost <1-65535> (for a port)
- ip ospf cost <1-65535> (for a VLAN)
- ip ospf dead-interval <0-2147483647> (for a port)
- ip ospf dead-interval <0-2147483647> (for a VLAN)
- ip ospf default-cost (for a VRF)
- ip ospf enable (for a port)
- ip ospf enable (for a VLAN)
- ip ospf hello-interval <1-65535> (for a port)
- ip ospf hello-interval <1-65535> (for a VLAN)
- ip ospf (loopback)
- ip ospf message-digest-key <1-255> md5-key WORD<0-16> (for a port)
- ip ospf message-digest-key <1-255> md5-key WORD<0-16> (for a VLAN)
- ip ospf mtu-ignore enable (for a port)
- ip ospf mtu-ignore enable (for a VLAN)
- ip ospf network <broadcast|nbma|passive> (for a port)
- ip ospf network <broadcast|nbma|passive> (for a VLAN)
- ip ospf poll-interval <0-2147483647> (for a port)
- ip ospf poll-interval <0-2147483647> (for a VLAN)
- ip ospf primary-md5-key <1-255> (for a port)
- ip ospf primary-md5-key <1-255> (for a VLAN)
- ip ospf priority <0-255> (for a port)
- ip ospf priority <0-255> (for a VLAN)
- ip ospf redistribute
- ip ospf retransmit-interval <0-3600> (for a port)
- ip ospf retransmit-interval <0-3600> (for a VLAN)
- ip ospf spf-run
- ip ospf transit-delay <0-3600> (for a port)
- ip ospf transit-delay <0-3600> (for a VLAN)
- ip ospf vlan (for a VLAN)
- ip pim active (for a port)
- ip pim active (for a VLAN)
- ip pim bootstrap-period <5-32757>
- ip pim bsr-candidate preference (for a port)

- ip pim bsr-candidate preference (for a VLAN)
- ip pim disc-data-timeout <5-65535>
- ip pim enable (for a port)
- ip pim enable (for a VLAN)
- ip pim fast-joinprune
- ip pim fwd-cache-timeout <10-86400>
- ip pim (globally)
- ip pim hello-interval <0-18724> (for a port)
- ip pim hello-interval <0-18724> (for a VLAN)
- ip pim interface-type <active|passive> (for a port)
- ip pim interface-type <active|passive> (for a VLAN)
- ip pim join-prune-interval <1-18724> (for a port)
- ip pim join-prune-interval <1-18724> (for a VLAN)
- ip pim join-prune-interval <1-18724> (globally)
- ip pim (loopback)
- ip pim mode
- ip pim passive (for a port)
- ip pim passive (for a VLAN)
- ip pim register-suppression-timeout <6-65535>
- ip pim rp-c-adv-timeout <5-26214>
- ip pim rp-candidate group
- ip pim static-rp
- ip pim unicast-route-change-timeout <2-65535>
- ip pim virtual-neighbor
- ip prefix-list
- ip prefix-list (for a VRF)
- ip rip advertise-when-down enable (for a port)
- ip rip advertise-when-down enable (for a VLAN)
- ip rip apply redistribute
- ip rip auto-aggregation enable (for a port)
- ip rip auto-aggregation enable (for a VLAN)
- ip rip cost (for a port)
- ip rip cost (for a VLAN)
- ip rip default-listen enable (for a port)
- ip rip default-listen enable (for a VLAN)
- ip rip default-supply enable (for a port)
- ip rip default-supply enable (for a VLAN)
- ip rip enable (for a port)
- ip rip enable (for a VLAN)
- ip rip holddown (for a port)
- ip rip holddown (for a VLAN)
- ip rip in-policy (for a port)
- ip rip in-policy (for a VLAN)
- ip rip listen (for a port)
- ip rip listen (for a VLAN)
- ip rip out-policy (for a port)
- ip rip out-policy (for a VLAN)
- ip rip poison enable (for a port)
- ip rip poison enable (for a VLAN)
- ip rip port
- ip rip receive version (for a port)
- ip rip receive version (for a VLAN)
- ip rip redistribute
- ip rip send (for a port)
- ip rip send (for a VLAN)
- ip rip supply (for a port)
- ip rip supply (for a VLAN)
- ip rip timeout (for a port)
- ip rip timeout (for a VLAN)
- ip rip triggered (for a port)
- ip rip triggered (for a VLAN)
- ip route (for a VRF)
- ip route (globally)
- ip route preference ebgp
- ip route preference ibgp

- ip route preference ospf-extern1
- ip route preference ospf-extern2
- ip route preference ospf-inter
- ip route preference ospf-intra
- ip route preference ospfv3-extern1
- ip route preference ospfv3-extern2
- ip route preference ospfv3-inter
- ip route preference ospfv3-intra
- ip route preference rip
- ip route preference spbm-level1
- ip route preference static
- ip route preference staticv6
- ip routing
- ip rsmlt
- ip rsmlt edge-support
- ip rvs-path-chk (for a port)
- ip rvs-path-chk (for a VLAN)
- ip rvs-path-chk mode (for a port)
- ip rvs-path-chk mode (for a VLAN)
- ip-source-address
- ip spb-multicast enable (for a port)
- ip spb-multicast enable (for a VLAN)
- ip supernet
- ip ttl
- ipv6 area
- ipv6 area range
- ipv6 area virtual-link
- ipv6 as-boundary-router
- ipv6 dhcp-relay (for a port)
- ipv6 dhcp-relay (for a VLAN)
- ipv6 dhcp-relay fwd-path
- ipv6 forwarding (for a port)
- ipv6 forwarding (for a VLAN)
- ipv6 forwarding (globally)
- ipv6 hop-limit
- ipv6 icmp error-interval
- ipv6 icmp error-quota
- ipv6 icmp redirect-msg
- ipv6 icmp unreach-msg
- ipv6 interface address (for a port)
- ipv6 interface address (for a VLAN)
- ipv6 interface address (for the management port)
- ipv6 interface enable (for a port)
- ipv6 interface enable (for a VLAN)
- ipv6 interface enable (for the management port)
- ipv6 interface (for a port)
- ipv6 interface hop-limit (for a port)
- ipv6 interface hop-limit (for a VLAN)
- ipv6 interface hop-limit (for the management port)
- ipv6 interface link-local (for a port)
- ipv6 interface link-local (for a VLAN)
- ipv6 interface link-local (for the management port)
- ipv6 interface mac-offset
- ipv6 interface mtu (for a port)
- ipv6 interface mtu (for a VLAN)
- ipv6 interface mtu (for the management port)
- ipv6 interface name (for a port)
- ipv6 interface name (for a VLAN)
- ipv6 interface name (for the management port)
- ipv6 interface reachable-time (for a port)
- ipv6 interface reachable-time (for a VLAN)
- ipv6 interface reachable-time (for the management port)
- ipv6 interface retransmit-timer (for a port)
- ipv6 interface retransmit-timer (for a VLAN)
- ipv6 interface retransmit-timer (for the management port)

- ipv6 interface vlan (for a port)
- ipv6 nd dad-ns (for a port)
- ipv6 nd dad-ns (for a VLAN)
- ipv6 nd dad-ns (for the management port)
- ipv6 nd (for a port)
- ipv6 nd hop-limit (for a port)
- ipv6 nd managed-config-flag (for a port)
- ipv6 nd managed-config-flag (for a VLAN)
- ipv6 nd mtu (for a port)
- ipv6 nd other-config-flag (for a port)
- ipv6 nd other-config-flag (for a VLAN)
- ipv6 nd prefix (for a port)
- ipv6 nd prefix (for a VLAN)
- ipv6 nd prefix-interface (for a port)
- ipv6 nd ra-lifetime (for a port)
- ipv6 nd ra-lifetime (for a VLAN)
- ipv6 nd reachable-time (for a port)
- ipv6 nd retransmit-timer (for a port)
- ipv6 nd rtr-advert-max-interval (for a port)
- ipv6 nd rtr-advert-max-interval (for a VLAN)
- ipv6 nd rtr-advert-min-interval (for a port)
- ipv6 nd rtr-advert-min-interval (for a VLAN)
- ipv6 nd send-ra (for a port)
- ipv6 nd send-ra (for a VLAN)
- ipv6 nd valid-life (for a port)
- ipv6 ospf area (for a VLAN)
- ipv6 ospf (for a VLAN)
- ipv6 prefix-list
- ipv6 redistribute
- ipv6 route
- ipv6 router-id
- ipv6 route static
- ipv6 rvs-path-chk (for a port)
- ipv6 rvs-path-chk (for a VLAN)
- ipv6 send-trap enable
- ipv6 tunnel
- ipv6 tunnel (for OSPF)
- ipv6 vrrp address (for a port)
- ipv6 vrrp address (for a VLAN)
- ipv6 vrrp (for a port)
- ipv6 vrrp (for a VLAN)
- ipvpn
- ipvpn enable
- ip vrf
- ip vrrp address (for a port)
- ip vrrp (for a port)
- ip vrrp (for a VLAN)
- i-sid
- isis accept adv-rtr (for a VRF)
- isis accept (for a VRF)
- isis apply accept (for the GRT)
- isis apply accept (for the VRF)
- isis apply redistribute
- isis hello-auth (on an MLT)
- isis hello-auth (on a port)
- isis l1-dr-priority (on an MLT)
- isis l1-dr-priority (on a port)
- isis l1-hello-interval (on an MLT)
- isis l1-hello-interval (on a port)
- isis l1-hello-multiplier (on an MLT)
- isis l1-hello-multiplier (on a port)
- isis (on an MLT)
- isis (on a port)
- isis redistribute bgp
- isis redistribute direct

- isis redistribute ospf
- isis redistribute rip
- isis redistribute static
- isis spbm (on an MLT)
- isis spbm (on a port)
- ist enable
- ist peer-ip
- is-type

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

Commands starting with L organized alphabetically

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

- l2 ping ip-address
- l2 ping vlan
- l2 tracemroute
- l2 traceroute ip-address
- l2 traceroute vlan
- l2 tracetree
- lacp aggregation enable
- lacp aggr-wait-time <200-2000>
- lacp enable (for a port)
- lacp fast-periodic-time <200-20000>
- lacp (globally)
- lacp key <0-65535>
- lacp mode
- lacp (on an MLT)
- lacp partner-key <0-65535>
- lacp partner-port <0-65535>
- lacp partner-port-priority <0-65535>
- lacp partner-state <0-255 | 0x0-0xff>
- lacp partner-system-id
- lacp partner-system-priority <0-65535>
- lacp priority <0-65535>
- lacp slow-periodic-time <10000-30000>
- lacp system-priority <0-65535>
- lacp timeout-scale <2-10>
- lacp timeout-time
- line-card
- link-flap-detect
- linktrace
- load-encryption-module
- load-license
- lock
- logging level
- logging logToExtFlash
- logging screen
- logging transferFile
- logging transferFile filename-prefix
- logging write
- login
- login-message
- logout
- loopback
- loop-detect
- loop-detect action
- loop-detect arp-detect
- lossless-port
- ls

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

Commands starting with M organized alphabetically

- mac-flap-time-limit
- mac-security add
- mac-security limit-learning enable
- mac-security limit-learning max-addrs
- mac-security limit-learning min-addrs
- mac-security limit-learning snmp-trap
- mac-security limit-learning violation-down-port
- mac-security mac-da-filter
- mac-security unknown-discard
- manual-area
- manualtrigger ip rip interface
- match as-path
- match community
- match community-exact
- match extcommunity
- match interface
- match local-preference
- match metric
- match network
- match next-hop
- match protocol
- match route-source
- match route-type
- match tag
- match vrf
- match vrfids
- max-logins
- max-lsp-gen-interval
- md5
- metric
- mirror-by-port
- mkdir
- mlt
- mlt member
- monitor ip mroute stats
- monitor ip vrrp statistics
- monitor mlt error collision
- monitor mlt error main
- monitor mlt stats interface main
- monitor mlt stats interface utilization
- monitor ports error
- monitor ports statistics bridging
- monitor ports statistics dhcp-relay
- monitor ports statistics interface
- monitor ports statistics ospf main
- monitor ports statistics rmon
- monitor ports statistics routing
- more
- multicast smlt-square

multicast software-forwarding
- mv
- mvpn enable
- mvpn fwd-cache-timeout <10-86400>

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

Commands starting with N organized alphabetically

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

- name
- name (for a port)
- neighbor-debug-all
- neighbor (for OSPF)
- neighbor password
- neighbor WORD<0-1536>
- neighbor WORD<0-1536> address-family
- neighbor WORD<0-1536> advertisement-interval <5-120>
- neighbor WORD<0-1536> default-ipv6-originate
- neighbor WORD<0-1536> default-originate
- neighbor WORD<0-1536> ebgp-multihop
- neighbor WORD<0-1536> enable
- neighbor WORD<0-1536> in-route-map WORD<0-256>
- neighbor WORD<0-1536> ipv6-in-route-map WORD<0-256>
- neighbor WORD<0-1536> ipv6-out-route-map WORD<0-256>
- neighbor WORD<0-1536> max-prefix <0-2147483647>
- neighbor WORD<0-1536> MD5-authentication enable
- neighbor WORD<0-1536> neighbor-debug-mask WORD<1-100>
- neighbor WORD<0-1536> next-hop-self
- neighbor WORD<0-1536> out-route-map WORD<0-256>
- neighbor WORD<0-1536> peer-group WORD<0-1536>
- neighbor WORD<0-1536> remote-as WORD<0-11>
- neighbor WORD<0-1536> remove-private-as enable
- neighbor WORD<0-1536> retry-interval <1-65535>
- neighbor WORD<0-1536> route-reflector-client
- neighbor WORD<0-1536> route-refresh
- neighbor WORD<0-1536> send-community
- neighbor WORD<0-1536> soft-reconfiguration-in enable
- neighbor WORD<0-1536> timers
- neighbor WORD<0-1536> update-source
- neighbor WORD<0-1536> weight
- network (for BGP)
- network (for OSPF)
- network (for RIP)
- nlb-mode
- no-med-path-is-worst
- ntp
- ntp server

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

©Avaya Inc. 2015 All Rights Reserved.

Commands starting with O organized alphabetically

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

- overload
- overload-on-startup

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

Home | Command modes | Alphabetical listing

Commands starting with P organized alphabetically

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

- password
- password access-level
- password aging-time
- passwordprompt
- pcap capture-filter
- pcap enable
- pcap enable mode
- pcap reset-stat
- peer
- permit
- ping
- ping-virtual-address
- pluggable-optical-module
- policy-vlan-precedence
- portlock enable
- prompt
- protocol-vlan
- psnp-interval
- pwc
- pwd

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

Home | Command modes | Alphabetical listing

Commands starting with Q organized alphabetically

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

- qos 802.1p-override
- qos egressmap
- qos if-policer
- qos if-shaper
- qos ingressmap
- qos level
- qos lossless-802.1p
- qos policy
- quick-start

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

Commands starting with R organized alphabetically

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

- radius
- radius cli-cmd-count
- radius cli-profile
- radius command-access-attribute
- radius enable
- radius server host
- radius-snmp
- radius sourceip-flag
- rate-limit
- redistribute bgp (for IS-IS)
- redistribute direct (for BGP)
- redistribute direct (for IS-IS)
- redistribute (for OSPF)
- redistribute (for RIP)
- redistribute ipv6-direct (for BGP)
- redistribute ipv6-static (for BGP)
- redistribute isis (for BGP)
- redistribute ospf (for BGP)
- redistribute ospf (for IS-IS)
- redistribute ospfv3 (for BGP)
- redistribute rip (for BGP)
- redistribute rip (for IS-IS)
- redistribute static (for BGP)
- redistribute static (for IS-IS)
- remote-mirroring
- remove
- rename
- reset
- restore
- retransmit-lsp-interval
- rfc1583-compatibility enable
- rlogin
- rmon
- rmon alarm
- rmon event
- rmon history
- rmon stats
- route-map
- router bgp
- router bgp as-4-byte enable
- router bgp as-dot enable
- router bgp enable
- router bgp enable globally
- route-reflector enable
- route-refresh
- router-id (for BGP)
- router-id (for OSPF)
- router isis
- router isis enable

router ospf
- router rip enable
- routing
- rsh

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

Commands starting with S organized alphabetically

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

- save clilog
- save config
- save log
- save snmplog
- save trace
- send-trap
- set as-path
- set as-path-mode
- set automatic-tag
- set community
- set community-mode
- set injectlist
- set ip-preference
- set local-preference
- set mask
- set metric
- set metric-type
- set metric-type-internal
- set next-hop
- set nssa-pbit
- set origin
- set origin-egp-as
- set tag
- set weight
- show access-policy
- show alarm database
- show alarm database
- show application slamon agent
- show application vsptalk
- show application vsptalk client
- show application vsptalk server
- show autotopology
- show banner
- show basic config
- show bgp ipv6 aggregates
- show bgp ipv6 imported-routes
- show bgp ipv6 networks
- show bgp ipv6 redistributed-routes
- show bgp ipv6 route
- show boot config
- show brouter
- show cfm cmac
- show cfm maintenance-association
- show cfm maintenance-domain
- show cfm maintenance-endpoint
- show cfm spbm
- show cli info
- show clilog
- show cli password

show clock
- show core-files
- show debug-file
- show debug ip pim
- show eapol auth-diags interface
- show eapol auth-stats interface
- show eapol multihost-session-stats interface
- show eapol port
- show eapol session interface
- show eapol session-stats interface
- show eapol status interface
- show eapol system
- show fabric
- show fdb-filter
- show filter acl
- show filter acl ace
- show filter acl action
- show filter acl arp
- show filter acl config
- show filter acl ethernet
- show filter acl ip
- show filter acl log
- show filter acl protocol
- show filter acl statistics
- show ftp-access
- show fulltech
- show ha-state
- show history
- show hosts
- show interfaces gigabitethernet
- show interfaces gigabitethernet config
- show interfaces gigabitethernet cp-limit
- show interfaces gigabitethernet error
- show interfaces gigabitethernet fdb-entry
- show interfaces gigabitethernet high-secure
- show interfaces gigabitethernet interface
- show interfaces gigabitethernet l1-config
- show interfaces gigabitethernet limit-fdb-learning
- show interfaces gigabitethernet loop-detected
- show interfaces gigabitethernet lossless-config
- show interfaces gigabitethernet mac-security
- show interfaces gigabitethernet name
- show interfaces gigabitethernet ospf
- show interfaces gigabitethernet rate-limit
- show interfaces gigabitethernet shape
- show interfaces gigabitethernet slpp
- show interfaces gigabitethernet state
- show interfaces gigabitethernet statistics
- show interfaces gigabitethernet statistics bridging
- show interfaces gigabitethernet statistics dhcp-relay
- show interfaces gigabitethernet statistics lacp
- show interfaces gigabitethernet statistics policer
- show interfaces gigabitethernet statistics rmon
- show interfaces gigabitethernet statistics verbose
- show interfaces gigabitethernet vlan
- show interfaces gigabitethernet vrfs
- show interfaces loopback
- show interfaces mgmtethernet
- show interfaces mgmtethernet config-L1
- show interfaces mgmtethernet error
- show interfaces mgmtethernet statistics
- show interfaces vlan
- show interfaces vlan arp
- show interfaces vlan autolearn-mac
- show interfaces vlan dhcp-relay

- show interfaces vlan igmp
- show interfaces vlan igmp-mrdisc
- show interfaces vlan ip
- show interfaces vlan manual-edit-mac
- show interfaces vlan nlb-mode
- show interfaces vlan vlan-bysrcmac
- show interfaces vlan vrfs
- show interface vlan nlb-mode
- show ip arp
- show ip arp interface
- show ip arp static-mcastmac
- show ip as-list
- show ip bgp aggregates
- show ip bgp cidr-only
- show ip bgp conf
- show ip bgp confederation
- show ip bgp dampened-paths
- show ip bgp flap-damp-config
- show ip bgp imported-routes
- show ip bgp neighbors
- show ip bgp networks
- show ip bgp peer-group
- show ip bgp redistributed-routes
- show ip bgp route
- show ip bgp stats
- show ip bgp summary
- show ip bgp vpnv4
- show ip community-list
- show ip dhcp-relay
- show ip directed-broadcast
- show ip dns
- show ip ecmp
- show ip extcommunity-list
- show ip forward-protocol udp
- show ip forward-protocol udp portfwd
- show ip forward-protocol udp portfwdlist
- show ip igmp access
- show ip igmp cache
- show ip igmp group
- show ip igmp group count
- show ip igmp group count group <A.B.C.D>
- show ip igmp group group <A.B.C.D>
- show ip igmp group group <A.B.C.D> tracked-members
- show ip igmp group member-subnet
- show ip igmp interface
- show ip igmp mrdisc
- show ip igmp mrdisc neighbors
- show ip igmp router-alert
- show ip igmp sender
- show ip igmp snooping
- show ip igmp snoop-trace
- show ip igmp ssm
- show ip igmp ssm-map
- show ip igmp static
- show ip igmp stream-limit
- show ip igmp sys
- show ip interface
- show ip ipfix
- show ip ipfix collector
- show ip ipfix export
- show ip ipfix exporter
- show ip ipfix flows
- show ip ipfix hash-statistics
- show ip ipfix interface
- show ip ipvpn

- show ip irdp
- show ip isid-list
- show ip isis accept
- show ip isis redistribute
- show ip mroute hw-resource-usage
- show ip mroute interface
- show ip mroute next-hop
- show ip mroute route
- show ip mroute static-source-group
- show ip mroute stats
- show ip ospf
- show ip ospf accept
- show ip ospf area
- show ip ospf area-range
- show ip ospf ase
- show ip ospf authentication
- show ip ospf default-cost
- show ip ospf host-route
- show ip ospf ifstats
- show ip ospf int-auth
- show ip ospf interface
- show ip ospf int-timers
- show ip ospf lsdb
- show ip ospf neighbor
- show ip ospf port-error
- show ip ospf redistribute
- show ip ospf stats
- show ip ospf virtual-link
- show ip pim
- show ip pim active-rp
- show ip pim bsr
- show ip pim interface
- show ip pim mode
- show ip pim mroute
- show ip pim neighbor
- show ip pim rp-candidate
- show ip pim rp-hash
- show ip pim static-rp
- show ip pim virtual-neighbor
- show ip prefix-list
- show ip redistribute
- show ip rip
- show ip rip interface
- show ip rip redistribute
- show ip route
- show ip route preference
- show ip routing
- show ip rsmlt
- show ip rsmlt edge-support
- show ip tcp statistics
- show ip udp statistics
- show ipv6 address
- show ipv6 dcache
- show ipv6 dhcp-relay
- show ipv6 forwarding
- show ipv6 global
- show ipv6 interface
- show ipv6 nd
- show ipv6 nd-prefix
- show ipv6 neighbor
- show ipv6 ospf
- show ipv6 ospf area
- show ipv6 ospf area-range
- show ipv6 ospf ase
- show ipv6 ospf interface

- show ipv6 ospf int-timers
- show ipv6 ospf lsdb
- show ipv6 ospf nbma-nbr interface
- show ipv6 ospf neighbor
- show ipv6 ospf redistribute
- show ipv6 ospf statistics
- show ipv6 prefix-list
- show ipv6 route
- show ipv6 tcp
- show ipv6 trace
- show ipv6 tunnel
- show ipv6 udp
- show ipv6 vrrp
- show ipv6 vrrp address
- show ipv6 vrrp interface
- show ipv6 vrrp interface gigabitethernet statistics
- show ipv6 vrrp statistics
- show ip vrf
- show ip vrf mvpn
- show ip vrrp
- show ip vrrp address
- show ip vrrp interface
- show ip vrrp interface gigabitEthernet
- show ip vrrp interface gigabitEthernet statistics
- show ip vrrp interface vlan
- show ip vrrp statistics
- show isis
- show isis adjacencies
- show isis area
- show isis int-auth
- show isis int-ckt-level
- show isis int-counters
- show isis interface
- show isis int-l1-cntl-pkts
- show isis int-l2-cntl-pkts
- show isis int-timers
- show isis lsdb
- show isis lsdb ip-unicast
- show isis manual-area
- show isis net
- show isis spbm
- show isis spb-mcast-summary
- show isis spbm drop-stats port
- show isis spbm ip-multicast-route
- show isis spbm ip-multicast-route group
- show isis spbm ip-multicast-route vlan
- show isis spbm ip-multicast-route vrf
- show isis spbm ip-multicast-route vsn-isid
- show isis spbm ip-unicast-fib
- show isis spbm i-sid
- show isis spbm multicast
- show isis spbm multicast-fib
- show isis spbm nick-name
- show isis spbm unicast-fib
- show isis spbm unicast-tree
- show isis statistics
- show isis system-id
- show ist mlt
- show ist stat
- show khi cpp
- show khi forwarding
- show khi performance
- show lacp
- show lacp interface
- show license

- show link-flap-detect
- show logging
- show logging file
- show mac-security mac-da-filter
- show mirror-by-port
- show mlt
- show mlt error collision
- show mlt error main
- show mlt stats
- show monitor-statistics
- show multicast software-forwarding
- show multicast square-smlt
- show ntp
- show pcap
- show pcap capture-filter
- show pcap dump
- show pcap port
- show pcap stats
- show pluggable-optical-modules
- show ports statistics ospf extended
- show ports statistics ospf main
- show qos 802.1p-override
- show qos egressmap
- show qos ingressmap
- show qos lossless-802.1p
- show qos policer
- show qos policy-config
- show qos shaper
- show qos statistics policy
- show radius
- show radius-server
- show radius-server statistics
- show radius snmp
- show remote-mirroring
- show rmon
- show rmon stats
- show route-map
- show routing statistics
- show running-config
- show slot
- show slpp
- show slpp interface
- show smlt
- show snmplog
- show snmp-server
- show software
- show software patch
- show spanning-tree bpdu-filtering
- show spanning-tree config
- show spanning-tree mstp config
- show spanning-tree mstp msti config
- show spanning-tree mstp msti port
- show spanning-tree mstp port role
- show spanning-tree mstp port statistics
- show spanning-tree mstp statistics
- show spanning-tree mstp status
- show spanning-tree rstp config
- show spanning-tree rstp port config
- show spanning-tree rstp port role
- show spanning-tree rstp port statistics
- show spanning-tree rstp port status
- show spanning-tree rstp statistics
- show spanning-tree rstp status
- show spanning-tree status
- show spbm

- show ssh
- show sys dns
- show sys force-msg
- show sys-info
- show syslog
- show syslog host
- show sys mgid-usage
- show sys msg-control
- show sys mtu
- show sys power
- show sys setting
- show sys software
- show sys stats ipmc-threshold-exceeded-cnt
- show sys topology-ip
- show tacacs
- show tech
- show telnet-access
- show trace cfm
- show trace file
- show trace level
- show trace modid-list
- show trace spbm isis
- show unsupported-lastset
- show users
- show vlacp
- show vlan advance
- show vlan autolearn-mac
- show vlan basic
- show vlan brouter-port
- show vlan i-sid
- show vlan mac-address-entry
- show vlan mac-address-static
- show vlan manual-edit-mac
- show vlan members
- show vlan nodal-mep
- show vlan nodal-mip-level
- show vlan remote-mac-table
- show vlan src-mac
- show vlan static-mcastmac
- show web-server
- shutdown
- shutdown (for the management port)
- slamon agent
- slamon agent-comm-port <0-65535>
- slamon install-cert-file
- slamon oper-mode enable
- slamon server
- slot reset
- slot shutdown
- slpp (for a port)
- slpp (globally)
- slpp (on a VLAN)
- smlt
- snmplog
- snmp-server authentication-trap enable
- snmp-server community
- snmp-server contact
- snmp-server force-iphdr-sender enable
- snmp-server force-trap-sender enable
- snmp-server group
- snmp-server host v1
- snmp-server host v2
- snmp-server host v3
- snmp-server location
- snmp-server login-success-trap enable

- snmp-server name
- snmp-server notify-filter
- snmp-server sender-ip
- snmp-server user
- snmp-server view
- snmp trap link-status
- software
- software patch
- software reset-commit-time
- source
- source-mac-vlan
- spanning-tree bpdu-filtering
- spanning-tree mstp cost
- spanning-tree mstp edge-port
- spanning-tree mstp force-port-state
- spanning-tree mstp forward-time
- spanning-tree mstp hello-time (on a port)
- spanning-tree mstp max-age
- spanning-tree mstp max-hop
- spanning-tree mstp msti (globally)
- spanning-tree mstp msti (on a port)
- spanning-tree mstp p2p
- spanning-tree mstp pathcost-type
- spanning-tree mstp port
- spanning-tree mstp priority (globally)
- spanning-tree mstp priority (on a port)
- spanning-tree mstp protocol-migration
- spanning-tree mstp region
- spanning-tree mstp tx-holdcount
- spanning-tree mstp version
- spanning-tree rstp cost
- spanning-tree rstp edge-port
- spanning-tree rstp forward-time
- spanning-tree rstp group-stp enable
- spanning-tree rstp hello-time
- spanning-tree rstp max-age
- spanning-tree rstp p2p
- spanning-tree rstp pathcost-type
- spanning-tree rstp port
- spanning-tree rstp priority (globally)
- spanning-tree rstp priority (on a port)
- spanning-tree rstp protocol-migration
- spanning-tree rstp stp
- spanning-tree rstp tx-holdcount
- spanning-tree rstp version
- spbm
- spbm <1-100>
- spbm <1-100> b-vid
- spbm <1-100> ip enable
- spbm <1-100> lsdb-trap enable
- spbm <1-100> multicast enable
- spbm <1-100> multicast fwd-cache-timeout <10-86400>
- spbm <1-100> nick-name
- spbm <1-100> smlt-peer-system-id
- spbm <1-100> smlt-virtual-bmac
- spbm ethertype
- speed
- speed (for the management port)
- spf-delay
- spoof-detect
- ssh (configuration)
- ssh (connection)
- subnet-vlan
- synchronization
- sys action

- sys action cpu-switch-over
- sys clipId-topology-ip
- sys data-path-fault-shutdown
- sys force-msg
- sys force-topology-ip-flag
- syslog enable
- syslog host
- sys log ip-header-type
- syslog max-hosts <1-10>
- sys mgmt-virtual-ip
- sys msg-control
- sys mtu
- sys name
- sys-name
- sys power
- sys shutdown
- sys software auto-commit
- sys software commit-time
- sys software patch
- system-id

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

©Avaya Inc. 2015 All Rights Reserved.

Home | Command modes | Alphabetical listing

Commands starting with T organized alphabetically

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

- tacacs accounting
- tacacs authentication
- tacacs authorization
- tacacs protocol enable
- tacacs server host
- tacacs server secondary-host
- tacacs switch
- tagged-frames-discard
- telnet
- telnet-access sessions
- terminal
- timers basic holddown (for OSPF)
- timers basic holddown (for RIP)
- timers basic timeout
- timers basic update
- trace cfm level <0-4>
- trace filter file
- trace filter module
- trace flags isis
- trace flags ospf
- trace grep
- trace ipv6 base
- trace ipv6 forwarding
- trace ipv6 nd
- trace ipv6 rtm
- trace ipv6 transport
- trace level
- traceroute
- trace route-map
- trace screen
- trace shutdown
- trace spbm isis level <0-4>
- trap
- traps
- tx-flow-control

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

©Avaya Inc. 2015 All Rights Reserved.

Commands starting with U organized alphabetically

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

- udp checksum
- udpsrc-by-vip
- untagged-frames-discard
- untag-port-default-vlan
- usb-stop

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

Commands starting with V organized alphabetically

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

- vlacp
- vlacp enable
- vlan action
- vlan agetime
- vlan create
- vlan create <2-4084> type
- vlan delete
- vlan i-sid
- vlan mac-address-entry
- vlan mac-address-static
- vlan members
- vlan mlt
- vlan nodal-mep
- vlan nodal-mip-level
- vlan ports ospf-passive
- vlan srcmac
- vlan static-mcastmac
- vrf (for a port)
- vrf (for a VLAN)
- vsptalk
- vsptalk { gtalk | avaya } client add-buddy
- vsptalk { gtalk | avaya } client username
- vsptalk { gtalk | avaya } enable
- vsptalk { gtalk | avaya } server address
- vsptalk { gtalk | avaya } server encryption
- vsptalk { gtalk | avaya } server port
- vsptalk { gtalk | avaya } server proxy
- vsptalk { gtalk | avaya } server ssltype
- vsptalk endpoint-address
- vsptalk event-notification enable

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

©Avaya Inc. 2015 All Rights Reserved.

Home | Command modes | Alphabetical listing

Commands starting with W organized alphabetically

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

- web-server

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

Application Configuration

s

- slamon agent
- slamon agent-comm-port <0-65535>
- slamon install-cert-file
- slamon oper-mode enable
- slamon server

v

- vsptalk
- vsptalk { gtalk | avaya } client add-buddy
- vsptalk { gtalk | avaya } client username
- vsptalk { gtalk | avaya } enable
- vsptalk { gtalk | avaya } server address
- vsptalk { gtalk | avaya } server encryption
- vsptalk { gtalk | avaya } server port
- vsptalk { gtalk | avaya } server proxy
- vsptalk { gtalk | avaya } server ssltype
- vsptalk endpoint-address
- vsptalk event-notification enable

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

BGP Router Configuration

A

- aggregate-address
- auto-peer-restart enable
- auto-summary

B

- bgp aggregation
- bgp always-compare-med
- bgp client-to-client reflection
- bgp cluster-id
- bgp confederation
- bgp default local-preference<0-2147483647>
- bgp deterministic-med enable
- bgp multiple-paths <1-8>

C

- comp-bestpath-med-confed

D

- debug-screen
- default-information
- default-metric (for BGP)

F

- flap-dampening

G

- global-debug mask

I

- ibgp-report-import-rt
- ignore-illegal-rtrid

N

- neighbor-debug-all
- neighbor password
- neighbor WORD<0-1536>
- neighbor WORD<0-1536> address-family
- neighbor WORD<0-1536> advertisement-interval <5-120>
- neighbor WORD<0-1536> default-ipv6-originate
- neighbor WORD<0-1536> default-originate
- neighbor WORD<0-1536> ebgp-multihop
- neighbor WORD<0-1536> enable
- neighbor WORD<0-1536> in-route-map WORD<0-256>

- neighbor WORD<0-1536> ipv6-in-route-map WORD<0-256>
- neighbor WORD<0-1536> ipv6-out-route-map WORD<0-256>
- neighbor WORD<0-1536> max-prefix <0-2147483647>
- neighbor WORD<0-1536> MD5-authentication enable
- neighbor WORD<0-1536> neighbor-debug-mask WORD<1-100>
- neighbor WORD<0-1536> next-hop-self
- neighbor WORD<0-1536> out-route-map WORD<0-256>
- neighbor WORD<0-1536> peer-group WORD<0-1536>
- neighbor WORD<0-1536> remote-as WORD<0-11>
- neighbor WORD<0-1536> remove-private-as enable
- neighbor WORD<0-1536> retry-interval <1-65535>
- neighbor WORD<0-1536> route-reflector-client
- neighbor WORD<0-1536> route-refresh
- neighbor WORD<0-1536> send-community
- neighbor WORD<0-1536> soft-reconfiguration-in enable
- neighbor WORD<0-1536> timers
- neighbor WORD<0-1536> update-source
- neighbor WORD<0-1536> weight
- network (for BGP)
- no-med-path-is-worst

Q

- quick-start

R

- redistribute direct (for BGP)
- redistribute ipv6-direct (for BGP)
- redistribute ipv6-static (for BGP)
- redistribute isis (for BGP)
- redistribute ospf (for BGP)
- redistribute ospfv3 (for BGP)
- redistribute rip (for BGP)
- redistribute static (for BGP)
- route-reflector enable
- route-refresh
- router-id (for BGP)

S

- synchronization

T

- traps

©Avaya Inc. 2015 All Rights Reserved.

GigabitEthernet Interface Configuration

A

- access-diffserv
- action
- auto-negotiate enable (on an Ethernet port)
- auto-negotiation-advertisements
- auto-recover-port

B

- brouter

C

- clear mac-address-table dynamic
- cp-limit (for a port)

D

- default-vlan-id
- duplex

E

- eapol max-request
- eapol quiet-interval
- eapol re-authentication
- eapol server-timeout
- eapol sess-manage-mode
- eapol sess-manage-open-immediate
- eapol status
- eapol supplicant-timeout
- eapol traffic-control
- eapol transmit-interval
- enable-diffserv
- encapsulation dot1q

F

- fabric statistics

H

- high-secure enable

I

- ip arp-proxy enable (for a port)
- ip arp-response (for a port)
- ip dhcp-relay (for a port)
- ip dhcp-relay fwd-path (for a port)
- ip dhcp-relay fwd-path mode (for a port)

- ip directed-broadcast (for a port)
- ip igmp access-list (for a port)
- ip igmp access-list mode (for a port)
- ip igmp (for an port)
- ip igmp igmpv3-explicit-host-tracking (for an Ethernet port)
- ip igmp immediate-leave (for an Ethernet port)
- ip igmp stream-limit (for a port)
- ip ipfix (on a port)
- ip irdp address (for a port)
- ip irdp holdtime (for a port)
- ip irdp maxadvertinterval (for a port)
- ip irdp minadvertinterval (for a port)
- ip irdp multicast (for a port)
- ip irdp preference (for a port)
- ip mroute (for a port)
- ip ospf advertise-when-down enable (for a port)
- ip ospf area (for a port)
- ip ospf authentication-key WORD<0-8> (for a port)
- ip ospf authentication-type <none|message-digest|simple> (for a port)
- ip ospf cost <1-65535> (for a port)
- ip ospf dead-interval <0-2147483647> (for a port)
- ip ospf enable (for a port)
- ip ospf hello-interval <1-65535> (for a port)
- ip ospf message-digest-key <1-255> md5-key WORD<0-16> (for a port)
- ip ospf mtu-ignore enable (for a port)
- ip ospf network <broadcast|nbma|passive> (for a port)
- ip ospf poll-interval <0-2147483647> (for a port)
- ip ospf primary-md5-key <1-255> (for a port)
- ip ospf priority <0-255> (for a port)
- ip ospf retransmit-interval <0-3600> (for a port)
- ip ospf transit-delay <0-3600> (for a port)
- ip pim active (for a port)
- ip pim bsr-candidate preference (for a port)
- ip pim enable (for a port)
- ip pim hello-interval <0-18724> (for a port)
- ip pim interface-type <active|passive> (for a port)
- ip pim join-prune-interval <1-18724> (for a port)
- ip pim passive (for a port)
- ip rip advertise-when-down enable (for a port)
- ip rip auto-aggregation enable (for a port)
- ip rip cost (for a port)
- ip rip default-listen enable (for a port)
- ip rip default-supply enable (for a port)
- ip rip enable (for a port)
- ip rip holddown (for a port)
- ip rip in-policy (for a port)
- ip rip listen (for a port)
- ip rip out-policy (for a port)
- ip rip poison enable (for a port)
- ip rip port
- ip rip receive version (for a port)
- ip rip send (for a port)
- ip rip supply (for a port)
- ip rip timeout (for a port)
- ip rip triggered (for a port)
- ip rvs-path-chk (for a port)
- ip rvs-path-chk mode (for a port)
- ip spb-multicast enable (for a port)
- ipv6 dhcp-relay (for a port)
- ipv6 forwarding (for a port)
- ipv6 interface address (for a port)
- ipv6 interface enable (for a port)
- ipv6 interface (for a port)
- ipv6 interface hop-limit (for a port)
- ipv6 interface link-local (for a port)

- ipv6 interface mtu (for a port)
- ipv6 interface name (for a port)
- ipv6 interface reachable-time (for a port)
- ipv6 interface retransmit-timer (for a port)
- ipv6 interface vlan (for a port)
- ipv6 nd dad-ns (for a port)
- ipv6 nd (for a port)
- ipv6 nd hop-limit (for a port)
- ipv6 nd managed-config-flag (for a port)
- ipv6 nd mtu (for a port)
- ipv6 nd other-config-flag (for a port)
- ipv6 nd prefix (for a port)
- ipv6 nd prefix-interface (for a port)
- ipv6 nd ra-lifetime (for a port)
- ipv6 nd reachable-time (for a port)
- ipv6 nd retransmit-timer (for a port)
- ipv6 nd rtr-advert-max-interval (for a port)
- ipv6 nd rtr-advert-min-interval (for a port)
- ipv6 nd send-ra (for a port)
- ipv6 nd valid-life (for a port)
- ipv6 rvs-path-chk (for a port)
- ipv6 vrrp address (for a port)
- ipv6 vrrp (for a port)
- ip vrrp address (for a port)
- ip vrrp (for a port)
- isis hello-auth (on a port)
- isis l1-dr-priority (on a port)
- isis l1-hello-interval (on a port)
- isis l1-hello-multiplier (on a port)
- isis (on a port)
- isis spbm (on a port)

L

- lacp aggregation enable
- lacp aggr-wait-time <200-2000>
- lacp enable (for a port)
- lacp fast-periodic-time <200-20000>
- lacp key <0-65535>
- lacp mode
- lacp partner-key <0-65535>
- lacp partner-port <0-65535>
- lacp partner-port-priority <0-65535>
- lacp partner-state <0-255 | 0x0-0xff>
- lacp partner-system-id
- lacp partner-system-priority <0-65535>
- lacp priority <0-65535>
- lacp slow-periodic-time <10000-30000>
- lacp system-priority <0-65535>
- lacp timeout-scale <2-10>
- lacp timeout-time
- lock
- loop-detect
- loop-detect action
- lossless-port

M

- mac-security limit-learning enable
- mac-security limit-learning max-addrs
- mac-security limit-learning min-addrs
- mac-security limit-learning snmp-trap
- mac-security limit-learning violation-down-port
- mac-security unknown-discard

N

- name (for a port)

P

- pcap enable mode
- policy-vlan-precedence
- protocol-vlan

Q

- qos 802.1p-override
- qos if-policer
- qos if-shaper
- qos level

R

- rate-limit
- remote-mirroring
- routing

S

- shutdown
- slpp (for a port)
- snmp trap link-status
- source-mac-vlan
- spanning-tree bpdu-filtering
- spanning-tree mstp cost
- spanning-tree mstp edge-port
- spanning-tree mstp force-port-state
- spanning-tree mstp hello-time (on a port)
- spanning-tree mstp msti (on a port)
- spanning-tree mstp p2p
- spanning-tree mstp port
- spanning-tree mstp priority (on a port)
- spanning-tree mstp protocol-migration
- spanning-tree rstp cost
- spanning-tree rstp edge-port
- spanning-tree rstp p2p
- spanning-tree rstp port
- spanning-tree rstp priority (on a port)
- spanning-tree rstp protocol-migration
- spanning-tree rstp stp
- speed
- spoof-detect
- subnet-vlan

T

- tagged-frames-discard
- tx-flow-control

U

- untagged-frames-discard
- untag-port-default-vlan

V

- vlacp
- vrf (for a port)

Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

Global Configuration

A

- access-policy
- access-policy <1-65535> accesslevel
- access-policy <1-65535> access-strict
- access-policy <1-65535> enable
- access-policy <1-65535> ftp
- access-policy <1-65535> host
- access-policy <1-65535> http
- access-policy <1-65535> mode
- access-policy <1-65535> name
- access-policy <1-65535> network
- access-policy <1-65535> precedence
- access-policy <1-65535> rlogin
- access-policy <1-65535> snmp-group
- access-policy <1-65535> snmpv3
- access-policy <1-65535> ssh
- access-policy <1-65535> telnet
- access-policy <1-65535> tftp
- access-policy <1-65535> username
- access-policy by-mac
- application
- auto-recover-delay
- autotopology

B

- banner
- boot config choice
- boot config delay
- boot config flags block-snmp
- boot config flags debug-config
- boot config flags debugmode
- boot config flags fabric-profile
- boot config flags factorydefaults
- boot config flags ftpd
- boot config flags ha-cpu
- boot config flags hsecure
- boot config flags logging
- boot config flags reboot
- boot config flags rlogind
- boot config flags savetostandby
- boot config flags spanning-tree-mode
- boot config flags sshd
- boot config flags telnetd
- boot config flags tftpd
- boot config flags trace-logging
- boot config flags verify-config
- boot config host
- boot config linecard-compatibility-mode
- boot config logfile

boot config master
- boot config multicast
- boot config sio console

C

- cfm cmac enable
- cfm cmac level <0-7>
- cfm cmac mepid <1-8191>
- cfm maintenance-association
- cfm maintenance-domain
- cfm maintenance-endpoint
- cfm spbm enable
- cfm spbm level <0-7>
- cfm spbm mepid <1-8191>
- clilog
- cli password
- cli timeout
- clock time-zone

D

- debug ip pim

E

- eapol enable
- eapol sess-manage enable
- end
- exception dump

F

- filter acl
- filter acl ace
- filter acl ace action
- filter acl ace arp
- filter acl ace ethernet
- filter acl ace ip
- filter acl ace protocol
- filter acl enable
- filter acl log buffer-wrap
- filter acl port
- filter acl set
- filter acl vlan

I

- interface GigabitEthernet
- interface Loopback
- interface mgmtEthernet
- interface mlt
- interface vlan
- ip alternative-route (globally)
- ip arp
- ip arp multicast-mac-flooding
- ip arp static-mcast
- ip as-list
- ip community-list
- ip dhcp-relay fwd-path
- ip dhcp-relay fwd-path enable
- ip dhcp-relay fwd-path mode
- ip domain-name
- ip ecmp
- ip extcommunity-list
- ip forward-protocol udp

- ip forward-protocol udp portfwd
- ip forward-protocol udp portfwdlist
- ip icmp
- ip igmp (globally)
- ip ipfix collector
- ip ipfix enable
- ip ipfix slot
- ip irdp
- ip isid-list (for the GRT)
- ip max-routes-trap enable
- ip more-specific-non-local-route
- ip mroute resource-usage egress-threshold
- ip mroute resource-usage log-msg trap-msg
- ip mroute static-source-group
- ip mroute stats enable
- ip mroute stream-limit (globally)
- ip name-server
- ip pim bootstrap-period <5-32757>
- ip pim disc-data-timeout <5-65535>
- ip pim fast-joinprune
- ip pim fwd-cache-timeout <10-86400>
- ip pim (globally)
- ip pim join-prune-interval <1-18724> (globally)
- ip pim mode
- ip pim register-suppression-timeout <6-65535>
- ip pim rp-c-adv-timeout <5-26214>
- ip pim rp-candidate group
- ip pim static-rp
- ip pim unicast-route-change-timeout <2-65535>
- ip pim virtual-neighbor
- ip prefix-list
- ip route (globally)
- ip route preference ebgp
- ip route preference ibgp
- ip route preference ospf-extern1
- ip route preference ospf-extern2
- ip route preference ospf-inter
- ip route preference ospf-intra
- ip route preference ospfv3-extern1
- ip route preference ospfv3-extern2
- ip route preference ospfv3-inter
- ip route preference ospfv3-intra
- ip route preference rip
- ip route preference spbm-level1
- ip route preference static
- ip route preference staticv6
- ip routing
- ip rsmlt edge-support
- ip supernet
- ip ttl
- ipv6 dhcp-relay fwd-path
- ipv6 forwarding (globally)
- ipv6 hop-limit
- ipv6 icmp error-interval
- ipv6 icmp error-quota
- ipv6 icmp redirect-msg
- ipv6 icmp unreach-msg
- ipv6 prefix-list
- ipv6 route
- ipv6 route static
- ipv6 tunnel
- ip vrf

L

lacp (globally)
- link-flap-detect
- load-encryption-module
- load-license
- logging level
- logging logToExtFlash
- logging screen
- logging transferFile
- logging transferFile filename-prefix
- logging write
- login-message
- loop-detect arp-detect

M

- mac-flap-time-limit
- mac-security add
- mac-security mac-da-filter
- max-logins
- mirror-by-port
- mlt
- mlt member
- multicast smlt-square
- multicast software-forwarding

N

- ntp
- ntp server

P

- password
- password access-level
- password aging-time
- passwordprompt
- pcap capture-filter
- pcap enable
- pcap reset-stat
- pluggable-optical-module
- portlock enable
- prompt

Q

- qos egressmap
- qos ingressmap
- qos lossless-802.1p
- qos policy

R

- radius
- radius cli-cmd-count
- radius cli-profile
- radius command-access-attribute
- radius enable
- radius server host
- radius-snmp
- radius sourceip-flag
- rmon
- rmon alarm
- rmon event
- rmon history
- rmon stats
- route-map

- router bgp
- router bgp as-4-byte enable
- router bgp as-dot enable
- router bgp enable
- router bgp enable globally
- router isis
- router isis enable
- router ospf
- router rip enable

S

- slot shutdown
- slpp (globally)
- snmplog
- snmp-server authentication-trap enable
- snmp-server community
- snmp-server contact
- snmp-server force-iphdr-sender enable
- snmp-server force-trap-sender enable
- snmp-server group
- snmp-server host v1
- snmp-server host v2
- snmp-server host v3
- snmp-server location
- snmp-server login-success-trap enable
- snmp-server name
- snmp-server notify-filter
- snmp-server sender-ip
- snmp-server user
- snmp-server view
- spanning-tree mstp forward-time
- spanning-tree mstp max-age
- spanning-tree mstp max-hop
- spanning-tree mstp msti (globally)
- spanning-tree mstp pathcost-type
- spanning-tree mstp priority (globally)
- spanning-tree mstp region
- spanning-tree mstp tx-holdcount
- spanning-tree mstp version
- spanning-tree rstp forward-time
- spanning-tree rstp group-stp enable
- spanning-tree rstp hello-time
- spanning-tree rstp max-age
- spanning-tree rstp pathcost-type
- spanning-tree rstp priority (globally)
- spanning-tree rstp tx-holdcount
- spanning-tree rstp version
- spbm
- spbm ethertype
- ssh (configuration)
- sys clipId-topology-ip
- sys data-path-fault-shutdown
- sys force-msg
- sys force-topology-ip-flag
- syslog enable
- syslog host
- sys log ip-header-type
- syslog max-hosts <1-10>
- sys mgmt-virtual-ip
- sys msg-control
- sys mtu
- sys name
- sys power
- sys software auto-commit

sys software commit-time
- sys software patch

T

- tacacs accounting
- tacacs authentication
- tacacs authorization
- tacacs protocol enable
- tacacs server host
- tacacs server secondary-host
- tacacs switch
- telnet-access sessions

U

- udp checksum
- udpsrc-by-vip

V

- vlacp enable
- vlan action
- vlan agetime
- vlan create
- vlan create <2-4084> type
- vlan delete
- vlan i-sid
- vlan mac-address-entry
- vlan mac-address-static
- vlan members
- vlan mlt
- vlan nodal-mep
- vlan nodal-mip-level
- vlan ports ospf-passive
- vlan srcmac
- vlan static-mcastmac

W

- web-server

©Avaya Inc. 2015 All Rights Reserved.

IS-IS Router Configuration

A

- accept adv-rtr (for the GRT)
- accept (for the GRT)
- accept i-sid (for the GRT)
- accept isid-list (for the GRT)
- accept route-map

C

- csnp-interval

I

- ip-source-address
- is-type

M

- manual-area
- max-lsp-gen-interval
- metric

O

- overload
- overload-on-startup

P

- psnp-interval

R

- redistribute bgp (for IS-IS)
- redistribute direct (for IS-IS)
- redistribute ospf (for IS-IS)
- redistribute rip (for IS-IS)
- redistribute static (for IS-IS)
- retransmit-lsp-interval

S

- spbm <1-100>
- spbm <1-100> b-vid
- spbm <1-100> ip enable
- spbm <1-100> lsdb-trap enable
- spbm <1-100> multicast enable
- spbm <1-100> multicast fwd-cache-timeout <10-86400>
- spbm <1-100> nick-name
- spbm <1-100> smlt-peer-system-id
- spbm <1-100> smlt-virtual-bmac

- spf-delay
- sys-name
- system-id

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

Loopback Interface Configuration

I

- ip address (loopback)
- ip area (loopback)
- ip dhcp-relay (loopback)
- ip ospf (loopback)
- ip pim (loopback)

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

mgmtEthernet Interface Configuration

A

- auto-negotiate (for the management port)

D

- duplex (for the management port)

I

- ip address (for the management port)
- ipv6 interface address (for the management port)
- ipv6 interface enable (for the management port)
- ipv6 interface hop-limit (for the management port)
- ipv6 interface link-local (for the management port)
- ipv6 interface mtu (for the management port)
- ipv6 interface name (for the management port)
- ipv6 interface reachable-time (for the management port)
- ipv6 interface retransmit-timer (for the management port)
- ipv6 nd dad-ns (for the management port)

S

- shutdown (for the management port)
- speed (for the management port)

©Avaya Inc. 2015 All Rights Reserved.

MLT Interface Configuration

C

- cp-limit (for an MLT)

I

- ip dhcp-relay (for an MLT)
- isis hello-auth (on an MLT)
- isis l1-dr-priority (on an MLT)
- isis l1-hello-interval (on an MLT)
- isis l1-hello-multiplier (on an MLT)
- isis (on an MLT)
- isis spbm (on an MLT)
- ist enable
- ist peer-ip

L

- lacp (on an MLT)

S

- smlt

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

OSPF Router Configuration

A

- accept adv-rtr (for OSPF)
- area
- area range
- area virtual-link
- area virtual-link message-digest-key
- as-boundary-router enable
- auto-vlink

B

- bad-lsa-ignore enable

D

- default-cost

H

- host-route

I

- ipv6 area
- ipv6 area range
- ipv6 area virtual-link
- ipv6 as-boundary-router
- ipv6 redistribute
- ipv6 router-id
- ipv6 tunnel (for OSPF)

N

- neighbor (for OSPF)
- network (for OSPF)

R

- redistribute (for OSPF)
- rfc1583-compatibility enable
- router-id (for OSPF)

T

- timers basic holddown (for OSPF)
- trap

©Avaya Inc. 2015 All Rights Reserved.

Privileged EXEC

A

- attribute

B

- backup
- boot

C

- cd
- clear alarm
- clear filter acl
- clear ip arp interface
- clear ip dhcp-relay
- clear ip ipfix hash-stats
- clear ip ipfix stats
- clear ip mroute stats
- clear ip route
- clear ipv6 dcache
- clear ipv6 neighbor-cache
- clear ipv6 route static
- clear ipv6 statistics
- clear ipv6 vrrp
- clear ip vrrp
- clear isis lsdb
- clear isis spbm drop-stats
- clear isis stats
- clear khi
- clear lacp
- clear logging
- clear mac-address-table
- clear mlt
- clear qos
- clear radius statistics
- clear slpp
- clear telnet
- clear trace
- !(command number)
- configure
- copy
- cp

D

- delete
- dir
- disable
- dos-chkdsk
- dos-format

E

- editing
- extflash-stop

F

- flight-recorder

G

- grep

I

- ip ospf spf-run

M

- mkdir
- monitor ip mroute stats
- monitor ip vrrp statistics
- monitor mlt error collision
- monitor mlt error main
- monitor mlt stats interface main
- monitor mlt stats interface utilization
- monitor ports error
- monitor ports statistics bridging
- monitor ports statistics dhcp-relay
- monitor ports statistics interface
- monitor ports statistics ospf main
- monitor ports statistics rmon
- monitor ports statistics routing
- more
- mv

P

- peer
- pwd

R

- rename
- reset
- restore
- rlogin
- rsh

S

- save clilog
- save config
- save log
- save snmplog
- save trace
- show access-policy
- show boot config
- show core-files
- show eapol session interface
- show filter acl
- show filter acl ace
- show filter acl action
- show filter acl arp
- show filter acl config
- show filter acl ethernet

- show filter acl ip
- show filter acl log
- show filter acl protocol
- show filter acl statistics
- show history
- show interfaces gigabitethernet
- show interfaces gigabitethernet config
- show interfaces gigabitethernet cp-limit
- show interfaces gigabitethernet error
- show interfaces gigabitethernet fdb-entry
- show interfaces gigabitethernet high-secure
- show interfaces gigabitethernet interface
- show interfaces gigabitethernet l1-config
- show interfaces gigabitethernet limit-fdb-learning
- show interfaces gigabitethernet loop-detected
- show interfaces gigabitethernet lossless-config
- show interfaces gigabitethernet mac-security
- show interfaces gigabitethernet name
- show interfaces gigabitethernet ospf
- show interfaces gigabitethernet rate-limit
- show interfaces gigabitethernet shape
- show interfaces gigabitethernet slpp
- show interfaces gigabitethernet state
- show interfaces gigabitethernet statistics
- show interfaces gigabitethernet statistics bridging
- show interfaces gigabitethernet statistics dhcp-relay
- show interfaces gigabitethernet statistics lacp
- show interfaces gigabitethernet statistics policer
- show interfaces gigabitethernet statistics rmon
- show interfaces gigabitethernet statistics verbose
- show interfaces gigabitethernet vlan
- show interfaces gigabitethernet vrfs
- show interfaces loopback
- show interfaces mgmtethernet
- show interfaces mgmtethernet config-L1
- show interfaces mgmtethernet error
- show interfaces mgmtethernet statistics
- show interfaces vlan
- show interfaces vlan arp
- show interfaces vlan autolearn-mac
- show interfaces vlan dhcp-relay
- show interfaces vlan igmp
- show interfaces vlan igmp-mrdisc
- show interfaces vlan ip
- show interfaces vlan manual-edit-mac
- show interfaces vlan nlb-mode
- show interfaces vlan vlan-bysrcmac
- show interfaces vlan vrfs
- show ip igmp access
- show ip igmp cache
- show ip igmp group
- show ip igmp group count
- show ip igmp group count group <A.B.C.D>
- show ip igmp group group <A.B.C.D>
- show ip igmp group group <A.B.C.D> tracked-members
- show ip igmp group member-subnet
- show ip igmp interface
- show ip igmp mrdisc
- show ip igmp mrdisc neighbors
- show ip igmp router-alert
- show ip igmp sender
- show ip igmp snooping
- show ip igmp snoop-trace
- show ip igmp ssm
- show ip igmp ssm-map

- show ip igmp static
- show ip igmp stream-limit
- show ip igmp sys
- show ip irdp
- show ip isid-list
- show ip redistribute
- show link-flap-detect
- show pluggable-optical-modules
- show ports statistics ospf extended
- show ports statistics ospf main
- show running-config
- show slot
- show spanning-tree bpdu-filtering
- software
- software patch
- software reset-commit-time
- source
- sys action
- sys action cpu-switch-over
- sys shutdown

T

- trace ipv6 base
- trace ipv6 forwarding
- trace ipv6 nd
- trace ipv6 rtm
- trace ipv6 transport
- traceroute

U

- usb-stop

©Avaya Inc. 2015 All Rights Reserved.

RIP Router Configuration

D

- default-metric (for RIP)
- domain

N

- network (for RIP)

R

- redistribute (for RIP)

T

- timers basic holddown (for RIP)
- timers basic timeout
- timers basic update

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

Route-Map Configuration

E

- enable (for a route policy)

M

- match as-path
- match community
- match community-exact
- match extcommunity
- match interface
- match local-preference
- match metric
- match network
- match next-hop
- match protocol
- match route-source
- match route-type
- match tag
- match vrf
- match vrfids

N

- name

P

- permit

S

- set as-path
- set as-path-mode
- set automatic-tag
- set community
- set community-mode
- set injectlist
- set ip-preference
- set local-preference
- set mask
- set metric
- set metric-type
- set metric-type-internal
- set next-hop
- set nssa-pbit
- set origin
- set origin-egp-as
- set tag
- set weight

NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

User EXEC

C

- clear-stats
- clock set

D

- debug-file remove
- dump ar

E

- eapol init
- eapol re-authenticate
- enable
- exit

H

- hash-calc getEcmpRoute
- hash-calc getmltindex traffic-type
- help

I

- ip bgp apply redistribute
- ip bgp restart-bgp
- ip bgp stats-clear-counters
- ip ecmp pathlist-apply
- ip igmp flush port
- ip igmp flush vlan
- ip ipfix flush
- ip ospf apply accept
- ip ospf apply accept adv-rtr
- ip ospf apply redistribute
- ip rip apply redistribute
- isis apply accept (for the GRT)
- isis apply accept (for the VRF)
- isis apply redistribute

L

- l2 ping ip-address
- l2 ping vlan
- l2 tracemroute
- l2 traceroute ip-address
- l2 traceroute vlan
- l2 tracetree
- line-card
- linktrace
- login
- logout

- loopback
- ls

M

- manualtrigger ip rip interface
- md5

P

- ping
- pwc

R

- remove

S

- show alarm database
- show alarm database
- show application slamon agent
- show application vsptalk
- show application vsptalk client
- show application vsptalk server
- show autotopology
- show banner
- show basic config
- show bgp ipv6 aggregates
- show bgp ipv6 imported-routes
- show bgp ipv6 networks
- show bgp ipv6 redistributed-routes
- show bgp ipv6 route
- show brouter
- show cfm cmac
- show cfm maintenance-association
- show cfm maintenance-domain
- show cfm maintenance-endpoint
- show cfm spbm
- show cli info
- show clilog
- show cli password
- show clock
- show debug-file
- show debug ip pim
- show eapol auth-diags interface
- show eapol auth-stats interface
- show eapol multihost-session-stats interface
- show eapol port
- show eapol session-stats interface
- show eapol status interface
- show eapol system
- show fabric
- show fdb-filter
- show ftp-access
- show fulltech
- show ha-state
- show hosts
- show ip arp
- show ip arp interface
- show ip arp static-mcastmac
- show ip as-list
- show ip bgp aggregates
- show ip bgp cidr-only
- show ip bgp conf
- show ip bgp confederation

- show ip bgp dampened-paths
- show ip bgp flap-damp-config
- show ip bgp imported-routes
- show ip bgp neighbors
- show ip bgp networks
- show ip bgp peer-group
- show ip bgp redistributed-routes
- show ip bgp route
- show ip bgp stats
- show ip bgp summary
- show ip bgp vpnv4
- show ip community-list
- show ip dhcp-relay
- show ip directed-broadcast
- show ip dns
- show ip ecmp
- show ip extcommunity-list
- show ip forward-protocol udp
- show ip forward-protocol udp portfwd
- show ip forward-protocol udp portfwdlist
- show ip interface
- show ip ipfix
- show ip ipfix collector
- show ip ipfix export
- show ip ipfix exporter
- show ip ipfix flows
- show ip ipfix hash-statistics
- show ip ipfix interface
- show ip ipvpn
- show ip isis accept
- show ip isis redistribute
- show ip mroute hw-resource-usage
- show ip mroute interface
- show ip mroute next-hop
- show ip mroute route
- show ip mroute static-source-group
- show ip mroute stats
- show ip ospf
- show ip ospf accept
- show ip ospf area
- show ip ospf area-range
- show ip ospf ase
- show ip ospf authentication
- show ip ospf default-cost
- show ip ospf host-route
- show ip ospf ifstats
- show ip ospf int-auth
- show ip ospf interface
- show ip ospf int-timers
- show ip ospf lsdb
- show ip ospf neighbor
- show ip ospf port-error
- show ip ospf redistribute
- show ip ospf stats
- show ip ospf virtual-link
- show ip pim
- show ip pim active-rp
- show ip pim bsr
- show ip pim interface
- show ip pim mode
- show ip pim mroute
- show ip pim neighbor
- show ip pim rp-candidate
- show ip pim rp-hash
- show ip pim static-rp

- show ip pim virtual-neighbor
- show ip prefix-list
- show ip rip
- show ip rip interface
- show ip rip redistribute
- show ip route
- show ip route preference
- show ip routing
- show ip rsmlt
- show ip rsmlt edge-support
- show ip tcp statistics
- show ip udp statistics
- show ipv6 address
- show ipv6 dcache
- show ipv6 dhcp-relay
- show ipv6 forwarding
- show ipv6 global
- show ipv6 interface
- show ipv6 nd
- show ipv6 nd-prefix
- show ipv6 neighbor
- show ipv6 ospf
- show ipv6 ospf area
- show ipv6 ospf area-range
- show ipv6 ospf ase
- show ipv6 ospf interface
- show ipv6 ospf int-timers
- show ipv6 ospf lsdb
- show ipv6 ospf nbma-nbr interface
- show ipv6 ospf neighbor
- show ipv6 ospf redistribute
- show ipv6 ospf statistics
- show ipv6 prefix-list
- show ipv6 route
- show ipv6 tcp
- show ipv6 trace
- show ipv6 tunnel
- show ipv6 udp
- show ipv6 vrrp
- show ipv6 vrrp address
- show ipv6 vrrp interface
- show ipv6 vrrp interface gigabitethernet statistics
- show ipv6 vrrp statistics
- show ip vrf
- show ip vrf mvpn
- show ip vrrp
- show ip vrrp address
- show ip vrrp interface
- show ip vrrp interface gigabitEthernet
- show ip vrrp interface gigabitEthernet statistics
- show ip vrrp interface vlan
- show ip vrrp statistics
- show isis
- show isis adjacencies
- show isis area
- show isis int-auth
- show isis int-ckt-level
- show isis int-counters
- show isis interface
- show isis int-l1-cntl-pkts
- show isis int-l2-cntl-pkts
- show isis int-timers
- show isis lsdb
- show isis lsdb ip-unicast
- show isis manual-area

- show isis net
- show isis spbm
- show isis spb-mcast-summary
- show isis spbm drop-stats port
- show isis spbm ip-multicast-route
- show isis spbm ip-multicast-route group
- show isis spbm ip-multicast-route vlan
- show isis spbm ip-multicast-route vrf
- show isis spbm ip-multicast-route vsn-isid
- show isis spbm ip-unicast-fib
- show isis spbm i-sid
- show isis spbm multicast
- show isis spbm multicast-fib
- show isis spbm nick-name
- show isis spbm unicast-fib
- show isis spbm unicast-tree
- show isis statistics
- show isis system-id
- show ist mlt
- show ist stat
- show khi cpp
- show khi forwarding
- show khi performance
- show lacp
- show lacp interface
- show license
- show logging
- show logging file
- show mac-security mac-da-filter
- show mirror-by-port
- show mlt
- show mlt error collision
- show mlt error main
- show mlt stats
- show monitor-statistics
- show multicast software-forwarding
- show multicast square-smlt
- show ntp
- show pcap
- show pcap capture-filter
- show pcap dump
- show pcap port
- show pcap stats
- show qos 802.1p-override
- show qos egressmap
- show qos ingressmap
- show qos lossless-802.1p
- show qos policer
- show qos policy-config
- show qos shaper
- show qos statistics policy
- show radius
- show radius-server
- show radius-server statistics
- show radius snmp
- show remote-mirroring
- show rmon
- show rmon stats
- show route-map
- show routing statistics
- show slpp
- show slpp interface
- show smlt
- show snmplog
- show snmp-server

- show software
- show software patch
- show spanning-tree config
- show spanning-tree mstp config
- show spanning-tree mstp msti config
- show spanning-tree mstp msti port
- show spanning-tree mstp port role
- show spanning-tree mstp port statistics
- show spanning-tree mstp statistics
- show spanning-tree mstp status
- show spanning-tree rstp config
- show spanning-tree rstp port config
- show spanning-tree rstp port role
- show spanning-tree rstp port statistics
- show spanning-tree rstp port status
- show spanning-tree rstp statistics
- show spanning-tree rstp status
- show spanning-tree status
- show spbm
- show ssh
- show sys dns
- show sys force-msg
- show sys-info
- show syslog
- show syslog host
- show sys mgid-usage
- show sys msg-control
- show sys mtu
- show sys power
- show sys setting
- show sys software
- show sys stats ipmc-threshold-exceeded-cnt
- show sys topology-ip
- show tacacs
- show tech
- show telnet-access
- show trace cfm
- show trace file
- show trace level
- show trace modid-list
- show trace spbm isis
- show unsupported-lastset
- show users
- show vlacp
- show vlan advance
- show vlan autolearn-mac
- show vlan basic
- show vlan brouter-port
- show vlan i-sid
- show vlan mac-address-entry
- show vlan mac-address-static
- show vlan manual-edit-mac
- show vlan members
- show vlan nodal-mep
- show vlan nodal-mip-level
- show vlan remote-mac-table
- show vlan src-mac
- show vlan static-mcastmac
- show web-server
- slot reset
- ssh (connection)

T

- telnet

terminal

- trace cfm level <0-4>
- trace filter file
- trace filter module
- trace flags isis
- trace flags ospf
- trace grep
- trace level
- trace route-map
- trace screen
- trace shutdown
- trace spbm isis level <0-4>

©Avaya Inc. 2015 All Rights Reserved.

VLAN Interface Configuration

D

- dsapssap

I

- ip address (on a VLAN)
- ip arp-proxy enable (for a VLAN)
- ip arp-response (for a VLAN)
- ip dhcp-relay (for a VLAN)
- ip directed-broadcast (for a VLAN)
- ip forward-protocol udp broadcastmask
- ip forward-protocol udp maxttl
- ip forward-protocol udp (on a VLAN)
- ip forward-protocol udp portfwdlist (on a VLAN)
- ip igmp access-list (for a VLAN)
- ip igmp access-list mode (for a VLAN)
- ip igmp (for a VLAN)
- ip igmp igmpv3-explicit-host-tracking (for a VLAN)
- ip igmp immediate-leave (for a VLAN)
- ip igmp immediate-leave-members
- ip igmp mrdisc
- ip igmp snoop-querier
- ip igmp snoop-querier-addr
- ip igmp static-group
- ip igmp stream-limit (for a VLAN)
- ip igmp stream-limit-group
- ip irdp address (for a VLAN)
- ip irdp holdtime (for a VLAN)
- ip irdp maxadvertinterval (for a VLAN)
- ip irdp minadvertinterval (for a VLAN)
- ip irdp multicast (for a VLAN)
- ip irdp preference (for a VLAN)
- ip ospf advertise-when-down enable (for a VLAN)
- ip ospf area (for a VLAN)
- ip ospf authentication-key WORD<0-8> (for a VLAN)
- ip ospf authentication-type <none|message-digest|simple> (for a VLAN)
- ip ospf cost <1-65535> (for a VLAN)
- ip ospf dead-interval <0-2147483647> (for a VLAN)
- ip ospf enable (for a VLAN)
- ip ospf hello-interval <1-65535> (for a VLAN)
- ip ospf message-digest-key <1-255> md5-key WORD<0-16> (for a VLAN)
- ip ospf mtu-ignore enable (for a VLAN)
- ip ospf network <broadcast|nbma|passive> (for a VLAN)
- ip ospf poll-interval <0-2147483647> (for a VLAN)
- ip ospf primary-md5-key <1-255> (for a VLAN)
- ip ospf priority <0-255> (for a VLAN)
- ip ospf retransmit-interval <0-3600> (for a VLAN)
- ip ospf transit-delay <0-3600> (for a VLAN)
- ip ospf vlan (for a VLAN)
- ip pim active (for a VLAN)

ip pim bsr-candidate preference (for a VLAN)
- ip pim enable (for a VLAN)
- ip pim hello-interval <0-18724> (for a VLAN)
- ip pim interface-type <active|passive> (for a VLAN)
- ip pim join-prune-interval <1-18724> (for a VLAN)
- ip pim passive (for a VLAN)
- ip rip advertise-when-down enable (for a VLAN)
- ip rip auto-aggregation enable (for a VLAN)
- ip rip cost (for a VLAN)
- ip rip default-listen enable (for a VLAN)
- ip rip default-supply enable (for a VLAN)
- ip rip enable (for a VLAN)
- ip rip holddown (for a VLAN)
- ip rip in-policy (for a VLAN)
- ip rip listen (for a VLAN)
- ip rip out-policy (for a VLAN)
- ip rip poison enable (for a VLAN)
- ip rip receive version (for a VLAN)
- ip rip send (for a VLAN)
- ip rip supply (for a VLAN)
- ip rip timeout (for a VLAN)
- ip rip triggered (for a VLAN)
- ip rsmlt
- ip rvs-path-chk (for a VLAN)
- ip rvs-path-chk mode (for a VLAN)
- ip spb-multicast enable (for a VLAN)
- ipv6 dhcp-relay (for a VLAN)
- ipv6 forwarding (for a VLAN)
- ipv6 interface address (for a VLAN)
- ipv6 interface enable (for a VLAN)
- ipv6 interface hop-limit (for a VLAN)
- ipv6 interface link-local (for a VLAN)
- ipv6 interface mac-offset
- ipv6 interface mtu (for a VLAN)
- ipv6 interface name (for a VLAN)
- ipv6 interface reachable-time (for a VLAN)
- ipv6 interface retransmit-timer (for a VLAN)
- ipv6 nd dad-ns (for a VLAN)
- ipv6 nd managed-config-flag (for a VLAN)
- ipv6 nd other-config-flag (for a VLAN)
- ipv6 nd prefix (for a VLAN)
- ipv6 nd ra-lifetime (for a VLAN)
- ipv6 nd rtr-advert-max-interval (for a VLAN)
- ipv6 nd rtr-advert-min-interval (for a VLAN)
- ipv6 nd send-ra (for a VLAN)
- ipv6 ospf area (for a VLAN)
- ipv6 ospf (for a VLAN)
- ipv6 rvs-path-chk (for a VLAN)
- ipv6 vrrp address (for a VLAN)
- ipv6 vrrp (for a VLAN)
- ip vrrp (for a VLAN)

N

- nlb-mode

S

- show interface vlan nlb-mode
- slpp (on a VLAN)

V

- vrf (for a VLAN)

NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

VRF Router Configuration

I

- ip alternative-route (on a VRF)
- ip arp (for a VRF)
- ip as-list (for a VRF)
- ip bgp
- ip bgp aggregate-address
- ip bgp aggregation
- ip bgp always-compare-med
- ip bgp auto-peer-restart enable
- ip bgp auto-summary
- ip bgp debug-screen
- ip bgp default-information
- ip bgp default local-preference
- ip bgp default-metric
- ip bgp deterministic-med enable
- ip bgp enable
- ip bgp flap-dampening
- ip bgp global-debug mask
- ip bgp ibgp-report-import-rt enable
- ip bgp ignore-illegal-rtrid enable
- ip bgp in-route-map
- ip bgp multiple-paths <1-8>
- ip bgp neighbor
- ip bgp neighbor password
- ip bgp network
- ip bgp no-med-path-is-worst enable
- ip bgp out-route-map WORD<0-256>
- ip bgp quick-start enable
- ip bgp redistribute
- ip bgp router-id {A.B.C.D}
- ip bgp synchronization
- ip bgp traps enable
- ip igmp generate-log (for a VRF)
- ip igmp generate-trap (for a VRF)
- ip igmp immediate-leave-mode (for a VRF)
- ip igmp ssm dynamic-learning (for a VRF)
- ip igmp ssm group-range (for a VRF)
- ip igmp ssm-map (for a VRF)
- ip isid-list (for a VRF)
- ip mroute resource-usage (for a VRF)
- ip ospf default-cost (for a VRF)
- ip ospf redistribute
- ip prefix-list (for a VRF)
- ip rip redistribute
- ip route (for a VRF)
- ipvpn
- ipvpn enable
- i-sid
- isis accept adv-rtr (for a VRF)
- isis accept (for a VRF)

isis redistribute bgp
- isis redistribute direct
- isis redistribute ospf
- isis redistribute rip
- isis redistribute static

M

- mvpn enable
- mvpn fwd-cache-timeout <10-86400>

©Avaya Inc. 2015 All Rights Reserved.

VRRP Router Configuration

I

- ipv6 send-trap enable

P

- ping-virtual-address

S

- send-trap

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

accept adv-rtr (for OSPF)

Use a route policy to define how the switch Redistribute external routes from a specified source into an OSPF domain. The policy defines which route types the switch accepts and Redistribute.

Syntax

- `accept adv-rtr {A.B.C.D}`
- `accept adv-rtr {A.B.C.D} enable`
- `accept adv-rtr {A.B.C.D} metric-type { type1 | type2 | any }`
- `accept adv-rtr {A.B.C.D} route-policy WORD<0-64>`
- `default accept adv-rtr {A.B.C.D}`
- `default accept adv-rtr {A.B.C.D} enable`
- `default accept adv-rtr {A.B.C.D} metric-type`
- `default accept adv-rtr {A.B.C.D} route-policy`
- `no accept adv-rtr {A.B.C.D}`
- `no accept adv-rtr {A.B.C.D} enable`

Default

None

Command mode

OSPF Router Configuration

Command parameters

Parameter	Description
{A.B.C.D}	Specifies the IP address.
enable	Enables an OSPF accept entry for a specified advertising router.
metric-type <type1|type2|any>	Indicates the OSPF external type. This parameter describes which types of OSPF external routes match this entry. any means match all external routes. type1 means match external type 1 only. type2 means match external type 2 only.
route-policy WORD<0-64>	Specifies the name of the route policy to use for filtering external routes advertised by the specified advertising router before accepting into the routing table.

©Avaya Inc. 2015 All Rights Reserved.

accept adv-rtr (for the GRT)

Configure an Intermediate-System-to-Intermediate-System (IS-IS) accept policy instance to apply to a specific advertising Backbone Edge Bridge (BEB) for the Global Routing Table (GRT).

Syntax

- `accept adv-rtr <x.xx.xx>`
- `accept adv-rtr <x.xx.xx> enable`
- `accept adv-rtr <x.xx.xx> i-sid <1-16777215>`
- `accept adv-rtr <x.xx.xx> i-sid <1-16777215> enable`
- `accept adv-rtr <x.xx.xx> i-sid <1-16777215> route-map WORD<1-64>`
- `accept adv-rtr <x.xx.xx> isid-list WORD<1-32>`
- `accept adv-rtr <x.xx.xx> isid-list WORD<1-32> enable`
- `accept adv-rtr <x.xx.xx> isid-list WORD<1-32> route-map WORD<1-64>`
- `accept adv-rtr <x.xx.xx> route-map WORD<1-64>`
- `no accept adv-rtr <x.xx.xx>`
- `no accept adv-rtr <x.xx.xx> enable`
- `no accept adv-rtr <x.xx.xx> i-sid <1-16777215>`
- `no accept adv-rtr <x.xx.xx> i-sid <1-16777215> enable`
- `no accept adv-rtr <x.xx.xx> i-sid <1-16777215> route-map`
- `no accept adv-rtr <x.xx.xx> isid-list WORD<1-32>`
- `no accept adv-rtr <x.xx.xx> isid-list WORD<1-32> enable`
- `no accept adv-rtr <x.xx.xx> route-map`

Default

None

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description
`<x.xx.xx>`	Specifies the Shortest Path Bridging MAC (SPBM) nickname at a level for each advertising BEB.
`adv-rtr`	Specifies the Shortest Path Bridging MAC (SPBM) nickname for an advertising BEB

<x.xx.xx>	for the IS-IS accept policy.
enable	Enables an IS-IS accept policy.
i-sid <0-16777215>	Specifies a service instance identifier (I-SID) number that represents a local or remote Layer 3 VSN for the IS-IS accept policy.
isid-list WORD <1-32>	Specifies a name for a list of I-SID numbers that represent local or remote Layer 3 VSN for the IS-IS accept policy.
route-map WORD<1-64>	Configures the IS-IS route policy by name.

©Avaya Inc. 2015 All Rights Reserved.

accept (for the GRT)

Configure an Intermediate-System-to-Intermediate-System (IS-IS) accept policy instance to apply to all routes from all Backbone Edge Bridges (BEBs) for the Global Routing Table (GRT).

Syntax

- `accept i-sid <1-16777215>`
- `accept i-sid <1-16777215> enable`
- `accept i-sid <1-16777215> route-map WORD<1-64>`
- `accept isid-list WORD<1-32>`
- `accept isid-list WORD<1-32> enable`
- `accept isid-list WORD<1-32> route-map WORD<1-64>`
- `accept route-map WORD<1-64>`
- `no accept i-sid <1-16777215>`
- `no accept i-sid <1-16777215> enable`
- `no accept i-sid <1-16777215> route-map`
- `no accept isid-list WORD<1-32>`
- `no accept isid-list WORD<1-32> enable`
- `no accept isid-list WORD<1-32> route-map`
- `no accept route-map`

Default

None

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description
`enable`	Enables an IS-IS accept policy.
`i-sid <1-16777215>`	Specifies a service instance identifier (I-SID) number that represents a local or remote Layer 3 VSN for the IS-IS accept policy.
`isid-list WORD <1-32>`	Specifies a name for a list of I-SID numbers that represent local or remote Layer 3 VSN for the IS-IS accept policy.
`route-map WORD<1-64>`	Configures the IS-IS route policy by name.

NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

accept i-sid (for the GRT)

Configure an Intermediate-System-to-Intermediate-System (IS-IS) accept policy instance to apply to a specific Service Instance Identifier (I-SID) for the Global Routing Table (GRT).

Syntax

- `accept i-sid <1-16777215>`
- `accept i-sid <1-16777215> enable`
- `accept i-sid <1-16777215> route-map WORD<1-64>`
- `no accept i-sid <1-16777215>`
- `no accept i-sid <1-16777215> enable`
- `no accept i-sid <1-16777215> route-map`

Default

None

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description
`enable`	Enables an IS-IS accept policy.
`i-sid <1-16777215>`	Specifies a service instance identifier (I-SID) number that represents a local or remote Layer 3 VSN for the IS-IS accept policy.
`route-map WORD<1-64>`	Configures the IS-IS route policy by name.

©Avaya Inc. 2015 All Rights Reserved.

accept isid-list (for the GRT)

Configure an Intermediate-System-to-Intermediate-System (IS-IS) accept policy instance to apply to a specific list of Service Instance Identifiers (I-SIDs) for the Global Routing Table (GRT).

Syntax

- `accept isid-list <1-16777215>`
- `accept isid-list <1-16777215> enable`
- `accept isid-list <1-16777215> route-map WORD<1-64>`
- `no accept isid-list <1-16777215>`
- `no accept isid-list <1-16777215> enable`
- `no accept isid-list <1-16777215> route-map`

Default

None

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description
`enable`	Enables an IS-IS accept policy.
`isid-list WORD <1-32>`	Specifies a name for a list of I-SID numbers that represent local or remote Layer 3 VSN for the IS-IS accept policy.
`route-map WORD<1-64>`	Configures the IS-IS route policy by name.

©Avaya Inc. 2015 All Rights Reserved.

accept route-map

Configure an Intermediate-System-to-Intermediate-System (IS-IS) accept policy instance to apply using a specific route-map for the Global Routing Table (GRT).

Syntax

- `accept route-map WORD<1-64>`
- `no accept route-map`

Default

None

Command mode

IS-IS Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

access-diffserv

Configure a port as trusted or untrusted to determine the Layer 3 QoS actions the switch performs. A trusted (core) port honors incoming Differentiated Services Code Point (DSCP) markings. An untrusted (access) port overrides DSCP markings.

Syntax

- `access-diffserv`
- `access-diffserv enable`
- `access-diffserv port {slot/port[-slot/port][,...]}`
- `access-diffserv port {slot/port[-slot/port][,...]} enable`
- `default access-diffserv`
- `default access-diffserv enable`
- `default access-diffserv port {slot/port[-slot/port][,...]}`
- `default access-diffserv port {slot/port[-slot/port][,...]} enable`
- `no access-diffserv`
- `no access-diffserv enable`
- `no access-diffserv port {slot/port[-slot/port][,...]}`
- `no access-diffserv port {slot/port[-slot/port][,...]} enable`

Default

The default configuration is trusted (disabled).

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	If enabled, specifies an access port and overrides incoming DSCP bits. If disabled, specifies a core port and honors and handles incoming DSCP bits. The default is disabled.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

access-policy

Configure an access policy to control access to the switch. You can define network stations that are explicitly allowed to access the switch or network stations that are explicitly forbidden to access the switch. For each service, you can also specify the level of access; for example, read-only or read/write/all. Use the command without parameters to globally enable access policies.

Syntax

- `access-policy`
- `access-policy <1-65535>`
- `default access-policy`
- `default access-policy <1-65535>`
- `no access-policy`
- `no access-policy <1-65535>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-65535>	Specifies the policy ID.

©Avaya Inc. 2015 All Rights Reserved.

access-policy <1-65535> accesslevel

Restrain access to criteria specified in the access policy. If true, the system accepts only the currently configured access level. If false, the system accepts access up to the configured access level.

Syntax

- `access-policy <1-65535> accesslevel { ro | rwa | rw }`
- `default access-policy <1-65535> accesslevel`

Default

`The default is ro.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`{ ro | rwa | rw }`	Specifies the access level.
`<1-65535>`	Specifies the policy ID.

©Avaya Inc. 2015 All Rights Reserved.

access-policy <1-65535> access-strict

Specify the level of access if you configure the policy to allow access. The access-strict command ties to the accesslevel command. If you enable access-strict, the access policy looks at the accesslevel value, and only applies to that access level. If you disable access-strict (false), the policy looks at the value for accesslevel, and then the system applies the policy to anyone with equivalent rights or higher.

Syntax

- `access-policy <1-65535> access-strict`
- `default access-policy <1-65535> access-strict`
- `no access-policy <1-65535> access-strict`

Default

`The default is disabled (false).`

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-65535>	Specifies the policy ID.

©Avaya Inc. 2015 All Rights Reserved.

access-policy <1-65535> enable

Activate the access policy.

Syntax

- `access-policy <1-65535> enable`
- `default access-policy <1-65535> enable`
- `no access-policy <1-65535> enable`

Default

`The default is disabled (off).`

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-65535>	Specifies the policy ID.

©Avaya Inc. 2015 All Rights Reserved.

access-policy <1-65535> ftp

Activate or disables FTP for the specified policy. Because FTP derives its login and password from the ACLI management filters, FTP works for read-write-all (rwa) and readwrite (rw) access but not for the read-only (ro) access.

Syntax

- `access-policy <1-65535> ftp`
- `default access-policy <1-65535> ftp`
- `no access-policy <1-65535> ftp`

Default

`The default is disabled.`

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-65535>	Specifies the policy ID.

©Avaya Inc. 2015 All Rights Reserved.

access-policy <1-65535> host

For remote login access, specify the trusted host address as an IP address.

Syntax

- `access-policy <1-65535> host WORD<0-46>`
- `default access-policy <1-65535> host`
- `no access-policy <1-65535> host`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-65535>	Specifies the policy ID.
WORD<0-46>	Specifies the IPv4 or IPv6 address.

©Avaya Inc. 2015 All Rights Reserved.

access-policy <1-65535> http

Activate the HTTP for this access policy.

Syntax

- `access-policy <1-65535> http`
- `default access-policy <1-65535> http`
- `no access-policy <1-65535> http`

Default

The default is disabled.

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-65535>	Specifies the policy ID.

©Avaya Inc. 2015 All Rights Reserved.

access-policy <1-65535> mode

Specify whether the designated network address is allowed access to the system through the specified access service.

Syntax

- `access-policy <1-65535> mode { allow | deny }`
- `default access-policy <1-65535> mode`

Default

`The default is allow.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`{ allow | deny }`	Allows or denies access to the designated network address. Note: If you configure the access policy mode to deny, the system checks the mode and service, and if they match the system denies the connection. With the access policy mode configured to deny, the system does not check accesslevel or access-strict information. If you configure the access policy mode to allow, the system checks the accesslevel and access-strict information.
`<1-65535>`	Specifies the policy ID.

©Avaya Inc. 2015 All Rights Reserved.

access-policy <1-65535> name

Specify a name expressed as a string.

Syntax

- `access-policy <1-65535> name WORD<0-15>`
- `default access-policy <1-65535> name`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-65535>	Specifies the policy ID.

©Avaya Inc. 2015 All Rights Reserved.

access-policy <1-65535> network

Specify the IP address and subnet mask that can access the system through the specified access service.

Syntax

- `access-policy <1-65535> network WORD<1-46> <0-128>`
- `default access-policy <1-65535> network`
- `no access-policy <1-65535> network`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-65535>	Specifies the policy ID.
WORD<1-46> <0-128>	Specifies the IP address and subnet mask

©Avaya Inc. 2015 All Rights Reserved.

access-policy <1-65535> precedence

Specify a precedence value for a policy, expressed as a number from 1-128. The precedence value determines which policy the system uses if multiple policies apply. Lower numbers take higher precedence.

Syntax

- `access-policy <1-65535> precedence <1-128>`
- `default access-policy <1-65535> precedence`

Default

`The default is 10.`

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-128>	Specifies a precedence value for a policy.
<1-65535>	Specifies the policy ID.

©Avaya Inc. 2015 All Rights Reserved.

access-policy <1-65535> rlogin

Activate remote logon for the access policy.

Syntax

- `access-policy <1-65535> rlogin`
- `default access-policy <1-65535> rlogin`
- `no access-policy <1-65535> rlogin`

Default

`The default is disabled.`

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-65535>	Specifies the policy ID.

©Avaya Inc. 2015 All Rights Reserved.

access-policy <1-65535> snmp-group

Add a Simple Network Management Protocol version 3 (SNMP-v3) group under the access policy.

Syntax

- `access-policy <1-65535> snmp-group WORD<1-32> { snmpv1 | snmpv2c | usm }`
- `no access-policy <1-65535> snmp-group WORD<1-32> { snmpv1 | snmpv2c | usm }`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`{ snmpv1 | snmpv2c | usm }`	Configures the security model.
`<1-65535>`	Specifies the policy ID.
`WORD<1-32>`	Specifies the name of the group.

©Avaya Inc. 2015 All Rights Reserved.

access-policy <1-65535> snmpv3

Activate Simple Network Management Protocol (SNMP) version 3 for the access policy.

Syntax

- `access-policy <1-65535> snmpv3`
- `default access-policy <1-65535> snmpv3`
- `no access-policy <1-65535> snmpv3`

Default

`The default is disabled.`

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-65535>	Specifies the policy ID.

©Avaya Inc. 2015 All Rights Reserved.

access-policy <1-65535> ssh

Activate Secure Shell (SSH) for the access policy.

Syntax

- `access-policy <1-65535> ssh`
- `default access-policy <1-65535> ssh`
- `no access-policy <1-65535> ssh`

Default

The default is disabled.

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-65535>	Specifies the policy ID.

©Avaya Inc. 2015 All Rights Reserved.

access-policy <1-65535> telnet

Activate Telnet for the access policy.

Syntax

- `access-policy <1-65535> telnet`
- `default access-policy <1-65535> telnet`
- `no access-policy <1-65535> telnet`

Default

`The default is disabled.`

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-65535>	Specifies the policy ID.

©Avaya Inc. 2015 All Rights Reserved.

access-policy <1-65535> tftp

Activate the Trivial File Transfer Protocol (TFTP) for this access policy.

Syntax

- `access-policy <1-65535> tftp`
- `default access-policy <1-65535> tftp`
- `no access-policy <1-65535> tftp`

Default

The default is disabled.

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-65535>	Specifies the policy ID.

©Avaya Inc. 2015 All Rights Reserved.

access-policy <1-65535> username

Specify the trusted host user name for remote login access.

Syntax

- `access-policy <1-65535> username WORD<0-30>`
- `default access-policy <1-65535> username`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-65535>	Specifies the policy ID.
WORD<0-30>	Specifies the username.

©Avaya Inc. 2015 All Rights Reserved.

access-policy by-mac

Configure access-policies by MAC address to allow or deny local MAC addresses on the network management port after an access policy is activated. If the source MAC does not match a configured entry, then the default action is taken.

Syntax

- `access-policy by-mac 0x00:0x00:0x00:0x00:0x00:0x00 { allow | deny }`
- `access-policy by-mac action { allow | deny }`
- `default access-policy by-mac <0x00:0x00:0x00:0x00:0x00:0x00>`
- `default access-policy by-mac action`
- `no access-policy by-mac <0x00:0x00:0x00:0x00:0x00:0x00>`

Default

`The default action is allow.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<0x00:0x00:0x00:0x00:0x00:0x00> <allow|deny>`	Adds a MAC address to the policy. Enter the MAC address in hexadecimal format. Specify the action to take for the MAC address.
`action <allow|deny>`	Specifies the action for a MAC address that does not match the policy.

©Avaya Inc. 2015 All Rights Reserved.

action

Flush or clear the Address Resolution Protocol (ARP) tables for administrative and troubleshooting purposes.

Syntax

- `action { none | flushMacFdb | flushArp | flushIp | triggerRipUpdate | flushAll | clearLoopDetectAlarm }`
- `action port {slot/port[-slot/port][,...]} { none | flushMacFdb | flushArp | flushIp | triggerRipUpdate | flushAll | clearLoopDetectAlarm }`
- `default action`
- `default action port {slot/port[-slot/port][,...]}`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
ClearLoopDetectAlarm	Sets action to clear loop detect alarm.
flushAll	Sets action to flush all.
flushArp	Sets action to flushArp.
flushIp	Flush or clear the routing tables for administrative and troubleshooting purposes.
flushMacFdb	Flush or clear the MAC address tables for administrative and troubleshooting purposes.
none	Sets action to none.
port {slot/port [-slot/port][,...]}	Specifies the slot and the port list that needs to be changed.
triggerRipUpdate	Force RIP to update the routing table so that the port or VLAN uses the latest routing information.

©Avaya Inc. 2015 All Rights Reserved.

aggregate-address

Add or delete an aggregate address in a BGP routing table.

Syntax

- aggregate-address WORD<1-256>
- aggregate-address WORD<1-256> advertise-map WORD<0-1536>
- aggregate-address WORD<1-256> as-set
- aggregate-address WORD<1-256> attribute-map WORD<0-1536>
- aggregate-address WORD<1-256> summary-only
- aggregate-address WORD<1-256> suppress-map WORD<0-1536>
- default aggregate-address WORD<1-256>
- default aggregate-address WORD<1-256> advertise-map
- default aggregate-address WORD<1-256> as-set
- default aggregate-address WORD<1-256> attribute-map
- default aggregate-address WORD<1-256> summary-only
- default aggregate-address WORD<1-256> suppress-map
- no aggregate-address WORD<1-256>
- no aggregate-address WORD<1-256> advertise-map WORD<0-1536>
- no aggregate-address WORD<1-256> as-set
- no aggregate-address WORD<1-256> attribute-map WORD<0-1536>
- no aggregate-address WORD<1-256> summary-only
- no aggregate-address WORD<1-256> suppress-map WORD<0-1536>

Default

The default value is disable.

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
advertise-map WORD<0-	Specifies the route map name (any string length between 0 and 64 characters) for route advertisements.

1536>	
as-set	Enables autonomous system (AS) information.
attribute-map WORD <0-1536>	Specifies the route map name (string length between 0 and 64 characters).
summary-only	Enables the summarization of routes not included in routing updates. This parameter creates the aggregate route and suppresses advertisements of more specific routes to all neighbors. The default value is disable.
suppress-map WORD<0-1536>	Specifies the route map name (string length between 0 and 64 characters) for the suppressed route list.
WORD <1-256>	Specifies the IPv4 or the IPv6 address and an integer value in the range of 1 to 256.

©Avaya Inc. 2015 All Rights Reserved.

application

Use this command to enter Application Configuration mode.

Syntax

- `application`

Default

None

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

area

Import information from other areas to learn their OSPF relationships and create normal, stubby, or not-so-stubby areas (NSSA). Place stubby or NSSAs at the edge of an OSPF routing domain.

Syntax

- `area {A.B.C.D}`
- `area {A.B.C.D} default-cost <0-16777215>`
- `area {A.B.C.D} import external`
- `area {A.B.C.D} import noexternal`
- `area {A.B.C.D} import nssa`
- `area {A.B.C.D} import-summaries enable`
- `area {A.B.C.D} stub`
- `default area {A.B.C.D}`
- `default area {A.B.C.D} default-cost`
- `default area {A.B.C.D} import`
- `default area {A.B.C.D} import-summaries enable`
- `default area {A.B.C.D} stub`
- `no area {A.B.C.D}`
- `no area {A.B.C.D} import-summaries enable`

Default

None

Command mode

OSPF Router Configuration

Command parameters

Parameter	Description
`default-cost <0-16777215>`	Stub area default metric for this stub area, which is the cost from 0 to 16 777 215. This is the metric value applied at the indicated type of service.
`import <external|noexternal|nssa>`	Specifies the type of area: external - Stub and NSSA (not so stubby area) are both false. noexternal-Configures the area as stub area. nssa - Configures the area as NSSA.
`import-summaries enable`	Configures the area support to import summary advertisements into a stub area. This parameter must be used only if the area is

	a stub area.
stub	Configures the import external option for this area as stub. A stub area has only one exit point (router interface) from the area.

©Avaya Inc. 2015 All Rights Reserved.

area range

Use aggregate area ranges to reduce the number of link-state advertisements that are required within the area. You can also control advertisements.

Syntax

- `area range {A.B.C.D} {A.B.C.D/X} { summary-link | nssa-extlink } advertise-metric <0-65535>`
- `area range {A.B.C.D} {A.B.C.D/X} { summary-link | nssa-extlink } advertise-mode { summarize | suppress | no-summarize }`
- `default area range {A.B.C.D} {A.B.C.D/X} { summary-link | nssa-extlink }`
- `default area range {A.B.C.D} {A.B.C.D/X} { summary-link | nssa-extlink } advertise-metric`
- `default area range {A.B.C.D} {A.B.C.D/X} { summary-link | nssa-extlink } advertise-mode`
- `no area range {A.B.C.D} {A.B.C.D/X} { summary-link | nssa-extlink }`

Default

None

Command mode

OSPF Router Configuration

Command parameters

Parameter	Description
<A.B.C.D> <A.B.C.D/X>	<A.B.C.D> identifies an OSPF area and <A.B.C.DX> is the IP address and subnet mask of the range, respectively.
<summary-link|nssa-extlink>	Specifies the LSA type. If you configure the range as type nssa-extlink then you cannot configure the advertise-metric.
advertise-metric <0-65535>	Changes the advertised metric cost of the OSPF area range.
advertise-mode <summarize|suppress|no-summarize>	Changes the advertisement mode of the range.

©Avaya Inc. 2015 All Rights Reserved.

area virtual-link

Use manual virtual interfaces to provide a backup link for vital OSPF traffic with a minimum of resource use.

Syntax

- `area virtual-link {A.B.C.D} {A.B.C.D}`
- `area virtual-link {A.B.C.D} {A.B.C.D} authentication-key WORD<0-8>`
- `area virtual-link {A.B.C.D} {A.B.C.D} authentication-type message-digest`
- `area virtual-link {A.B.C.D} {A.B.C.D} authentication-type none`
- `area virtual-link {A.B.C.D} {A.B.C.D} authentication-type simple`
- `area virtual-link {A.B.C.D} {A.B.C.D} dead-interval <0-2147483647>`
- `area virtual-link {A.B.C.D} {A.B.C.D} hello-interval <1-65535>`
- `area virtual-link {A.B.C.D} {A.B.C.D} primary-md5-key <1-255>`
- `area virtual-link {A.B.C.D} {A.B.C.D} retransmit-interval <0-3600>`
- `area virtual-link {A.B.C.D} {A.B.C.D} transit-delay <0-3600>`
- `default area virtual-link {A.B.C.D} {A.B.C.D}`
- `default area virtual-link {A.B.C.D} {A.B.C.D} authentication-type`
- `default area virtual-link {A.B.C.D} {A.B.C.D} dead-interval`
- `default area virtual-link {A.B.C.D} {A.B.C.D} hello-interval`
- `default area virtual-link {A.B.C.D} {A.B.C.D} primary-md5-key`
- `default area virtual-link {A.B.C.D} {A.B.C.D} retransmit-interval`
- `default area virtual-link {A.B.C.D} {A.B.C.D} transit-delay`
- `no area virtual-link {A.B.C.D} {A.B.C.D}`

Default

None

Command mode

OSPF Router Configuration

Command parameters

Parameter	Description
<A.B.C.D> <A.B.C.D>	Creates a virtual interface area identifier. <A.B.C.D> <A.B.C.D> specify the area ID and the virtual interface ID, respectively.

`authentication-key WORD<0-8>`	Configures the authentication key of up to eight characters.
`authentication-type <none|simple|message-digest>`	Configures the authentication type for the OSPF area. authentication-type is: none, simple password, or MD5 authentication. If simple, all OSPF updates received by the interface must contain the authentication key specified by the area authentication-key command. If MD5, they must contain the MD5 key. The default is none.
`dead-interval <0-2147483647>`	Configures the dead interval, in seconds, for the virtual interface, the number of seconds that a router Hello packets are not seen before its neighbors declare the router down. This value must be at least four times the Hello interval value. The default is 60.
`hello-interval <1-65535>`	Configures the Hello interval, in seconds, on the virtual interface for the length of time (in seconds) between the Hello packets that the router sends on the interface. The default is 10.
`primary-md5-key <1-255>`	Changes the primary key used to encrypt outgoing packets. <1-255> is the ID for the message digest key.
`retransmit-interval <0-3600>`	Configures the retransmit interval for the virtual interface, the number of seconds between link-state advertisement retransmissions. The range is from 0 to 3600.
`transit-delay <0-3600>`	Configures the transit delay for the virtual interface, the estimated number of seconds required to transmit a link-state update over the interface. The range is from 0 to 3600.

©Avaya Inc. 2015 All Rights Reserved.

area virtual-link message-digest-key

Configure a Message Digest 5 algorithm (MD5) key for the virtual interface.

Syntax

- `area virtual-link message-digest-key {A.B.C.D} {A.B.C.D} <1-255> md5-key WORD<1-16>`
- `default area virtual-link message-digest-key {A.B.C.D} {A.B.C.D} <1-255>`
- `no area virtual-link message-digest-key {A.B.C.D} {A.B.C.D} <1-255>`

Default

None

Command mode

OSPF Router Configuration

Command parameters

Parameter	Description
<A.B.C.D> <A.B.C.D> <1-255> md5-key WORD<0-16>	Adds a Message Digest 5 algorithm (MD5) key to the interface. At most, you can configure two MD5 keys to an interface. <A.B.C.D> identifies an OSPF area. <A.B.C.D> is the virtual interface id. <1-255> is the ID for the message digest key WORD<0-16> is an alphanumeric password in the range of 0 to 16 characters.

©Avaya Inc. 2015 All Rights Reserved.

as-boundary-router enable

Configure the router as an autonomous system boundary router (ASBR).

Syntax

- `as-boundary-router enable`
- `default as-boundary-router`
- `default as-boundary-router enable`
- `no as-boundary-router`
- `no as-boundary-router enable`

Default

`The default is disabled.`

Command mode

OSPF Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

attribute

Modifies MS-DOS file attributes.

Syntax

- `attribute WORD<1-99> WORD<1-1536>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
WORD<1-1536>	Sets or clears the read-only file attribute.
WORD<1-99>	Specifies the filename.

©Avaya Inc. 2015 All Rights Reserved.

auto-negotiate enable (on an Ethernet port)

Enable autonegotiation on the Ethernet port to optimally operate on the network.

Syntax

- `auto-negotiate`
- `auto-negotiate enable`
- `auto-negotiate port {slot/port[-slot/port][,...]}`
- `auto-negotiate port {slot/port[-slot/port][,...]} enable`
- `default auto-negotiate`
- `default auto-negotiate enable`
- `default auto-negotiate port {slot/port[-slot/port][,...]}`
- `default auto-negotiate port {slot/port[-slot/port][,...]} enable`
- `no auto-negotiate`
- `no auto-negotiate enable`
- `no auto-negotiate port {slot/port[-slot/port][,...]}`
- `no auto-negotiate port {slot/port[-slot/port][,...]} enable`

Default

`The default is true, enabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables or disables Autonegotiation for the port or other ports of the module or both. Note: The 10 Gigabit Ethernet fiber-based I/O module ports can operate at either 1 Gigabit per second (Gbps) or 10 Gbps, dependent upon the capabilities optical transceiver that you install. This presents an ambiguity with respect the autonegotiation settings of the port, while 1 Gigabit Ethernet (GbE) ports require autonegotiation; autonegotiation is not defined and is non-existent for 10 GbE ports. For a 10 GbE fiber-based I/O module, you have the capability to swap back-and-forth between 1 GbE and 10 GbE operation by simply swapping transceivers. To help with this transition between 1 GbE and 10 GbE port operation, Avaya allows you to configure autonegotiation when you install a 10 GbE transceiver, even though autonegotiation is not defined for 10GbE. You can do this in anticipation of a

	port changeover from 10 GbE to 1 GbE. In this manner, you could essentially preconfigure a port in 1 GbE mode while the 10G transceiver is still installed. The port is ready to go upon the changeover to the 1 GbE transceiver. In addition, you can use a saved configuration file with autonegotiation enabled to boot a system with either 10 GbE or 1 GbE transceivers installed. If you install a 1 GbE transceiver, the system applies autonegotiation. If you install a 10 GbE transceiver, the system does not remove the autonegotiation settings from the configuration, but the system simply ignores the configuration because autonegotiation settings are irrelevant to a 10 GbE transceiver. The system preserves the saved configuration for autonegotiation when resaved no matter which speed of transceiver you install.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

auto-negotiate (for the management port)

Configure auto-negotiation for the Ethernet management port.

Syntax

- `auto-negotiate [port {slot/port[-slot/port][,...]}] [enable]`
- `default auto-negotiate [port {slot/port[-slot/port][,...]}] [enable]`
- `no auto-negotiate [port {slot/port[-slot/port][,...]}] [enable]`

Default

`The default is enabled.`

Command mode

mgmtEthernet Interface Configuration

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port.

©Avaya Inc. 2015 All Rights Reserved.

auto-negotiation-advertisements

Configure autonegotiation advertisements after you enable autonegotiation.

Syntax

- `auto-negotiation-advertisements 1000-full`
- `auto-negotiation-advertisements 100-full`
- `auto-negotiation-advertisements 100-half`
- `auto-negotiation-advertisements 10-full`
- `auto-negotiation-advertisements 10-half`
- `auto-negotiation-advertisements none`
- `auto-negotiation-advertisements port {slot/port[-slot/port][,...]} 1000-full`
- `auto-negotiation-advertisements port {slot/port[-slot/port][,...]} 100-full`
- `auto-negotiation-advertisements port {slot/port[-slot/port][,...]} 100-half`
- `auto-negotiation-advertisements port {slot/port[-slot/port][,...]} 10-full`
- `auto-negotiation-advertisements port {slot/port[-slot/port][,...]} 10-half`
- `auto-negotiation-advertisements port {slot/port[-slot/port][,...]} none`
- `default auto-negotiation-advertisements`
- `default auto-negotiation-advertisements port {slot/port[-slot/port][,...]}`
- `no auto-negotiation-advertisements`
- `no auto-negotiation-advertisements port {slot/port[-slot/port][,...]}`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`1000-full`	Advertises 1000 Mbps full duplex.
`100-full`	Advertises 100 Mbps full duplex.
`100-half`	Advertises 100 Mbps half duplex.
`10-full`	Advertises 10 Mbps full duplex.
`10-half`	Advertises 10 Mbps half duplex.

none	Configures the value to none.
port {slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

auto-peer-restart enable

Enable the process that automatically restarts a connection to a BGP neighbor.

Syntax

- `auto-peer-restart enable`
- `default auto-peer-restart`
- `default auto-peer-restart enable`
- `no auto-peer-restart`
- `no auto-peer-restart enable`

Default

`The default value is enable.`

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
`enable`	Enables the process that automatically restarts a connection to a BGP neighbor.

©Avaya Inc. 2015 All Rights Reserved.

auto-recover-delay

Set the time delay for the automatic recovery of ports.

Syntax

- `auto-recover-delay <5-3600>`
- `default auto-recover-delay <5-3600>`
- `no auto-recover-delay <5-3600>`

Default

The default is 30.

Command mode

Global Configuration

Command parameters

Parameter	Description
<5-3600>	Specifies the range to be set for the auto-recovery of ports in seconds. The range varies between 5 to 3600 seconds.

©Avaya Inc. 2015 All Rights Reserved.

auto-recover-port

Enable or disable autorecovery on a port.

Syntax

- `auto-recover-port`
- `auto-recover-port enable`
- `auto-recover-port port {slot/port[-slot/port][,...]}`
- `auto-recover-port port {slot/port[-slot/port][,...]} enable`
- `default auto-recover-port`
- `default auto-recover-port enable`
- `default auto-recover-port port {slot/port[-slot/port][,...]}`
- `default auto-recover-port port {slot/port[-slot/port][,...]} enable`
- `no auto-recover-port`
- `no auto-recover-port enable`
- `no auto-recover-port port {slot/port[-slot/port][,...]}`
- `no auto-recover-port port {slot/port[-slot/port][,...]} enable`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables spoof detection on the port.
`port {slot/port [-slot/port][,...]}`	Specifies the port list.

©Avaya Inc. 2015 All Rights Reserved.

auto-summary

Summarize the networks based on class limits after BGP is enabled. (For example, Class A, B, C networks).

Syntax

- `auto-summary`
- `default auto-summary`
- `no auto-summary`

Default

`The default value is enable.`

Command mode

BGP Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

autotopology

Configure the SynOptics Network Management Protocol (SONMP) to allow a network management station (NMS) formulate a map that shows the interconnections between Layer 2 devices in a network.

Syntax

- `autotopology`
- `default autotopology`
- `no autotopology`

Default

`The default status is enabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

auto-vlink

Use automatic virtual links to provide an automatic, dynamic backup link for vital OSPF traffic. Automatic virtual links require more system resources than manually configured virtual links.

Syntax

- `auto-vlink`
- `default auto-vlink`
- `no auto-vlink`

Default

None

Command mode

OSPF Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

backup

Use this command to backup all files, including the directory, of the internal flash or external flash to the USB flash. Important: You must disable logging to the compact flash you want to restore before you can use the backup. The system verifies that the USB flash device has enough available space to perform the backup operation. If the USB flash device does not have enough available space, an error message appears. The backup command uses the following filepath on the USB flash device: /usb/intflash/intflashbackup_yyyymmddhhmmss.tgz or /usb/extflash/extflashbackup_yyyymmddhhmmss.tgz

Syntax

- `backup extflash`
- `backup intflash`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
extflash	Copies all files from the CP module external flash to the USB drive at /usb/extflash. If the external flash is used for logging, the system automatically disables logging to the external flash.
intflash	Copies all files from the CP module internal flash to the USB drive at /usb/intflash. This command causes the system to verify that an empty 4 GB USB flash device is in the CP module. If the internal flash is used for logging, the system automatically enables logging to the external flash, if one exists, or disables logging.

©Avaya Inc. 2015 All Rights Reserved.

bad-lsa-ignore enable

Configures the switch to accept bad LSAs, for example, with a hole in the mask. If you use the no operator with this command, the switch ignores bad LSAs.

Syntax

- `bad-lsa-ignore enable`
- `default bad-lsa-ignore`
- `default bad-lsa-ignore enable`
- `no bad-lsa-ignore`
- `no bad-lsa-ignore enable`

Default

`The default is disabled.`

Command mode

OSPF Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

banner

Configure the ACLI logon banner to display a warning message to users before authentication.

Syntax

- banner custom
- banner displaymotd
- banner motd WORD<1-1516>
- banner static
- banner WORD<1-80>
- default banner
- default banner displaymotd
- default banner motd
- no banner
- no banner displaymotd
- no banner motd

Default

The default configuration uses the default banner with no message of the day.

Command mode

Global Configuration

Command parameters

Parameter	Description
custom	Activates the custom banner.
displaymotd	Activates or disables the message of the day.
motd WORD<1-1516>	Creates a message of the day to display with the logon banner. To provide a string with spaces, include the text in quotation marks ("").
static	Activates static banner.
WORD<1-80>	Adds lines of text to the ACLI logon banner.

©Avaya Inc. 2015 All Rights Reserved.

bgp aggregation

Enables or disables the aggregation feature on the interface.

Syntax

- `bgp aggregation`
- `bgp aggregation enable`
- `default bgp aggregation`
- `default bgp aggregation enable`
- `no bgp aggregation`
- `no bgp aggregation enable`

Default

`The default value is enable.`

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
`enable`	Enables the aggregation feature on the interface.

©Avaya Inc. 2015 All Rights Reserved.

bgp always-compare-med

Enables the comparison of the multiexit discriminator (MED) parameter for paths from neighbors in different autonomous systems. A path with a lower MED is preferred over a path with a higher MED.

Syntax

- `bgp always-compare-med`
- `default bgp always-compare-med`
- `no bgp always-compare-med`

Default

`The default value is disable.`

Command mode

BGP Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

bgp client-to-client reflection

Enables or disables route reflection between two route reflector clients. This option is applicable only if the route reflection value is set to enable.

Syntax

- `bgp client-to-client reflection`
- `default bgp client-to-client reflection`
- `no bgp client-to-client reflection`

Default

`The default value is enable.`

Command mode

BGP Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

bgp cluster-id

Configures a cluster ID. This option applies only if the route reflection value is set to enable, and if multiple route reflectors are in a cluster.

Syntax

- `bgp cluster-id {A.B.C.D}`
- `no bgp cluster-id {A.B.C.D}`

Default

None

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
<A.B.C.D>	Specifies the cluster ID of the reflector router.

©Avaya Inc. 2015 All Rights Reserved.

bgp confederation

Configures a BGP confederation.

Syntax

- `bgp confederation identifier <0-65535>`
- `bgp confederation peers WORD<0-255>`
- `default bgp confederation`
- `default bgp confederation identifier`
- `default bgp confederation peers`
- `no bgp confederation`
- `no bgp confederation identifier`
- `no bgp confederation peers`

Default

`The default value is 0.`

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
`peers WORD <0-255>`	Lists adjoining ASs that are part of the confederation in the format (5500,65535,0,10,...,...).
`identifier <0-65535>`	Specifies the confederation identifier.

©Avaya Inc. 2015 All Rights Reserved.

bgp default local-preference<0-2147483647>

Specifies the default value of the local preference attribute. You cannot change the default value when BGP is enabled.

Syntax

- `bgp default local-preference <0-2147483647>`
- `default bgp default local-preference`
- `no bgp default local-preference`
- `no bgp default local-preference <0-2147483647>`

Default

`The default value is 100.`

Command mode

BGP Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

bgp deterministic-med enable

Enables deterministic Multiexit Discriminator (MED).

Syntax

- `bgp deterministic-med enable`
- `default bgp deterministic-med`
- `default bgp deterministic-med enable`
- `no bgp deterministic-med`
- `no bgp deterministic-med enable`

Default

`The default value is enable.`

Command mode

BGP Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

bgp multiple-paths <1-8>

Configures the maximum number of equal-cost-paths that are available to a BGP router by limiting the number of equal-cost-paths that can be stored in the routing table.

Syntax

- `bgp multiple-paths <1-8>`
- `default bgp multiple-paths`

Default

`The default value is 1.`

Command mode

BGP Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

boot

Restart the switch to implement configuration changes or recover from a system failure. When you restart the system, you can specify an optional configuration file to use to load the device. If no config file is specified, the run-time ACLI uses the configuration file specified by the boot config choice command. The image booted is that specified by the software activate command.

Syntax

- `boot`
- `boot config WORD<1-99>`
- `boot -y`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`config WORD<1-99>`	Specifies the software configuration device and file name in one of the following formats:/intflash/<file>/extflash/<file> /usb/<file> The filename, including the directory structure, can include up to 99 characters.
`-y`	Suppresses the confirmation message before the switch restarts. If you omit this parameter, you must confirm the action before the switch restarts.

©Avaya Inc. 2015 All Rights Reserved.

boot config choice

Change the boot source order to change the order in which the system accesses the configuration files. If you change the primary source, the system uses your configuration first, and then accesses the default locations. If the default locations do not contain a configuration or backup configuration file, the system loads the default configuration.

Syntax

- `boot config choice primary backup-config-file WORD<0-255>`
- `boot config choice primary config-file WORD<0-255>`
- `default boot config choice primary`
- `default boot config choice primary backup-config-file`
- `default boot config choice primary config-file`

Default

`By default, the primary source is the internal flash.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`{backup-config-file|config-file}`	Specifies that the boot source uses either the configuration file or a backup configuration file.
`WORD<0-255>`	Identifies the configuration file. WORD<0-255> is the device and file name, up to 255 characters including the path, in one of the following formats: a.b.c.d:<file>, /intflash/<file>, /extflash/<file>, and /usb/<file>.

©Avaya Inc. 2015 All Rights Reserved.

boot config delay

Configure the standby-to-master delay to set the number of seconds a standby CPU waits before trying to become the master CPU. The time delay you configure applies during a cold start. It does not apply to a failover start.

Syntax

- `boot config delay <0-255>`
- `default boot config delay`

Default

`The default value is 10.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<0-255>`	Specifies the number of seconds a standby CPU waits before trying to become the master CPU.

©Avaya Inc. 2015 All Rights Reserved.

boot config flags block-snmp

Activate or disable Simple Network Management Protocol (SNMP) management.

Syntax

- `boot config flags block-snmp`
- `default boot config flags block-snmp`
- `no boot config flags block-snmp`

Default

`The default is disabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

boot config flags debug-config

Activate or disable run-time debugging of the configuration file. After you enable debug-config and save the configuration, the debug output either displays on the console or logs to an output file the next time the switch reboots. You do not have to restart the switch after you enable debug-config, unless you want to immediately debug the configuration.

Syntax

- `boot config flags debug-config`
- `boot config flags debug-config console`
- `boot config flags debug-config file`
- `default boot config flags debug-config`
- `no boot config flags debug-config`

Default

`The default is disabled.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`console`	Displays the lineby-line configuration file processing and result of the execution on the console while the device loads the configuration file.
`file`	Logs the line-by-line configuration file processing and result of the execution to the debug file while the device loads the configuration file. The system logs the debug-config output to the /extflash/debugconfig_primary.txt for the primary configuration file. The system logs the debug config output to the /extflash/debugconfig_backup.txt for the backup configuration, if the backup configuration file loads.

©Avaya Inc. 2015 All Rights Reserved.

boot config flags debugmode

Control whether the switch stops in debug mode following a fatal error. Debug mode provides information equivalent to the trace commands. If you enable this flag, the switch does not restart following a fatal error. If you change this flag, you must restart the switch. Do not change this flag unless directed by Avaya.

Syntax

- `boot config flags debugmode`
- `default boot config flags debugmode`
- `no boot config flags debugmode`

Default

`The default is disabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

boot config flags fabric-profile

Configure the system to give preference to one type of traffic over the other in times of over subscription.

Syntax

- `boot config flags fabric-profile <1-3>`
- `default boot config flags fabric-profile`

Default

`The default is 1, balanced.`

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-3>	Specifies the value as one of the following: 1- balanced, 2-unicast optimized, and 3-multicast optimized.

©Avaya Inc. 2015 All Rights Reserved.

boot config flags factorydefaults

Specify whether the switch uses the factory default settings at startup. This flag automatically resets to the default setting after the CPU restarts. If you change this flag you must restart the switch.

Syntax

- `boot config flags factorydefaults`
- `no boot config flags factorydefaults`

Default

`The default is disabled.`

Command mode

Global Configuration

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

boot config flags ftpd

Activate or disable the FTP server on the switch. To enable FTP, ensure that the tftpd flag is disabled.

Syntax

- `boot config flags ftpd`
- `default boot config flags ftpd`
- `no boot config flags ftpd`

Default

`The default is disabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

boot config flags ha-cpu

Activate or disable High Availability (HA) mode. Switches with two CPUs use HA mode to recover quickly from a failure of one of the CPUs. If you enable High Availability mode, the secondary CPU resets to load settings from the saved configuration file. You must reset the master CPU after the secondary CPU starting is complete. CAUTION: Enabling HA mode can disable certain features.

Syntax

- `boot config flags ha-cpu`
- `default boot config flags ha-cpu`
- `no boot config flags ha-cpu`

Default

`The default is disabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

boot config flags hsecure

Activate or disable High Secure mode. The hsecure command provides the following password behavior: 10 character enforcement, aging time, failed login attempt limitation, and designated IP address filtration. If you enable High Secure mode, you must restart the switch to enforce secure passwords. If you operate the switch in High Secure mode, the switch prompts a password change if you enter invalid-length passwords.

Syntax

- `boot config flags hsecure`
- `default boot config flags hsecure`
- `no boot config flags hsecure`

Default

`The default is disabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

boot config flags logging

If an external flash device exists in the system, you can use the logging command to activate or disable system logging to a file on the external flash. The system names log files according to the following: - File names appear in 8.3 (xxxxxxxx.sss) format. - The first 6 characters of the file name contain the last three bytes of the chassis base MAC address. - The next two characters in the file name specify the slot number of the CPU that generated the logs. - The last three characters in the file name are the sequence number of the log file. The system generates multiple sequence numbers for the same chassis and same slot if: - You replace the CPU. - You reinsert the CPU. - The system reaches the maximum log file size.

Syntax

- `boot config flags logging`
- `default boot config flags logging`
- `no boot config flags logging`

Default

`The default is enabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

boot config flags reboot

Activate or disable automatic reboot on a fatal error. The reboot command is equivalent to the debugmode command. If you change the reboot value, you must restart the switch. Do not change this parameter unless directed by Avaya.

Syntax

- `boot config flags reboot`
- `default boot config flags reboot`
- `no boot config flags reboot`

Default

`The default is enabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

boot config flags rlogind

Activate or disable the remote login (rlogin) and remote shell (rsh) server.

Syntax

- `boot config flags rlogind`
- `default boot config flags rlogind`
- `no boot config flags rlogind`

Default

`The default is disabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

boot config flags savetostandby

Activate or disable automatic save of the configuration file to the standby CPU. If you operate a dual CPU system, Avaya recommends that you enable this flag for ease of operation.

Syntax

- `boot config flags savetostandby`
- `default boot config flags savetostandby`
- `no boot config flags savetostandby`

Default

`The default is disabled.`

Command mode

Global Configuration

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

boot config flags spanning-tree-mode

Specify the Multiple Spanning Tree Protocol (MSTP) or Rapid Spanning Tree Protocol (RSTP) mode. If you do not specify a protocol, the switch uses the default mode. If you change the spanning tree mode, you must save the current configuration and restart the switch.

Syntax

- `boot config flags spanning-tree-mode mstp`
- `boot config flags spanning-tree-mode rstp`
- `default boot config flags spanning-tree-mode`
- `no boot config flags spanning-tree-mode`

Default

`The default is MSTP.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

boot config flags sshd

Activate or disable the Secure Shell (SSH) server service.

Syntax

- `boot config flags sshd`
- `default boot config flags sshd`
- `no boot config flags sshd`

Default

`The default is disabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

boot config flags telnetd

Activate or disable the Telnet server service. If you disable the Telnet server service in a dual CPU system, the Telnet server prevents a Telnet connection initiated from the other CPU.

Syntax

- `boot config flags telnetd`
- `default boot config flags telnetd`
- `no boot config flags telnetd`

Default

`The default is disabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

boot config flags tftpd

Activate or disable Trivial File Transfer Protocol (TFTP) server service. If you disable the TFTP server you can still copy files between the CPUs.

Syntax

- `boot config flags tftpd`
- `default boot config flags tftpd`
- `no boot config flags tftpd`

Default

`The default is disabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

boot config flags trace-logging

Activate or disable the creation of trace logs. Do not change this parameter unless directed by Avaya.

Syntax

- `boot config flags trace-logging`
- `default boot config flags trace-logging`
- `no boot config flags trace-logging`

Default

`The default is disabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

boot config flags verify-config

Activates syntax checking of the configuration file. When you enable the verify-config flag, the primary configuration file is pre-checked for syntax errors. If the system finds an error, the system loads the backup configuration file. If you disable the verify-config flag, the system ignores any lines with errors during loading of the primary configuration file. If the primary configuration file is not present or cannot be found, the system tries to load the backup file. The system does not check the backup file for syntax errors. The system ignores any lines with errors during the loading of the backup configuration file. If no backup file exists, the system defaults to factory defaults.

Syntax

- `boot config flags verify-config`
- `default boot config flags verify-config`
- `no boot config flags verify-config`

Default

`The default is enabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

boot config host

Configure the remote host logon to modify parameters for FTP and TFTP access. Use the default parameters for TFTP transfers. If you want to use FTP as transfer mechanism, you must change the password to a valid value.

Syntax

- `boot config host ftp-debug`
- `boot config host password WORD<0-16>`
- `boot config host tftp-debug`
- `boot config host tftp-hash`
- `boot config host tftp-rexmit <1-120>`
- `boot config host tftp-timeout <1-120>`
- `boot config host user WORD<0-16>`
- `default boot config host ftp-debug`
- `default boot config host tftp-debug`
- `default boot config host tftp-hash`
- `default boot config host tftp-rexmit`
- `default boot config host tftp-timeout`
- `default boot config host user`
- `no boot config host ftp-debug`
- `no boot config host tftp-debug`
- `no boot config host tftp-hash`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`ftp-debug`	Enables or disables the debug mode on FTP. If you enable the debug mode, debug messages appear on the management console screen. The default is disabled.
`password`	Configures the password to enable FTP transfers. WORD<0-16> is the password, up to 16 characters. After you configure this password, you can use only FTP for remote host logon. Important: This password must match the password for the FTP server, or the FTP

WORD<0-16>	operation fails. Also, if you configure the password to a valid value, then all copying to and from the network uses FTP instead of TFTP. If the user name or password is incorrect, copying over the network fails.
tftp-debug	Enables or disables debug mode on TFTP or TFTPD. If you enable the debug mode, debug messages appear on the management console screen. The default is disabled.
tftp-hash	Enables or disables the TFTP hash bucket display. The default is disabled.
tftp-rexmit <1-120>	Configures the TFTP retransmission timeout in seconds. The default is 2.
tftp-timeout <1-120>	Configures the TFTP timeout in seconds. The default is 6.
user WORD<0-16>	Configures the remote user logon. WORD<0-16> is the user logon name (up to 16 characters). The default is target.

©Avaya Inc. 2015 All Rights Reserved.

boot config linecard-compatibility-mode

Configure the minimum generation of modules the Virtual Services Platform 9000 supports. Both Virtual Services Platform 9010 and Virtual Services Platform 9012 support first and second generation modules.

Syntax

- `boot config linecard-compatibility-mode gen1`
- `boot config linecard-compatibility-mode gen2`
- `default boot config linecard-compatibility-mode`

Default

`gen1`

Command mode

Global Configuration

Command parameters

Parameter	Description
gen1	Specifies VSP 9000 supports both first and second generation modules.
gen2	Specifies VSP 9000 only supports second generation modules. After reboot in second generation mode, the system disables all first generation modules, and provides full fastpath routing for one million routes.

©Avaya Inc. 2015 All Rights Reserved.

boot config logfile

Configure logfile parameters. The log file is named using an 8.3 (xxxxxxxx.sss) format. The first six characters of the file name contain the last three bytes of the chassis base MAC address. The next two characters specify the slot number of the CP module that generated the logs. The last three characters denote the sequence number of the log file. Multiple sequence numbers are generated for the same chassis and same slot, if you replace or reinsert the CP module, or if the maximum log file size is reached.

Syntax

- `boot config logfile <64-500> <500-16384> <10-90>`
- `default boot config logfile`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<10-90>	Specifies the maximum percentage, from 10-90%, of space on the external storage device the log file can use. Virtual Services Platform 9000 does not support this parameter.
<500-16384>	Specifies the maximum size of the log file from 500-16384 KB.
<64-500>	Specifies the minimum free memory space on the external storage device from 64- 500 KB. Virtual Services Platform 9000 does not support this parameter.

©Avaya Inc. 2015 All Rights Reserved.

boot config master

Specify the primary CPU to determine which CPU you use as the master after the switch performs a full power cycle. After the CPU becomes the primary, the master LED for the CPU is on.

Syntax

- `boot config master <1-2>`

Default

`The default is slot 1.`

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-2>	Specifies the slot number for the master CPU. This variable can be 1 or 2. The default is slot 1.

©Avaya Inc. 2015 All Rights Reserved.

boot config multicast

Configures system multicast scaling.

Syntax

- `boot config multicast <0-2147483647>`
- `default boot config multicast`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<0-2147483647>	Specifies the scaling value.

©Avaya Inc. 2015 All Rights Reserved.

boot config sio console

Configure the serial port devices to define connection settings for the console port.

Syntax

- `boot config sio { console } 8databits`
- `boot config sio { console } baud <9600 - 115200>`
- `default boot config sio { console } 8databits`
- `default boot config sio { console } baud`
- `no boot config sio console 8databits`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`<9600-115200>`	Configures the baud rate for the port. The default baud rate is 9600.
`8databits`	Specifies either 8 (activated) or 7 (disabled) data bits for each byte for the software to interpret. The default is 8.

©Avaya Inc. 2015 All Rights Reserved.

brouter

Configure a port as a brouter port.

Syntax

- `brouter port {slot/port} vlan <2-4084> subnet {A.B.C.D/X}`
- `brouter port {slot/port} vlan <2-4084> subnet {A.B.C.D/X} mac-offset <0-65535>`
- `brouter port {slot/port} vlan <2-4084> subnet {A.B.C.D} {A.B.C.D}`
- `brouter vlan <2-4084> subnet {A.B.C.D/X}`
- `brouter vlan <2-4084> subnet {A.B.C.D/X} mac-offset <0-65535>`
- `brouter vlan <2-4084> subnet {A.B.C.D} {A.B.C.D}`
- `no brouter`
- `no brouter port {slot/port}`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`mac-offset <0-65535>`	Specifies the Mac-offset value.
`port {slot/port}`	Specifies the slot and port.
`subnet <{A.B.C.D/X}|{A.B.C.D}>`	Assigns an IP address and mask for the management port.
`vlan <2-4084>`	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

cd

Changes the current filesystem directory path.

Syntax

- `cd WORD<1-99>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
WORD<1-99>	Specifies the directory name.

©Avaya Inc. 2015 All Rights Reserved.

cfm cmac enable

Enables CFM for C-VLANs, which creates the MD, MA, and MEP, and then associate the MEP and MIP level to C-VLANs.

Syntax

- `cfm cmac enable`
- `no cfm cmac enable`

Default

`The default is disabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

cfm cmac level <0-7>

Configures the maintenance level for the MEP and MIP associated with C-VLANs.

Syntax

- `cfm cmac level <0-7>`
- `default cfm cmac level`

Default

`The default is 4.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

cfm cmac mepid <1-8191>

Assigns a global MEP ID for all CFM CMAC MEPs.

Syntax

- `cfm cmac mepid <1-8191>`
- `default cfm cmac mepid`

Default

`The default is 1.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

cfm maintenance-association

Create the Connectivity Fault Management (CFM) Maintenance-Association (MA).

Syntax

- `cfm maintenance-association WORD<1-22> WORD<1-22>`
- `cfm maintenance-association WORD<1-22> WORD<1-22> index <1-2147483647>`
- `no cfm maintenance-association WORD<1-22> WORD<1-22>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`index <1-2147483647>`	Specifies a Maintenance-Association (MA) entry index.
`WORD<1-22> WORD<1-22>`	Creates the Connectivity Fault Management (CFM) Maintenance-Association (MA). The first parameter, specifies the Maintenance-Domain (MD) name. The second parameter, specifies the MA name. The default is disabled.

©Avaya Inc. 2015 All Rights Reserved.

cfm maintenance-domain

Create the Connectivity Fault Management (CFM) Maintenance-Domain (MD).

Syntax

- `cfm maintenance-domain WORD<1-22>`
- `cfm maintenance-domain WORD<1-22> index <1-2147483647>`
- `cfm maintenance-domain WORD<1-22> index <1-2147483647> maintenance-level <0-7>`
- `cfm maintenance-domain WORD<1-22> level <0-7>`
- `cfm maintenance-domain WORD<1-22> maintenance-level <0-7>`
- `cfm maintenance-domain WORD<1-22> maintenance-level <0-7> index <1-2147483647>`
- `no cfm maintenance-domain WORD<1-22>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`index <1-2147483647>`	Specifies a Maintenance-Domain (MD) entry index.
`level <0-7>`	Specifies the Maintenance-Domain (MD) level for an existing Maintenance-Domain (MD).
`maintenance-level <0-7>`	Specifies the Maintenance-Domain (MD) maintenance level when creating the Maintenance-Domain (MD).
`WORD<1-22>`	Specifies the Maintenance-Domain (MD) name.

©Avaya Inc. 2015 All Rights Reserved.

cfm maintenance-endpoint

Create the Connectivity Fault Management (CFM) Maintenance-Endpoint (MEP).

Syntax

- `cfm maintenance-endpoint WORD<1-22> WORD<1-22> <1-8191>`
- `cfm maintenance-endpoint WORD<1-22> WORD<1-22> <1-8191> enable`
- `cfm maintenance-endpoint WORD<1-22> WORD<1-22> <1-8191> state enable`
- `no cfm maintenance-endpoint WORD<1-22> WORD<1-22> <1-8191>`
- `no cfm maintenance-endpoint WORD<1-22> WORD<1-22> <1-8191> enable`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`<1-8191>`	Specifies the Maintenance Endpoint (MEP) ID.
`enable`	Enables an existing Maintenance Endpoint (MEP). Use this parameter with the no option to disable an existing MEP.
`state enable`	Enables the Maintenance Endpoint (MEP) when creating the MEP. Use the no option to disable the Maintenance Endpoint.
`WORD<1-22> WORD<1-22>`	The first parameter, specifies the Maintenance-Domain (MD) name. The second parameter, specifies the Maintenance-Association name.

©Avaya Inc. 2015 All Rights Reserved.

cfm spbm enable

Enables CFM for B-VLANs, which creates the MD, MA, and MEP, and then associate the MEP and MIP level to B-VLANs.

Syntax

- `cfm spbm enable`
- `no cfm spbm enable`

Default

`The default is disabled.`

Command mode

Global Configuration

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

cfm spbm level <0-7>

Configures the maintenance level for every CFM SPBM MEP and MIP level on all SPBM VLANs.

Syntax

- `cfm spbm level <0-7>`
- `default cfm spbm level`

Default

`The default is 4.`

Command mode

Global Configuration

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

cfm spbm mepid <1-8191>

Assigns a global MEP ID for all CFM SPBM MEPs.

Syntax

- `cfm spbm mepid <1-8191>`
- `default cfm spbm mepid`

Default

`The default is 1.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

clear alarm

Clear the alarm database to remove old information after a condition is resolved or to reset statistics.

Syntax

- `clear alarm database`
- `clear alarm database alarm-id WORD<0-100>`
- `clear alarm statistics`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`database`	Clears the alarm database.
`statistics`	Clears the alarm database statistics.
`WORD<0-100>`	Specifies an alarm ID to clear.

©Avaya Inc. 2015 All Rights Reserved.

clear filter acl

Clear Access Control List (ACL) statistics if you no longer require previous statistics or log information.

Syntax

- `clear filter acl log`
- `clear filter acl statistics <1-2048>`
- `clear filter acl statistics <1-2048> <1-2000>`
- `clear filter acl statistics <1-2048> qos`
- `clear filter acl statistics <1-2048> security`
- `clear filter acl statistics all`
- `clear filter acl statistics default`
- `clear filter acl statistics default <1-2048>`
- `clear filter acl statistics global`
- `clear filter acl statistics global <1-2048>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`[<1-2048>]`	Specifies the ACL identifier.
`<1-2000>`	Specifies the ACE identifier.
`all`	Clears all statistics for all access control entries.
`default <1-2048>`	Clears traffic statistics for an access control entry (ACE).
`global <1-2048>`	Clears global statistics for an access control entry (ACE).
`qos`	Clears access control list (ACL) statistics for QoS access control entries (ACEs).
`security`	Clears access control list (ACL) statistics for Security ACEs.

©Avaya Inc. 2015 All Rights Reserved.

clear ip arp interface

Clear the ARP timers.

Syntax

- `clear ip arp interface gigabitethernet {slot/port[-slot/port][,...]}`
- `clear ip arp interface vlan <1-4084>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-4084>`	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

clear ip dhcp-relay

Clears the DHCP Relay counters.

Syntax

- `clear ip dhcp-relay counters`
- `clear ip dhcp-relay counters interface gigabitethernet {slot/port[-slot/port][,...]}`
- `clear ip dhcp-relay counters interface vlan <1-4084>`
- `clear ip dhcp-relay counters vrf WORD<1-16>`
- `clear ip dhcp-relay counters vrfid <0-511>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`interface gigabitethernet {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`vlan <1-4084>`	Specifies the VLAN ID.
`vrf WORD<1-16>`	Specifies a VRF name.
`vrfid <0-511>`	Specifies a VRF ID.

©Avaya Inc. 2015 All Rights Reserved.

clear ip ipfix hash-stats

Clear Internet Protocol Flow Information eXport (IPFIX) statistics to remove the hash statistics. The command is not supported for second generation Input/Output (I/O) modules.

Syntax

- `clear ip ipfix hash-stats`
- `clear ip ipfix hash-stats {slot[-slot][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot[-slot][,...]}`	Identifies the slot in one of the following formats: a single slot (3), a range of slots (3-4), or a series of slots (3,5,6). If you do not specify a slot, you clear the statistics for all slots. Valid slots are 3-12.

©Avaya Inc. 2015 All Rights Reserved.

clear ip ipfix stats

Clear Internet Protocol Flow Information eXport (IPFIX) statistics to remove the exporter statistics.

Syntax

- `clear ip ipfix stats`
- `clear ip ipfix stats {slot[-slot][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot[-slot][,...]}`	Identifies the slot in one of the following formats: a single slot (3), a range of slots (3-4), or a series of slots (3,5,6). If you do not specify a slot, you clear the statistics for all slots. Valid slots are 3-12.

©Avaya Inc. 2015 All Rights Reserved.

clear ip mroute stats

Clear multicast routing process statistics.

Syntax

- `clear ip mroute stats`

Default

None

Command mode

Privileged EXEC

©Avaya Inc. 2015 All Rights Reserved.

clear ip route

Clear the routing table.

Syntax

- `clear ip route gigabitethernet {slot/port}`
- `clear ip route vlan <1-4084>`

Default

None

Command mode

Privileged EXEC

©Avaya Inc. 2015 All Rights Reserved.

clear ipv6 dcache

Clear the destination cache.

Syntax

- `clear ipv6 dcache`
- `clear ipv6 dcache gigabitethernet {slot/port}`
- `clear ipv6 dcache mgmtethernet {slot/port}`
- `clear ipv6 dcache tunnel <1-2000>`
- `clear ipv6 dcache vlan <1-4084>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`gigabitethernet {slot/port}`	Identifies the slot and port.
`mgmtethernet {slot/port}`	Identifies the slot and port for the management interface. The slot can be either slot 1 or slot 2.
`tunnel <1-2000>`	Specifies the tunnel ID.
`vlan <1-4084>`	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

clear ipv6 neighbor-cache

Clear the neighbor cache.

Syntax

- `clear ipv6 neighbor-cache`
- `clear ipv6 neighbor-cache gigabitEthernet <slot/port>`
- `clear ipv6 neighbor-cache mgmtethernet <slot/port>`
- `clear ipv6 neighbor-cache vlan <1-4084>`

Default

`The default is disabled.`

Command mode

Privileged EXEC

©Avaya Inc. 2015 All Rights Reserved.

clear ipv6 route static

Clear IPv6 static routes.

Syntax

- `clear ipv6 route static`

Default

None

Command mode

Privileged EXEC

©Avaya Inc. 2015 All Rights Reserved.

clear ipv6 statistics

Use this command to clear IPv6 statistics.

Syntax

- `clear ipv6 statistics all`
- `clear ipv6 statistics interface`
- `clear ipv6 statistics interface general`
- `clear ipv6 statistics interface general gigabitethernet {slot/port}`
- `clear ipv6 statistics interface general mgmtethernet {slot/port}`
- `clear ipv6 statistics interface general tunnel <1-2000>`
- `clear ipv6 statistics interface general vlan <1-4084>`
- `clear ipv6 statistics interface icmp`
- `clear ipv6 statistics tcp`
- `clear ipv6 statistics udp`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`all`	Clears all statistics.
`general`	Clears general statistics.
`gigabitEthernet{slot/port}`	Clears statistics for a brouter interface.
`icmp`	Clears Internet Control Message Protocol (ICMP) statistics.
`mgmtethernet{slot/port}`	Clears statistics for a management port.
`tcp`	Clears TCP statistics.
`tunnel <1-2000>`	Clears statistics for a tunnel.
`udp`	Clears UDP statistics.
`vlan <1-4084>`	Clears statistics for a tunnel.

©Avaya Inc. 2015 All Rights Reserved.

clear ipv6 vrrp

Clears the IPv6 VRRP configuration.

Syntax

- `clear ipv6 vrrp gigabitethernet {slot/port[-slot/port][,...]} vrid <1-255>`
- `clear ipv6 vrrp vlan <1-4084> vrid <1-255>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`gigabitethernet {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`vlan <1-4084>`	Specifies the VLAN ID.
`vrid <1-255>`	Specifies the ID of the virtual router.

©Avaya Inc. 2015 All Rights Reserved.

clear ip vrrp

Clear the Virtual Router Redundancy Protocol (VRRP) configuration.

Syntax

- `clear ip vrrp gigabitethernet {slot/port[-slot/port][,...]} vrid <1-255>`
- `clear ip vrrp vlan <1-4084> vrid <1-255>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-255>`	Specifies the ID of the virtual router.
`<1-4084>`	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

clear isis lsdb

Clear the Intermediate-System-to-Intermediate-System (IS-IS) Link State Database (LSDB). The command clears learned Link State Packets (LSPs) only. The command does not clear local generated LSPs. As soon as the platform clears the LSDB the LSP synchronization process starts immediately and the LSDB synchronizes with its neighbors.

Syntax

- `clear isis lsdb`

Default

None

Command mode

Privileged EXEC

©Avaya Inc. 2015 All Rights Reserved.

clear isis spbm drop-stats

Clears packet drop statistics.

Syntax

- `clear isis spbm drop-stats`
- `clear isis spbm drop-stats {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

clear isis stats

Clear Intermediate-System-to-Intermediate-System (IS-IS) statistics.

Syntax

- `clear isis stats`
- `clear isis stats error-counters`
- `clear isis stats packet-counters`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`error-counters`	Clears the IS-IS stats error-counters.
`packet-counters`	Clears the IS-IS stats packet-counters.

©Avaya Inc. 2015 All Rights Reserved.

clear khi

Clear the forwarding health and CPP statistics information.

Syntax

- `clear khi cpp iocop-statistics`
- `clear khi cpp port-statistics`
- `clear khi cpp protocol-drops`
- `clear khi forwarding`
- `clear khi forwarding slot <3-12>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`cpp iocop-statistics`	Clears statistics for packets generated by the interface modules and sent to the control processor.
`cpp port-statistics`	Clears statistics for control packets that go to the control processor.
`cpp protocol-drops`	Clears information about packets dropped due to CP Limit violations.
`slot <3-12>`	Clears the forwarding health information for a particular interface module.

©Avaya Inc. 2015 All Rights Reserved.

clear lacp

Clear link aggregation information and statistics.

Syntax

- `clear lacp link-aggregate <1-512>`
- `clear lacp stats`
- `clear lacp stats port {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-512>`	Specifies the MLT ID.

©Avaya Inc. 2015 All Rights Reserved.

clear logging

Clear the log file.

Syntax

- `clear logging`

Default

None

Command mode

Privileged EXEC

©Avaya Inc. 2015 All Rights Reserved.

clear mac-address-table

Clear the entries in the MAC address table.

Syntax

- `clear mac-address-table port {slot/port[-slot/port][,...]} address WORD<17-17>`
- `clear mac-address-table port {slot/port[-slot/port][,...]} address WORD<17-17> interface vlan <1-4084>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`interface vlan <1-4084>`	Specifies the VLAN ID.
`WORD<17-17>`	Specifies the MAC address.

©Avaya Inc. 2015 All Rights Reserved.

clear mac-address-table dynamic

Clear the dynamic entries in the MAC address table.

Syntax

- `clear mac-address-table dynamic 0x00:0x00:0x00:0x00:0x00:0x00 <1-4084>`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
<1-4084>	Specifies a VLAN ID.
0x00:0x00:0x00:0x00:0x00:0x00	Specifies the MAC address.

©Avaya Inc. 2015 All Rights Reserved.

clear mlt

Clear interswitch trunking (IST) statistics.

Syntax

- `clear mlt ist stats`

Default

None

Command mode

Privileged EXEC

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

clear qos

Clear quality of service (QoS) information.

Syntax

- `clear qos statistics policy`
- `clear qos statistics policy <1-16000>`
- `clear qos statistics policy slot {slot[-slot][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`<1-16000>`	Specifies a policy ID.
`slot {slot[-slot][,...]}`	Clears QoS statistics for a specific slot, from 3-12.

©Avaya Inc. 2015 All Rights Reserved.

clear radius statistics

Clear server statistics.

Syntax

- `clear radius statistics`

Default

None

Command mode

Privileged EXEC

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

clear slpp

Clears SLPP information.

Syntax

- `clear slpp stats`
- `clear slpp stats port {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

clear-stats

Clear port statistic counters.

Syntax

- `clear-stats`
- `clear-stats port {slot/port[-slot/port][,...]}`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

clear telnet

Close open Telnet sessions.

Syntax

- `clear telnet <0-7>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
<0-7>	Specifies the Telnet session ID to close.

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

clear trace

Clear the trace file.

Syntax

- `clear trace`

Default

None

Command mode

Privileged EXEC

©Avaya Inc. 2015 All Rights Reserved.

clilog

Use ACLI logging to track all ACLI commands executed and for fault management purposes. ACLI commands are logged to the system log file as CLILOG module.

Syntax

- `clilog enable`
- `default clilog enable`
- `no clilog enable`

Default

`The default is disabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

cli password

Configure new passwords for each access level, or change the logon or password for the different access levels of the switch. After you receive the Avaya Virtual Services Platform 9000, use default passwords to initially access ACLI. If you use Simple Network Management Protocol version 3 (SNMPv3), you can change encrypted passwords.

Syntax

- `cli password WORD<1-20> layer1`
- `cli password WORD<1-20> layer2`
- `cli password WORD<1-20> layer3`
- `cli password WORD<1-20> read-only`
- `cli password WORD<1-20> read-write`
- `cli password WORD<1-20> read-write-all`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`<layer1|layer2|layer3|read-only|read-write|read-write-all>`	Changes the password for the specific access level. The read-only default logon is ro and the default password is ro. The Layer 1 read/write logon is l1 and the default password is l1.The Layer 2 read/write logon is l2 and the default password is l2. The Layer 3 read/write logon is l3 and the default password is l3. The read/write logon is rw and the default password is rw. The read/write/all logon is rwa and the default password is rwa.
`WORD<1-20>`	Specifies the user login name.

©Avaya Inc. 2015 All Rights Reserved.

cli timeout

Configure the idle timeout period before automatic logoff for ACLI and Telnet sessions.

Syntax

- `cli timeout <30-65535>`
- `default cli timeout`

Default

The default is 900 seconds.

Command mode

Global Configuration

Command parameters

Parameter	Description
<30-65535>	Configures the timeout value, in seconds, to wait for a Telnet or ACLI login session before terminating the connection.

©Avaya Inc. 2015 All Rights Reserved.

clock set

Configure the calendar time in the form of month, day, year, hour, minute, and second.

Syntax

- `clock set <MMddyyyyhhmmss>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<MMddyyyyhhmmss>	Specifies the month, day, year, hours, minutes, and seconds.

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

clock time-zone

Configure the time zone to use an internal system clock to maintain accurate time. The time zone data in Linux includes daylight changes for all time zones from 1901 to 2038. You do not need to configure daylight savings.

Syntax

- `clock time-zone`
- `clock time-zone WORD<1-10>`
- `clock time-zone WORD<1-10> WORD<1-20>`
- `clock time-zone WORD<1-10> WORD<1-20> WORD<1-20>`
- `default clock time-zone`
- `no clock time-zone`

Default

`The default is Coordinated Universal Time (UTC).`

Command mode

Global Configuration

Command parameters

Parameter	Description
WORD<1-10>	Specifies a directory name or a time zone name in /usr/share/zoneinfo, for example, Africa, Australia, Antarctica, or US. To see a list of options, enter clock time-zone at the command prompt without variables.
WORD<1-20> WORD<1-20>	The first instance of WORD<1-20> is the area within the timezone. The value represents a time zone data file in /usr/share/zoneinfo/WORD<1-10>/ , for example, Shanghai in Asia. The second instance of WORD<1-20>is the subarea. The value represents a time zone data file in /usr/share/zoneinfo/WORD<1-10>/WORD<1-20>/, for example, Vevay in America/Indiana. To see a list of options, enter clock time-zone at the command prompt without variables.

©Avaya Inc. 2015 All Rights Reserved.

!(command number)

Executes a previously used command that appears in the output of the show history command. This command is a UNIX feature provided on the VSP 9000. Specify the number that appears before the command in the show history output. You must be in the correct mode to reuse the command.

Syntax

- `!(command number)`

Default

None

Command mode

Privileged EXEC

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

comp-bestpath-med-confed

When enabled, compares multiexit discriminator (MED) attributes within a confederation.

Syntax

- `comp-bestpath-med-confed enable`
- `default comp-bestpath-med-confed`
- `default comp-bestpath-med-confed enable`
- `no comp-bestpath-med-confed`
- `no comp-bestpath-med-confed enable`

Default

`The default value is enable.`

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
`enable`	Enables and compares multiexit discriminator attributes within a BGP confederation.

©Avaya Inc. 2015 All Rights Reserved.

configure

Log on to Global Configuration mode.

Syntax

- `configure`
- `configure network`
- `configure network address {A.B.C.D}`
- `configure network address {A.B.C.D} filename WORD<1-239>`
- `configure network filename WORD<1-239>`
- `configure network filename WORD<1-239> address {A.B.C.D}`
- `configure terminal`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`address {A.B.C.D}`	Specifies an address of the TFTP server.
`filename WORD<1-239>`	Specifies the filename of the configuration file.
`network`	Configures the device from a TFTP network host.
`terminal`	Configures the device from a terminal.

©Avaya Inc. 2015 All Rights Reserved.

copy

Copy files as part of an upgrade procedure to back up files or to move files to another location.

Syntax

- `copy clilog WORD<1-255>`
- `copy running-config startup-config`
- `copy WORD<1-255> WORD<1-255>`
- `copy WORD<1-255> WORD<1-255> -y`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`clilog WORD<1-255>`	Copies the log file to a specific location. You can specify the name and location for the log file in one of the following formats: a.b.c.d:<file>, x:x:x:x:x:x:x:x:<file>, /intflash/<file>, /extflash/<file>, /mnt/intflash/<file>, /mnt/extflash/<file>, and /usb/<file>.
`running-config startup-config`	Copies the running configuration file to /intflash/config.cfg by default.
`WORD<1-255> WORD<1-255>`	Specifies the name and location of the file to copy. You can specify the name and location in one of the following formats: a.b.c.d:<file>, /intflash/<file>, /extflash/<file>, /mnt/intflash/<file>, /mnt/extflash/<file> and /usb/<file>. The first WORD<1-255> identifies the source location and file name. The second WORD<1-255> identifies the destination location and file name.
`-y`	Suppresses the confirmation message before the file copies. If you omit this parameter, you are asked to confirm the action before the switch copies the file.

©Avaya Inc. 2015 All Rights Reserved.

cp

Use this command to copy files.

Syntax

- `cp WORD<1-255> WORD<1-255>`
- `cp WORD<1-255> WORD<1-255> -y`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
WORD <1-255> WORD <1-255>	The first WORD<1-255>specifies the file to copy. The second WORD<1-255> uses one of the following formats: /intflash/ <file> /extflash/ <file> /usb/<file> /mnt/intflash/ <file> /mnt/extflash/ <file>/mnt/intflash is equivalent to the /intflash of the standby CP (if present). /mnt/extflash is equivalent to the /extflash of the standby CP (if present). The VSP will support /mnt/intflash and /mnt/extflash in this release. Word<1-255> is a string of 1-255 characters.
-y	Suppresses the confirmation message before the file copies. If you omit this parameter, you are asked to confirm the action.

©Avaya Inc. 2015 All Rights Reserved.

cp-limit (for an MLT)

Configure the CP Limit functionality to protect the switch from becoming congested by an excess of data flowing through one or more ports.

Syntax

- `cp-limit <1000-20000>`
- `cp-limit <1000-20000> shutdown`
- `no cp-limit shutdown`

Default

`The default limit is 5000.`

Command mode

MLT Interface Configuration

Command parameters

Parameter	Description
`<1000-20000>`	Specifies the packet rate value in the range of 1000 to 20000. The value determines the number of packets coming to the CP every second.
`shutdown`	Enables the shutdown of the MLT.

©Avaya Inc. 2015 All Rights Reserved.

cp-limit (for a port)

Configure the CP Limit functionality to protect the switch from becoming congested by an excess of data flowing through one or more ports.

Syntax

- `cp-limit <1000-20000>`
- `cp-limit <1000-20000> shutdown`
- `cp-limit port {slot/port[-slot/port][,...]} <1000-20000>`
- `cp-limit port {slot/port[-slot/port][,...]} <1000-20000> shutdown`
- `cp-limit port {slot/port[-slot/port][,...]} shutdown`
- `cp-limit shutdown`
- `default cp-limit`
- `default cp-limit port {slot/port[-slot/port][,...]}`
- `no cp-limit port {slot/port[-slot/port][,...]} shutdown`
- `no cp-limit shutdown`

Default

`The default limit is 5000.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<1000-20000>`	Specifies the packet rate value in the range of 1000 to 20000. The value determines the number of packets coming to the CP every second.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`shutdown`	Enables the shutdown of the port.

©Avaya Inc. 2015 All Rights Reserved.

csnp-interval

Configure the Complete Sequence Number Packets (CSNP) interval in seconds. This command is a system level parameter that applies to Level 1 CSNP generation on all interfaces.

Syntax

- `csnp-interval <1-600>`
- `default csnp-interval`
- `no csnp-interval`

Default

`The default CSNP interval is 10 seconds.`

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description
`<1-600>`	Configures the interval, in seconds.

©Avaya Inc. 2015 All Rights Reserved.

debug-file remove

Clears all types of debug files. Use this command to remove all debug files for all slots, or all debug files for specific slots. To remove a specific file, use the remove command instead. Debug files include core, archive, dmalloc, wd_stats, PMEM and flrec files.

Syntax

- `debug-file remove`
- `debug-file remove {slot[-slot][,...]}`
- `debug-file remove {slot[-slot][,...]} all`
- `debug-file remove all`

Default

`None`

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot[-slot][,...]}`	Removes debug files for a specific slot or slots. You can specify a specific slot number , a range of slots, or use the value of all to view information for all slots.
`all`	Removes all types of debug files. If you do not use this parameter, you remove all but the most recent file. If you use this parameter without the slot parameter, you remove all debug files for all slots.

©Avaya Inc. 2015 All Rights Reserved.

debug ip pim

Use PIM traces to aid in PIM troubleshooting.

Syntax

- `debug ip pim assert`
- `debug ip pim bstrap`
- `debug ip pim group {A.B.C.D}`
- `debug ip pim hello`
- `debug ip pim join-prune`
- `debug ip pim pimdbglog`
- `debug ip pim pimdbgtrace`
- `debug ip pim rcv-dbg-trace`
- `debug ip pim register`
- `debug ip pim regstop`
- `debug ip pim rp-adv`
- `debug ip pim send-dbg-trace`
- `debug ip pim source {A.B.C.D}`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`assert`	Sets the assert debug traces to true.
`bstrap`	Sets bootstrap debug traces to true.
`group <A.B.C.D>`	Sets the group value to a specific multicast group value from a specific group IP address.
`hello`	Sets hello debug trace to true.
`join-prune`	Sets join/prune debug trace to true.
`pimdbglog`	Enables whether the switch logs debug traces.
`pimdbgtrace`	Enables or disables PIM debug traces.
`rcv-dbg-trace`	Sets trace messages received by the switch to true.
`register`	Sets register debug trace to true.

regstop	Sets register stop debug trace to true.
rp-adv	Sets rendezvous point (RP) advertisement debug trace to true.
send-dbg-trace	Sets send trace messages forwarded by the switch to true.
source <A.B.C.D>	Sets debug traces from a specific source IP address to true.

©Avaya Inc. 2015 All Rights Reserved.

debug-screen

Display debug messages on the console, or saves them in a log file.

Syntax

- `debug-screen { off | on }`
- `default debug-screen`
- `no debug-screen`

Default

`The default value is off.`

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
<on|off>	Disables BGP screen logging (off) or enable BGP screen logging (on).

©Avaya Inc. 2015 All Rights Reserved.

default-cost

Configures the default OSPF metrics.

Syntax

- `default default-cost`
- `default default-cost ethernet`
- `default default-cost fast-ethernet`
- `default default-cost forty-gig-ethernet`
- `default default-cost gig-ethernet`
- `default default-cost ten-gig-ethernet`
- `default-cost ethernet <1-65535>`
- `default-cost fast-ethernet <1-65535>`
- `default-cost forty-gig-ethernet <1-65535>`
- `default-cost gig-ethernet <1-65535>`
- `default-cost ten-gig-ethernet <1-65535>`

Default

None

Command mode

OSPF Router Configuration

Command parameters

Parameter	Description
`ethernet <1-65535>`	Configures the OSPF default metrics for 10 Mb/s Ethernet. The default is 100.
`fast-ethernet <1-65535>`	Configures the OSPF default metrics for 100 Mb/s (Fast) Ethernet. The default is 10.
`forty-gig-ethernet <1-65535>`	Configures the OSPF default metrics for 40 Gigabit Ethernet. The default is 1.
`gig-ethernet <1-65535>`	Configures the OSPF default metrics for Gigabit Ethernet. The default is 1.
`ten-gig-ethernet <1-65535>`	Configures the OSPF default metrics for 10 Gigabit Ethernet. The default is 1.

©Avaya Inc. 2015 All Rights Reserved.

default-information

Enable the advertisement of a default route to peers, if it is present in the routing table.

Syntax

- `default default-information originate`
- `default-information originate`
- `no default-information originate`

Default

`The default value is disable.`

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
`originate`	Enables the origination default route.

©Avaya Inc. 2015 All Rights Reserved.

default-metric (for BGP)

Configure a value that is sent to a BGP neighbor to determine the cost of a route a neighbor is using.

Syntax

- `default default-metric`
- `default-metric <-1-2147483647>`
- `no default-metric`
- `no default-metric <-1-2147483647>`

Default

`The default value is -1.`

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
`<-1-2147483647>`	Specifies the range of the default metric. A default metric value helps solve the problems associated with redistributing routes that have incompatible metrics.

©Avaya Inc. 2015 All Rights Reserved.

default-metric (for RIP)

Configure RIP default import metric. This value is used by RIP announce of OSPF internal routes if the policy does not specify metric. 0 is used for deconfiguration.

Syntax

- `default default-metric`
- `default-metric <0-15>`

Default

`The default value is 8.`

Command mode

RIP Router Configuration

Command parameters

Parameter	Description
`<0-15>`	Configures the value of default import metric to import a route into RIP domain.

©Avaya Inc. 2015 All Rights Reserved.

default-vlan-id

Configure the default VLAN ID for the port.

Syntax

- `default-vlan-id <0-4084>`
- `default-vlan-id port {slot/port[-slot/port][,...]} <0-4084>`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<0-4084>`	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

delete

Use this command to delete files.

Syntax

- `delete WORD<1-255>`
- `delete WORD<1-255> -y`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
WORD<1-255>	Specifies the name and location of the file to delete in one of the following formats: /intflash/<file>, /extflash/<file>, /usb/<file>, /mnt/intflash/, and <file>/mnt/extflash/. <file>/mnt/intflash is equivalent to the /intflash of the standby CP (if present). /mnt/extflash is equivalent to the /extflash of the standby CP (if present). The VSP will support /mnt/intflash and /mnt/extflash. WORD<1-255> is a string of 1-255 characters.
-y	Suppresses the confirmation message before the file copies. If you omit this parameter, you are asked to confirm the action before the switch deletes the file.

©Avaya Inc. 2015 All Rights Reserved.

dir

View the free space and files in flash memory.

Syntax

- `dir`
- `dir -l`
- `dir -r`
- `dir WORD<1-99>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`-l`	Displays all the details of all the files like name, size and time and date of the file created.
`-r`	Displays the recursive directories.
`Word <1-99>`	Specifies the name of the particular file to view details.

©Avaya Inc. 2015 All Rights Reserved.

disable

Turns off privileged commands and returns you to the User Exec prompt.

Syntax

Default

None

Command mode

Privileged EXEC

©Avaya Inc. 2015 All Rights Reserved.

domain

Specify the RIP domain.

Syntax

- `default domain`
- `domain <0-39321>`

Default

`The default is 0.`

Command mode

RIP Router Configuration

Command parameters

Parameter	Description
`<0-39321>`	Specifies the RIP domain.

©Avaya Inc. 2015 All Rights Reserved.

dos-chkdsk

Check MS DOS file system for any inconsistencies.

Syntax

- `dos-chkdsk WORD <1-99>`
- `dos-chkdsk WORD <1-99> repair`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`repair`	Repairs the errors found.
`WORD <1-99>`	Specifies the device name to repair which is /extflash or /usb.

©Avaya Inc. 2015 All Rights Reserved.

dos-format

Format the external flash or USB.

Syntax

- `dos-format WORD <1-99>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
WORD <1-99>	Specifies the device name to format which is /extflash or /usb.

©Avaya Inc. 2015 All Rights Reserved.

dsapssap

Configure the multiple DSAP and SSAP to create a protocol-based VLAN.

Syntax

- `default dsapssap <0x0-0xffff | 0x0-0x0>`
- `dsapssap <0x0-0xffff | 0x0-0x0>`
- `no dsapssap <0x0-0xffff | 0x0-0x0>`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`<0x0-0xffff | 0x0-0x0>`	Configures a table used to maintain DSAP/SSAP values assigned to an sna802dot2 or user defined VLAN.

©Avaya Inc. 2015 All Rights Reserved.

dump ar

To aid in troubleshooting, a dump of the hardware records can be captured.

Syntax

- `dump ar <1-12> WORD<1-1536> <0-3>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<0-3>	Specifies the verbosity from 0 to 3. Higher numbers specify more verbosity.
<1-12>	Specifies the slot number from 1 to 12.
WORD<1-1536>	Specifies a record type in the AR table. Options include vlan, ip_subnet, mac_vlan, mac, arp, ip, ipmc, ip_filter, protocol, all.

©Avaya Inc. 2015 All Rights Reserved.

duplex

Configure the duplex mode on the Ethernet module. This command applies to 10/100/1000 Mb/s ports.

Syntax

- `default duplex`
- `default duplex [port {slot/port[-slot/port][,...]}] <half|full>`
- `default duplex port {slot/port[-slot/port][,...]}`
- `duplex { half | full }`
- `duplex port {slot/port[-slot/port][,...]} { half | full }`

Default

`The default is half.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<half|full>`	Specifies half- or full-duplex mode. 1 and 10 Gb/s ports must use full-duplex mode.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

duplex (for the management port)

Configure the duplex mode for the Ethernet management port.

Syntax

- `default duplex [port {slot/port[-slot/port][,...]}]`
- `duplex [port {slot/port[-slot/port][,...]}]<half|full>`

Default

`The default is half-duplex mode.`

Command mode

mgmtEthernet Interface Configuration

Command parameters

Parameter	Description
`<half|full>`	Specifies half- or full-duplex mode.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port the following format: a single slot and port (2/1).

©Avaya Inc. 2015 All Rights Reserved.

eapol enable

Configure Extensible Authentication Protocol (EAPoL) on the Virtual Services Platform 9000.

Syntax

- `eapol enable`

Default

None

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

eapol init

Initialize Extensible Authentication Protocol (EAPoL) administration traffic control direction.

Syntax

- `eapol init`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port] [,...]}`	Initializes Extensible Authentication Protocol (EAP) administration traffic control direction.

©Avaya Inc. 2015 All Rights Reserved.

eapol max-request

Configures the maximum EAP requests sent to supplicant before timing out the session.

Syntax

- `default eapol max-request`
- `default eapol port {slot/port[-slot/port][,...]} max-request`
- `eapol max-request <1-10>`
- `eapol port {slot/port[-slot/port][,...]} max-request <1-10>`

Default

`The default is 2.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<1-10>`	Specifies the maximum EAP requests sent to supplicant before timing out the session.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

eapol quiet-interval

Specifies the time interval between authentication failure and start of a new authentication.

Syntax

- `default eapol port {slot/port[-slot/port][,...]} quiet-interval`
- `default eapol quiet-interval`
- `eapol port {slot/port[-slot/port][,...]} quiet-interval <1-65535>`
- `eapol quiet-interval <1-65535>`

Default

`The default is 60.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<1-65535>`	Specifies the time interval in seconds between authentication failure and start of a new authentication.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

eapol re-authenticate

Starts re-authentication immediately.

Syntax

- `eapol re-authenticate {slot/port[-slot/port][,...]}`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port] [,...]}`	Identifies the slot and port.

©Avaya Inc. 2015 All Rights Reserved.

eapol re-authentication

Configures reauthentication.

Syntax

- `default eapol port {slot/port[-slot/port][,...]} re-authentication`
- `default eapol port {slot/port[-slot/port][,...]} re-authentication enable`
- `default eapol port {slot/port[-slot/port][,...]} re-authentication-period`
- `default eapol re-authentication`
- `default eapol re-authentication enable`
- `default eapol re-authentication-period`
- `eapol port {slot/port[-slot/port][,...]} re-authentication`
- `eapol port {slot/port[-slot/port][,...]} re-authentication enable`
- `eapol port {slot/port[-slot/port][,...]} re-authentication-period <1-2147483647>`
- `eapol re-authentication`
- `eapol re-authentication enable`
- `eapol re-authentication-period <1-2147483647>`
- `no eapol port {slot/port[-slot/port][,...]} re-authentication`
- `no eapol port {slot/port[-slot/port][,...]} re-authentication enable`
- `no eapol re-authentication`
- `no eapol re-authentication enable`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables reauthenticating an existing supplicant at a specified time interval. The default is disabled.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`re-`	

authentication-period <1-2147483647>	Specifies the time interval in seconds between successive reauthentications. The default is 3600.

©Avaya Inc. 2015 All Rights Reserved.

eapol server-timeout

Specifies the time to wait for a response from RADIUS server.

Syntax

- `default eapol port {slot/port[-slot/port][,...]} server-timeout`
- `default eapol server-timeout`
- `eapol port {slot/port[-slot/port][,...]} server-timeout <1-65535>`
- `eapol server-timeout <1-65535>`

Default

`The default is 30.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<1-65535>`	Specifies the time in seconds to wait for a response from RADIUS server.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

eapol sess-manage enable

Enable the device to communicate through Extensible Authentication Protocol (EAPoL) and globally enable the session management.

Syntax

- `eapol`
- `eapol sess-manage`
- `eapol sess-manage enable`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`sess-manage enable`	Enables the session management on EAPoL.

©Avaya Inc. 2015 All Rights Reserved.

eapol sess-manage-mode

Enables the port session to be managed by an external device.

Syntax

- `default eapol port {slot/port[-slot/port][,...]} sess-manage-mode`
- `default eapol port {slot/port[-slot/port][,...]} sess-manage-mode enable`
- `default eapol sess-manage-mode`
- `default eapol sess-manage-mode enable`
- `eapol port {slot/port[-slot/port][,...]} sess-manage-mode`
- `eapol port {slot/port[-slot/port][,...]} sess-manage-mode enable`
- `eapol sess-manage-mode`
- `eapol sess-manage-mode enable`
- `no eapol port {slot/port[-slot/port][,...]} sess-manage-mode`
- `no eapol port {slot/port[-slot/port][,...]} sess-manage-mode enable`
- `no eapol sess-manage-mode`
- `no eapol sess-manage-mode enable`

Default

`The default is disabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables the port session to be managed by an external device.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

eapol sess-manage-open-immediate

Configures if the port is opened immediately after 8021x authentication.

Syntax

- `default eapol port {slot/port[-slot/port][,...]} sess-manage-open-immediate`
- `default eapol port {slot/port[-slot/port][,...]} sess-manage-open-immediate enable`
- `default eapol sess-manage-open-immediate`
- `default eapol sess-manage-open-immediate enable`
- `eapol port {slot/port[-slot/port][,...]} sess-manage-open-immediate`
- `eapol port {slot/port[-slot/port][,...]} sess-manage-open-immediate enable`
- `eapol sess-manage-open-immediate`
- `eapol sess-manage-open-immediate enable`
- `no eapol port {slot/port[-slot/port][,...]} sess-manage-open-immediate`
- `no eapol port {slot/port[-slot/port][,...]} sess-manage-open-immediate enable`
- `no eapol sess-manage-open-immediate`
- `no eapol sess-manage-open-immediate enable`

Default

`The default is enabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables the port to be opened immediately after 8021x authentication.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

eapol status

Enable Extensible Authentication Protocol (EAPoL) on an interface.

Syntax

- `default eapol port {slot/port[-slot/port][,...]} status`
- `eapol port {slot/port[-slot/port][,...]} status authorized`
- `eapol port {slot/port[-slot/port][,...]} status auto`
- `eapol port {slot/port[-slot/port][,...]} status unauthorized`
- `eapol status {authorized|auto|unauthorized}`
- `no eapol port {slot/port[-slot/port][,...]} status`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`authorized`	Specifies the port is always authorized.
`auto`	Specifies that port authorization depends on the results of the EAPoL authentication by the RADIUS server.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`unauthorized`	Specifies the port is always unauthorized.

©Avaya Inc. 2015 All Rights Reserved.

eapol supplicant-timeout

Syntax

- `default eapol port {slot/port[-slot/port][,...]} supplicant-timeout`
- `default eapol supplicant-timeout`
- `eapol port {slot/port[-slot/port][,...]} supplicant-timeout <1-65535>`
- `eapol supplicant-timeout <1-65535>`

Default

`The default is 30.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<1-65535>`	Specifies the time in seconds to wait for response from supplicant for all EAP packets except EAP Request/Identity.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

eapol traffic-control

Specifies the desired level of traffic control of port.

Syntax

- `default eapol port {slot/port[-slot/port][,...]} traffic-control`
- `default eapol traffic-control`
- `eapol port {slot/port[-slot/port][,...]} traffic-control in`
- `eapol port {slot/port[-slot/port][,...]} traffic-control in-out`
- `eapol traffic-control in`
- `eapol traffic-control in-out`
- `no eapol port {slot/port[-slot/port][,...]} traffic-control`
- `no eapol traffic-control`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`{in|in-out}`	Specifies the desired level of traffic control of port. The default is in-out.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

eapol transmit-interval

Specifies the time to wait for response from supplicant for EAP Request/Identity packets.

Syntax

- `default eapol port {slot/port[-slot/port][,...]} transmit-interval`
- `default eapol transmit-interval`
- `eapol port {slot/port[-slot/port][,...]} transmit-interval <1-65535>`
- `eapol transmit-interval <1-65535>`

Default

`The default is 30.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<1-65535>`	Specifies the time in seconds to wait for response from supplicant for EAP Request/Identity packets.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

editing

Use a VI line editor to modify script files.

Syntax

- `editing WORD<1-99>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
WORD<1-99>	Specifies the filename and path to edit.

©Avaya Inc. 2015 All Rights Reserved.

enable

Use this command to enter Privileged EXEC mode in ACLI.

Syntax

- `enable`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

enable-diffserv

Enable DiffServ so that the switch provides DiffServ-based QoS on that port.

Syntax

- `default enable-diffserv`
- `default enable-diffserv enable`
- `default enable-diffserv port {slot/port[-slot/port][,...]}`
- `default enable-diffserv port {slot/port[-slot/port][,...]} enable`
- `enable-diffserv`
- `enable-diffserv enable`
- `enable-diffserv port {slot/port[-slot/port][,...]}`
- `enable-diffserv port {slot/port[-slot/port][,...]} enable`
- `no enable-diffserv`
- `no enable-diffserv enable`
- `no enable-diffserv port {slot/port[-slot/port][,...]}`
- `no enable-diffserv port {slot/port[-slot/port][,...]} enable`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables DiffServ for the specified port. The default is disabled.
`port {slot/port [-slot/port][,...]}`	Specifies the slot and port, or slot and port list. To delete the current configuration, use the no option in the command: no enable-diffserv [port <portList>].

©Avaya Inc. 2015 All Rights Reserved.

enable (for a route policy)

Enable the route policy.

Syntax

- `default enable`
- `enable`
- `no enable`

Default

`The default is disable.`

Command mode

Route-Map Configuration

©Avaya Inc. 2015 All Rights Reserved.

encapsulation dot1q

Enable tagging on the ports before configuring Untagged VLANs.

Syntax

- `default encapsulation dot1q`
- `default encapsulation dot1q port {slot/port[-slot/port][,...]}`
- `encapsulation dot1q`
- `encapsulation dot1q port {slot/port[-slot/port][,...]}`
- `no encapsulation dot1q`
- `no encapsulation dot1q port {slot/port[-slot/port][,...]}`

Default

None

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

end

Use this command to return to the Privileged EXEC mode from Global Configuration mode or higher.

Syntax

- end

Default

None

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

exception dump

Configure and enable the core-file collection on the switch.

Syntax

- `exception dump {slot[-slot][,...]} core-pattern`
- `exception dump {slot[-slot][,...]} core-pattern WORD<1-32>`
- `exception dump {slot[-slot][,...]} directory WORD<1-64>`
- `exception dump {slot[-slot][,...]} enable`
- `exception dump {slot[-slot][,...]} max-disk-space <100-1024>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`{slot [-slot][,...]}`	Specifies the slot list to enable the core-files on the switch. Valid slots are 1 to 12, SF1 to SF6, or all.
`core-pattern WORD <1-32>`	Denotes the pattern for generating core-file names.
`directory WORD <1-64>`	Specifies the directory to store core-files. WORD<1-64> specifies the name of the directory file to be stored in the range of 1 to 64 characters.
`enable`	Enables the core-file collection on the slots specified.
`max-disk-space<100-1024>`	Specifies the maximum disk space (in MB) allocated for the collection of core-files.

©Avaya Inc. 2015 All Rights Reserved.

exit

Use this command to exit a command mode and enter the lower command mode. If you use this command in User EXEC mode, you end the current ACLI session.

Syntax

- `exit`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

extflash-stop

Use this command to safely remove the external Compact Flash device.

Syntax

- `extflash-stop`

Default

None

Command mode

Privileged EXEC

©Avaya Inc. 2015 All Rights Reserved.

fabric statistics

Enable fabric statistics on the given port.

Syntax

- `default fabric statistics`
- `default fabric statistics enable`
- `default fabric statistics port {slot/port}`
- `fabric statistics`
- `fabric statistics enable`
- `fabric statistics port {slot/port}`
- `no fabric statistics`
- `no fabric statistics enable`
- `no fabric statistics port {slot/port}`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables fabric statistics on the port specified.
`port {slot/port}`	Specifies the port number that needs to be changed.

©Avaya Inc. 2015 All Rights Reserved.

filter acl

Use an access control list (ACL) to specify an ordered list of ACEs, or filter rules.

Syntax

- `default filter acl <1-2048>`
- `default filter acl <1-2048> name`
- `filter acl <1-2048> enable`
- `filter acl <1-2048> name WORD<0-32>`
- `filter acl <1-2048> type { inVlan | outVlan | inPort | outPort }`
- `filter acl <1-2048> type { inVlan | outVlan | inPort | outPort } name WORD<0-32>`
- `no filter acl <1-2048>`
- `no filter acl <1-2048> enable`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`<1-2048>`	Specifies a unique identifier (1 to 2048) for this ACL.
`name WORD<0-32>`	Specifies an optional descriptive name for the ACL.
`type <inVlan|outVlan|inPort|outPort>`	Specifies the access control list (ACL) type. inVlan and inPort are ingress ACLs, and outVlan and outPort are egress ACLs.

©Avaya Inc. 2015 All Rights Reserved.

filter acl ace

Use an access control entry (ACE) to define a packet pattern and the desired behavior for packets that carry the pattern.

Syntax

- `default filter acl ace <1-2048> <1-2000>`
- `default filter acl ace <1-2048> <1-2000> enable`
- `default filter acl ace <1-2048> <1-2000> name`
- `filter acl ace <1-2048> <1-2000>`
- `filter acl ace <1-2048> <1-2000> enable`
- `filter acl ace <1-2048> <1-2000> name WORD<1-32>`
- `no filter acl ace <1-2048> <1-2000>`
- `no filter acl ace <1-2048> <1-2000> enable`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`<1-2000>`	Specifies an access control entry (ACE) ID from 1 to 2000.
`<1-2048>`	Specifies an access control list (ACL) ID from 1 to 2048.
`enable`	Enables an access control entry (ACE) within an access control list (ACL). After you enable an ACE, to make changes, first disable it.
`name WORD<1-32>`	Specifies an optional descriptive name for the access control entry (ACE) that uses 1-32 characters.

©Avaya Inc. 2015 All Rights Reserved.

filter acl ace action

Configure the access control entry (ACE) action mode as deny or permit.

Syntax

- default filter acl ace action <1-2048> <1-2000> { permit | deny }
- default filter acl ace action <1-2048> <1-2000> { permit | deny } copy-to-pcap
- default filter acl ace action <1-2048> <1-2000> { permit | deny } count
- default filter acl ace action <1-2048> <1-2000> { permit | deny } internal-qos
- default filter acl ace action <1-2048> <1-2000> { permit | deny } ipfix-enable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } log
- default filter acl ace action <1-2048> <1-2000> { permit | deny } mlt-index
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count dscp
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count dscp log
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count dscp log redirect-next-hop
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count dscp log redirect-next-hop ttl
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count dscp log redirect-next-hop ttl unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count dscp log redirect-next-hop unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count dscp log redirect-next-hop unreachable ttl
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count dscp log ttl
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count dscp log ttl unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count dscp log unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count dscp redirect-next-hop
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count

dscp redirect-next-hop ttl

- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count dscp redirect-next-hop ttl unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count dscp redirect-next-hop unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count dscp ttl
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count dscp ttl unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count dscp unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count log
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count log redirect-next-hop
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count log redirect-next-hop unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count log unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count redirect-next-hop
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count redirect-next-hop unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip dscp
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip dscp log
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip dscp log redirect-next-hop
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip dscp log redirect-next-hop ttl
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip dscp log redirect-next-hop ttl unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip dscp log redirect-next-hop unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip dscp log redirect-next-hop unreachable ttl
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip dscp log ttl
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip dscp log ttl unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip dscp log unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip dscp redirect-next-hop
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip dscp redirect-next-hop ttl
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip dscp redirect-next-hop ttl unreachable

- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip dscp redirect-next-hop unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip dscp ttl
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip dscp ttl unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip dscp unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip log
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip log redirect-next-hop
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip log redirect-next-hop ttl
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip log redirect-next-hop ttl unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip log redirect-next-hop unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip log ttl
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip log ttl unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip log unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip redirect-next-hop
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip redirect-next-hop ttl
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip redirect-next-hop ttl unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip redirect-next-hop unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip ttl
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip ttl unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-mlt
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-mlt count
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-mlt count log
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-mlt count log redirect-next-hop
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-mlt count log redirect-next-hop unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-mlt count log unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-mlt count redirect-next-hop

default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-mlt count redirect-next-hop unreachable

- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-mlt count unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-mlt log
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-mlt log redirect-next-hop
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-mlt log redirect-next-hop unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-mlt log unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-mlt redirect-next-hop
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-mlt redirect-next-hop unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-mlt unreachable
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ports
- default filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-vlan
- default filter acl ace action <1-2048> <1-2000> { permit | deny } police
- default filter acl ace action <1-2048> <1-2000> { permit | deny } redirect-next-hop
- default filter acl ace action <1-2048> <1-2000> { permit | deny } remark-dot1p
- default filter acl ace action <1-2048> <1-2000> { permit | deny } remark-dscp
- default filter acl ace action <1-2048> <1-2000> { permit | deny } unreachable
- filter acl ace action <1-2048> <1-2000> { permit | deny }
- filter acl ace action <1-2048> <1-2000> { permit | deny } copy-to-pcap
- filter acl ace action <1-2048> <1-2000> { permit | deny } count
- filter acl ace action <1-2048> <1-2000> { permit | deny } internal-qos <0-7>
- filter acl ace action <1-2048> <1-2000> { permit | deny } ipfix-enable
- filter acl ace action <1-2048> <1-2000> { permit | deny } log
- filter acl ace action <1-2048> <1-2000> { permit | deny } mlt-index <1-16>
- filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip {A.B.C.D}
- filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip {A.B.C.D} dscp <0-256 | 0-256>
- filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip {A.B.C.D} ttl <2-255>
- filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-mlt <1-512>
- filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ports {slot/port[-slot/port][,...]}
- filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-vlan <1-4084>
- filter acl ace action <1-2048> <1-2000> { permit | deny } police <1-16000>

filter acl ace action <1-2048> <1-2000> { permit | deny } redirect-next-hop WORD<1-45>

- filter acl ace action <1-2048> <1-2000> { permit | deny } remark-dot1p <0-7>
- filter acl ace action <1-2048> <1-2000> { permit | deny } remark-dscp <0-256 | 0-256>
- filter acl ace action <1-2048> <1-2000> { permit | deny } unreachable { deny | permit }
- no filter acl ace action <1-2048> <1-2000> { permit | deny }
- no filter acl ace action <1-2048> <1-2000> { permit | deny } copy-to-pcap
- no filter acl ace action <1-2048> <1-2000> { permit | deny } count
- no filter acl ace action <1-2048> <1-2000> { permit | deny } internal-qos
- no filter acl ace action <1-2048> <1-2000> { permit | deny } ipfix-enable
- no filter acl ace action <1-2048> <1-2000> { permit | deny } log
- no filter acl ace action <1-2048> <1-2000> { permit | deny } mlt-index
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count dscp
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count dscp log
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count dscp log redirect-next-hop
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count dscp log redirect-next-hop ttl
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count dscp log ttl
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count dscp redirect-next-hop
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count dscp redirect-next-hop ttl
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count dscp ttl
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count log
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count log redirect-next-hop
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip count redirect-next-hop
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip dscp
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip dscp log
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip dscp log redirect-next-hop
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip dscp log redirect-next-hop ttl
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip dscp log ttl
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip dscp redirect-next-hop
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip dscp redirect-

next-hop ttl

- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip dscp ttl
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip log
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip log redirect-next-hop
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip log redirect-next-hop ttl
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip log ttl
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip redirect-next-hop
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip redirect-next-hop ttl
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ip ttl
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-mlt
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-mlt count
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-mlt count log
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-mlt count log redirect-next-hop
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-mlt count redirect-next-hop
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-mlt log
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-mlt log redirect-next-hop
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-mlt redirect-next-hop
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-ports
- no filter acl ace action <1-2048> <1-2000> { permit | deny } monitor-dst-vlan
- no filter acl ace action <1-2048> <1-2000> { permit | deny } police
- no filter acl ace action <1-2048> <1-2000> { permit | deny } redirect-next-hop
- no filter acl ace action <1-2048> <1-2000> { permit | deny } remark-dot1p
- no filter acl ace action <1-2048> <1-2000> { permit | deny } remark-dscp

Default

The default to configure ACE actions to meter flows after a packet matches an ACE is disabled.

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-2000>	Specifies the access control entry (ACE) ID. Use ACE IDs 1-1000 for security rules. Use ACE IDs 1001-2000 for QoS rules.
<1-2048>	Specifies an access control list (ACL) ID from 1 to 2048.
	Configures the action mode for security access control entries (ACEs). Each

<permit|deny>	ACE has a mode of permit or deny the matched traffic. You can use filters to configure metering of permitted traffic. If you need to enable IPFIX on denied traffic, you must enable it on an individual port basis, which enables IPFIX monitoring on all traffic that enters a port. Note For each Security ACE (1-1000), you must define one or more actions as well as the associated action mode (permit or deny). Otherwise, the security ACE cannot be enabled. There is no default configuration for Security ACEs. With QoS ACEs (1001-2000), the action mode is not configurable. QoS ACEs are always set to action mode permit.
copy-to-pcap	Sends a copy of the packet to the secondary CP module. The access control entry (ACE) ID must be in the range of 1-1000. The default is disabled.
count	Enables the ability to count matching packets. Use this parameter with either a security or QoS access control entry (ACE). The default is disabled.
internal-qos	Configures the Quality of Service (QoS) level. The access control entry (ACE) ID must be in the range of 1001-2000. The default value is 1.
ipfix-enable	Enables Information Protocol Flow Information eXport (IPFIX) metering. The default is disabled.
log	Enables logging to the master CP module. Use this parameter with either a security or QoS access control entry (ACE). The default is disabled.
mlt-index <1-16>	If you use this action, the access control entry (ACE) overrides the mlt-index chosen by the MLT algorithm for packets sent on MLT ports. The MLT index ranges from 1-16. If three ports exist in an MLT (for example: A, B, and C) and you specify an index of 6, the Virtual Services Platform 9000 applies the MOD function and chooses port C. If port C becomes nonoperational, the filtered packets exit the platform from port B. Multicast traffic does not support the MLT index. This variable is a security action. The ACE ID must be in the range of 1-1000.
monitor-dst-ip {A.B.C.D} [dscp<0-63>] [ttl <2-255>]	Configures Layer 3 mirroring. The destination must be an IP address {A.B.C.D}. The default DSCP is 256 (disabled) and the default TTL is 64. For Layer 3 mirroring, every hop in the path from the mirrored port to the remote-mirroring port must be routed. Avaya recommends that you configure the remote-mirrored port in its own VLAN at the last hop to prevent flooding.
monitor-dst-mlt <1-512>	Configures mirroring to a destination MLT group. This action is a security action. The ACE ID must be in the range of 1- 1000.
monitor-dst-ports {slot/port[-slot/port][,...]}	Configures mirroring to a destination port or ports. This action is a security action. The ACE ID must be in the range of 1-1000. {slot/port[-slot/port][,...]} identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
monitor-dst-vlan <1-4084>	Configures mirroring to a destination VLAN. This action is a security action. The ACE ID must be in the range of 1- 1000.
police <1-16000>	Polices the packet according to the specified policy ID (1-16000). A policy must exist. This action is a QoS action. The ACE ID must be in the range of 1001-2000.
redirect-next-hop WORD<1-15>	Specifies the next-hop IP address for redirect mode (a.b.c.d). This action is a security action. The ACE ID must be in the range of 1-1000.
remark-dot1p <0-7>	Specifies the new 802.1 priority bit for matching packets: zero, one, two, three, four, five, six, or seven. This action is a QoS action. The ACE ID must be in the range of 1001-2000.
remark-dscp <0-63>	Specifies the new Per-Hop Behavior (PHB) for matching packets: phbcs0, phbcs1, phbaf11, phbaf12, phbaf13, phbcs2, phbaf21,phbaf22, phbaf23, phbcs3, phbaf31, phbaf32, phbaf33, phbcs4,phbaf41, phbaf42, phbaf43, phbcs5, phbef, phbcs6, phbcs7. This action is a QoS action. The ACE ID must be in the range of 1001-2000.
unreachable	Denies or permits packet dropping when the next-hop for the packet is unreachable. The default value is deny. This action is a security action. The

<deny|permit>	ACE ID must be in the range of 1-1000.

©Avaya Inc. 2015 All Rights Reserved.

filter acl ace arp

Use access control entry (ACE) ARP entries so that the filter looks for ARP requests or responses.

Syntax

- `default filter acl ace arp <1-2048> <1-2000>`
- `filter acl ace arp <1-2048> <1-2000> operation eq arprequest`
- `filter acl ace arp <1-2048> <1-2000> operation eq arpresponse`
- `no filter acl ace arp <1-2048> <1-2000>`
- `no filter acl ace arp <1-2048> <1-2000> operation`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`operation eq <arprequest|arpresponse>`	Specifies an ARP operation type of arpRequest or arpResponse. For ARP, only one operator and attribute exist (eq and operation).

©Avaya Inc. 2015 All Rights Reserved.

filter acl ace ethernet

Use Ethernet access control entries (ACEs) to filter on Ethernet parameters.

Syntax

- `default filter acl ace ethernet <1-2048> <1-2000>`
- `filter acl ace ethernet <1-2048> <1-2000> dst-mac eq WORD<1-1024>`
- `filter acl ace ethernet <1-2048> <1-2000> dst-mac mask WORD<1-1024> WORD<1-1024>`
- `filter acl ace ethernet <1-2048> <1-2000> ether-type eq WORD<1-200>`
- `filter acl ace ethernet <1-2048> <1-2000> port eq {slot/port}`
- `filter acl ace ethernet <1-2048> <1-2000> src-mac eq WORD<1-1024>`
- `filter acl ace ethernet <1-2048> <1-2000> src-mac mask WORD<1-1024> WORD<1-1024>`
- `filter acl ace ethernet <1-2048> <1-2000> vlan-id eq <1-4084>`
- `filter acl ace ethernet <1-2048> <1-2000> vlan-id mask <1-4084> <0-0xFFF | 0x0-0x0>`
- `filter acl ace ethernet <1-2048> <1-2000> vlan-tag-prio eq <0-7>`
- `filter acl ace ethernet <1-2048> <1-2000> vlan-tag-prio mask <0-7> <0-0x7 | 0x0-0x0>`
- `no filter acl ace ethernet <1-2048> <1-2000>`
- `no filter acl ace ethernet <1-2048> <1-2000> dst-mac`
- `no filter acl ace ethernet <1-2048> <1-2000> ether-type`
- `no filter acl ace ethernet <1-2048> <1-2000> port`
- `no filter acl ace ethernet <1-2048> <1-2000> src-mac`
- `no filter acl ace ethernet <1-2048> <1-2000> vlan-id`
- `no filter acl ace ethernet <1-2048> <1-2000> vlan-tag-prio`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`dst-mac <eq|mask> WORD<1-`	The <eq|mask> parameter specifies an operator for a field match condition. The WORD<1-1024> parameter specifies a list of destination MAC addresses separated by

1024>	a comma, or a range of MAC addresses specified from low to high; for example, [AA:BB:CC:DD:EE:FF].
ether-type <eq> WORD<1-200>	The <eq> parameter specifies an operator for a field match condition: equal to. The WORD<1-200> parameter specifies an ether-type name: ip, arp, ipx802dot3, ipx802dot2, ipxSnap, ipxEthernet2, appleTalk, AppleTalk-Arp, sna802dot2, snaEthernet2, netBios, xns, vines, ipV6, rarp, PPPoE-discovery, or PPPoE-session.
port eq <slot/port>	Specifies ports to which to match, where <slot/port> specifies the ports.
src-mac <eq|mask> WORD<1-1024>	The <eq|mask> parameter specifies an operator for a field match condition: equal to. The WORD<1-1024> parameter specifies a list of source MAC addresses separated by separated by a comma, or a range of MAC addresses specified from low to high; for example, [AA:BB:CC:DD:EE:FF].
vlan-id <eq|mask> <1-4084>	Specifies VLANs to match, where <1-4084> specifies the VLAN IDs.
vlan-tag-prio <eq|mask> <0-7>	The <eq|mask> parameter specifies an operator for a field match condition. The <0-7> parameter specifies a VLAN tag priority from 0-7 or undefined.

©Avaya Inc. 2015 All Rights Reserved.

filter acl ace ip

Use IP access control entries (ACEs) to filter on the source IP address, destination IP address, DiffServ Code Point (DSCP), protocol, IP options, and IP fragmentation parameters.

Syntax

- `default filter acl ace ip <1-2048> <1-2000>`
- `filter acl ace ip <1-2048> <1-2000> dscp eq <0-63 | 0-63>`
- `filter acl ace ip <1-2048> <1-2000> dscp mask <0-63 | 0-63> <0-0x40 | 0x0-0x0>`
- `filter acl ace ip <1-2048> <1-2000> dst-ip eq {A.B.C.D}`
- `filter acl ace ip <1-2048> <1-2000> dst-ip mask {A.B.C.D} <0-32>`
- `filter acl ace ip <1-2048> <1-2000> dst-ip mask {A.B.C.D} {A.B.C.D}`
- `filter acl ace ip <1-2048> <1-2000> ip-frag-flag eq { noFragment | anyFragment }`
- `filter acl ace ip <1-2048> <1-2000> ip-options any`
- `filter acl ace ip <1-2048> <1-2000> ip-protocol-type eq WORD<1-256>`
- `filter acl ace ip <1-2048> <1-2000> src-ip eq {A.B.C.D}`
- `filter acl ace ip <1-2048> <1-2000> src-ip mask {A.B.C.D} <0-32>`
- `filter acl ace ip <1-2048> <1-2000> src-ip mask {A.B.C.D} {A.B.C.D}`
- `filter acl ace ip <1-4096> <1-1000> dst-ip eq WORD <1-1024>`
- `no filter acl ace ip <1-2048> <1-2000>`
- `no filter acl ace ip <1-2048> <1-2000> dscp`
- `no filter acl ace ip <1-2048> <1-2000> dst-ip`
- `no filter acl ace ip <1-2048> <1-2000> ip-frag-flag`
- `no filter acl ace ip <1-2048> <1-2000> ip-options`
- `no filter acl ace ip <1-2048> <1-2000> ip-protocol-type`
- `no filter acl ace ip <1-2048> <1-2000> src-ip`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
dscp <eq|mask> WORD <0-256>	The <eq|mask> parameter specifies an operator for a field match condition. The equals to parameter specifies the PHB name or DSCP value {0 to 256, where 256 => disable}, or phbcs0, phbcs1, phbaf11, phbaf12, phbaf13, phbcs2, phbaf21, phbaf22,phbaf23, phbcs3, phbaf31, phbaf32, phbaf33, phbcs4, phbaf41,phbaf42, phbaf43, phbcs5, phbcs6, phbef, or phbcs7.
dst-ip <eq|mask> WORD <1-1024>	The <eq|mask> parameter specifies an operator for a field match condition. The WORD<1-1024> parameter specifies the destination IP address list in one of the following formats: a.b.c.d, [w.x.y.z-p.q.r.s], [l.m.n.o/mask], [a.b.c.d/len].
ip-frag-flag eq <noFragment|anyFragment>	The eq parameter specifies an operator for a field match condition: equal to. The ip-frag-flag parameter specifies a match option for IP fragments: noFragment or anyFragment.
ip-options any	Matches to an IP option. Any is the only option.
ip-protocol-type <eq> WORD <1-256>	The <eq> parameter specifies an operator for a field match condition: equal to. The WORD<1-256> parameter specifies one or more IP protocol types: (1-256), or icmp, tcp, udp, ipsecesp, ipsecah, ospf, vrrp, undefined.
src-ip <eq|mask> WORD <1-1024>	The <eq|mask> parameter specifies an operator for a field match condition: equal to, not equal to, less than or equal to, greater than or equal to. The WORD<1-1024> parameter specifies a source IP address list in one of the following formats: a.b.c.d, [w.x.y.z-p.q.r.s], [l.m.n.o/mask], [a.b.c.d/len].

©Avaya Inc. 2015 All Rights Reserved.

filter acl ace protocol

Use protocol access control entries (ACEs) to filter on the TCP source port, UDP source port, TCP destination port, UDP destination port, ICMP message type, and TCP flags.

Syntax

- `default filter acl ace protocol <1-2048> <1-2000>`
- `filter acl ace protocol <1-2048> <1-2000> dst-port eq WORD<1-60>`
- `filter acl ace protocol <1-2048> <1-2000> dst-port mask WORD<1-60> <0x0-0xFFFF>`
- `filter acl ace protocol <1-2048> <1-2000> icmp-msg-type eq WORD<1-200>`
- `filter acl ace protocol <1-2048> <1-2000> src-port eq <0-65535>`
- `filter acl ace protocol <1-2048> <1-2000> src-port mask <0-65535> <0x0-0xFFFF>`
- `filter acl ace protocol <1-2048> <1-2000> tcp-flags eq WORD<1-50>`
- `filter acl ace protocol <1-2048> <1-2000> tcp-flags mask WORD<1-50> <0-0x3F | 0x0-0x0>`
- `no filter acl ace protocol <1-2048> <1-2000>`
- `no filter acl ace protocol <1-2048> <1-2000> dst-port`
- `no filter acl ace protocol <1-2048> <1-2000> icmp-msg-type`
- `no filter acl ace protocol <1-2048> <1-2000> src-port`
- `no filter acl ace protocol <1-2048> <1-2000> tcp-flags`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`dst-port <eq|mask> WORD<1-60>`	The <eq|mask> parameter specifies an operator for a field match condition: equal to. The WORD<1-60> parameter specifies the destination port for the TCP protocol: (0-65535), or {echo| ftpdata| ftpcontrol| ssh| telnet| dns| http|bgp| hdot323| bootpServer| boorpClient| tftp| rip| rtp| rctp| undefined}.
`icmp-msg-type <eq> WORD <1-200>`	Specifies the internet Control Message Protocol (ICMP) message type attribute of the protocol. The <eq> parameter specifies an operator for a field match condition: equal to. The WORD<1-200> parameter specifies one or more IP protocol types (0-255), or {echoreply|destunreach| sourcequench| redirect| echo-request| routeradv|routerselect| time-exceeded| param-problem| timestamp-request|timestamp-reply| addressmask-request| addressmask-reply| traceroute}.

src-port <eq|mask> WORD<1-65535>	The <eq|mask> parameter specifies an operator for a field match condition. The WORD <1-65535> parameter specifies the destination port for the TCP protocol {0-65535}.
tcp-flags <eq|mask> WORD<1-50>	Specifies TCP-flags attribute of the protocol. The <eq|mask> parameter specifies an operator for a field match condition. The WORD <1-50> parameter specifies one or more TCP flags: {none| fin| syn| rst| push| ack| urg|undefined}. The tcp-flags and icmp-msg-type command options support lists.

©Avaya Inc. 2015 All Rights Reserved.

filter acl enable

Enable the access control list (ACL) on the filter.

Syntax

- `default filter acl <1-2048> enable`
- `filter acl <1-2048> enable`
- `no filter acl <1-2048> enable`

Default

`The default state is enable.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<1-2048>`	Specifies the access control list (ACL) ID int he range of 1 to 2048.
`enable`	Enables the access control list (ACL) state, and all associated ACEs.

©Avaya Inc. 2015 All Rights Reserved.

filter acl log buffer-wrap

Enable buffer wrap on filter log.

Syntax

- `default filter acl log buffer-wrap`
- `filter acl log buffer-wrap`
- `no filter acl log buffer-wrap`

Default

None

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

filter acl port

Associate ports with, or remove ports from, an ACL so that filters do or do not apply to port traffic, respectively.

Syntax

- `default filter acl port <1-2048> {slot/port[-slot/port][,...]}`
- `filter acl port <1-2048> {slot/port[-slot/port][,...]}`
- `no filter acl port <1-2048> {slot/port[-slot/port][,...]}`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Associates a port or a port list to a particular ACL.
`<1-2048>`	Specifies an access control list (ACL) ID from 1-2048.

©Avaya Inc. 2015 All Rights Reserved.

filter acl set

Configure an access control list (ACL) filter.

Syntax

- `default filter acl set <1-2048> default-action`
- `default filter acl set <1-2048> global-action`
- `default filter acl set <1-2048> global-action ipfix-enable`
- `default filter acl set <1-2048> global-action monitor-dst-mlt`
- `default filter acl set <1-2048> global-action monitor-dst-ports`
- `default filter acl set <1-2048> global-action monitor-dst-vlan`
- `filter acl set <1-2048> default-action deny`
- `filter acl set <1-2048> default-action deny control-packet-action deny`
- `filter acl set <1-2048> default-action deny control-packet-action permit`
- `filter acl set <1-2048> default-action permit`
- `filter acl set <1-2048> global-action ipfix-enable`
- `filter acl set <1-2048> global-action monitor-dst-mlt <1-512>`
- `filter acl set <1-2048> global-action monitor-dst-ports {slot/port[-slot/port][,...]}`
- `filter acl set <1-2048> global-action monitor-dst-vlan <1-4084>`
- `no filter acl set <1-2048> global-action ipfix-enable`
- `no filter acl set <1-2048> global-action monitor-dst-mlt`
- `no filter acl set <1-2048> global-action monitor-dst-ports`
- `no filter acl set <1-2048> global-action monitor-dst-vlan`

Default

`The default action is deny. IPFIX is disabled by default.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<1-2048>`	Specifies the access control list (ACL) ID. The range is from 1-2048.

`default-action <permit|deny>`	Specifies the action to be taken when none of the access control entries (ACEs) match. The options are deny or permit.
`global-action{ipfix-enable|monitor-dst-mlt<1-512>|monitor-dst-ports {slot/port [-slot/port][,...]}|monitor-dst-vlan <1-4084>}`	Specifies the action to be taken for all access control entry (ACE) matches. The options are: ipfix-enable|monitor-dst-mlt <1-512>|monitor-dst-ports {slot/port [-slot/port][,...]}|monitor-dst-vlan <1-4084> <1-512> specifies the MLT ID. {slot/port [-slot/port][,...]} specifies the slot and the port number. <1-4084> specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

filter acl vlan

Associate VLANs with, or remove VLANs from, an access control list (ACL) so that filters do or do not apply to VLAN traffic, respectively.

Syntax

- `default filter acl vlan <1-2048> <1-4084>`
- `filter acl vlan <1-2048> <1-4084>`
- `no filter acl vlan <1-2048> <1-4084>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-2048>	Specifies an access control list (ACL) ID from 1-2048.
<1-4084>	Specifies the VLAN IDs from 1-4084.

©Avaya Inc. 2015 All Rights Reserved.

flap-dampening

Enable route suppression for routes that flap on and off.

Syntax

- `default flap-dampening`
- `default flap-dampening enable`
- `flap-dampening`
- `flap-dampening enable`
- `no flap-dampening`
- `no flap-dampening enable`

Default

`The default value is enable.`

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
`enable`	Enables Border Gateway Protocol (BGP) flap-dampening.

©Avaya Inc. 2015 All Rights Reserved.

flight-recorder

Perform various functions on the flight recorder data on the switch.

Syntax

- `flight-recorder all {slot [-slot][,...]}`
- `flight-recorder archive {slot [-slot][,...]}`
- `flight-recorder snapshot {slot [-slot][,...]}`
- `flight-recorder trace {slot [-slot][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`all {slot [-slot][,...]}`	Creates flight recorder snapshot, trace, and archive. {slot[-slot][,...]} specifies the slot number. Valid slots are 1 to 12, SF1 to SF6, or all.
`archive {slot [-slot][,...]}`	Creates tarball of flight recorder files, log files, config file and others. {slot [-slot][,...]} specifies the slot number. Valid slots are 1 to 12, SF1 to SF6, or all.
`snapshot {slot [-slot][,...]}`	Takes the snapshot of flight recorder PMEM data. {slot[-slot][,...]} specifies the slot number. Valid slots are 1 to 12, SF1 to SF6, or all.
`trace {slot [-slot][,...]}`	Takes the snapshot of always-on-trace data. {slot [-slot][,...]} specifies the slot number. Valid slots are 1 to 12, SF1 to SF6, or all.

©Avaya Inc. 2015 All Rights Reserved.

global-debug mask

Display specific debug messages for your global BGP configuration.

Syntax

- `default global-debug mask`
- `global-debug mask WORD<1-100>`
- `no global-debug mask`

Default

None

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
`mask WORD <1-100>`	Specifies one or more mask choices that you enter, separated by commas with no space between choices. For example,[<mask>,<mask>,<mask>...]. Options include: none, all, error, packet, event, trace, warning, state, init, filter, update.

©Avaya Inc. 2015 All Rights Reserved.

grep

Use this Unix command to search files for lines that match a given expression.

Syntax

- `grep WORD<0-1536> WORD<1-99>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
WORD <0-1536>	Searches files for lines that match a given expression. WORD<0-1536> specifies the string to match.
WORD <0-99>	Specifies a filename, /intflash/<file>, /extflash/<file>, /usb/<file>.

©Avaya Inc. 2015 All Rights Reserved.

hash-calc getEcmpRoute

View the Equal Cost Multipath (ECMP) route calculated by the hash algorithm from a source IP address to a destination IP address as a description.

Syntax

- `hash-calc getECMPRoute src-ip {A.B.C.D} dest-ip {A.B.C.D/X}`
- `hash-calc getECMPRoute src-ip {A.B.C.D} dest-ip {A.B.C.D/X} dest-ip-port <0-65535>`
- `hash-calc getECMPRoute src-ip {A.B.C.D} dest-ip {A.B.C.D/X} dest-ip-port <0-65535> ingress-port {slot/port}`
- `hash-calc getECMPRoute src-ip {A.B.C.D} dest-ip {A.B.C.D/X} ingress-port {slot/port}`
- `hash-calc getECMPRoute src-ip {A.B.C.D} dest-ip {A.B.C.D/X} src-ip-port <0-65535>`
- `hash-calc getECMPRoute src-ip {A.B.C.D} dest-ip {A.B.C.D/X} src-ip-port <0-65535> dest-ip-port <0-65535>`
- `hash-calc getECMPRoute src-ip {A.B.C.D} dest-ip {A.B.C.D/X} src-ip-port <0-65535> dest-ip-port <0-65535> ingress-port {slot/port}`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`dest-ip {A.B.C.D/X}`	Specifies the destination address and mask. The source and destination addresses cannot have the same value.
`dest-ip-port <0-65535>`	Specifies the destination IP port.
`getECMPRoute`	Views the Equal Cost Multipath (ECMP) route calculated by the hash algorithm from a source IP address to a destination IP address as a description.
`ingress-port {slot/port}`	Specifies the ingress port.
`src-ip {A.B.C.D}`	Specifies the source address. The source and destination addresses cannot have the same value.
`src-ip-port <0-65535>`	Specifies the source IP port.

©Avaya Inc. 2015 All Rights Reserved.

hash-calc getmltindex traffic-type

View the MLT port calculated by the MLT hash algorithm to determine through which MLT port a packet will exit the system.

Syntax

- `hash-calc getmltindex traffic-type ipv4 dest-val WORD<1-1536> src-val WORD<1-1536> mltID <1-512>`
- `hash-calc getmltindex traffic-type ipv4 dest-val WORD<1-1536> src-val WORD<1-1536> mltID <1-512> dst-port <0-65535>`
- `hash-calc getmltindex traffic-type ipv4 dest-val WORD<1-1536> src-val WORD<1-1536> mltID <1-512> src-port <0-65535>`
- `hash-calc getmltindex traffic-type ipv6 dest-val WORD<1-1536> src-val WORD<1-1536> mltID <1-512>`
- `hash-calc getmltindex traffic-type ipv6 dest-val WORD<1-1536> src-val WORD<1-1536> mltID <1-512> dst-port <0-65535>`
- `hash-calc getmltindex traffic-type ipv6 dest-val WORD<1-1536> src-val WORD<1-1536> mltID <1-512> src-port <0-65535>`
- `hash-calc getmltindex traffic-type non-ip dest-val WORD<1-1536> src-val WORD<1-1536> mltID <1-512>`
- `hash-calc getmltindex traffic-type non-ip dest-val WORD<1-1536> src-val WORD<1-1536> mltID <1-512> dst-port <0-65535>`
- `hash-calc getmltindex traffic-type non-ip dest-val WORD<1-1536> src-val WORD<1-1536> mltID <1-512> src-port <0-65535>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`dest-val WORD<1-1536>`	Specifies the destination address in the range of 1 to 1536. The source and destination addresses cannot have the same value.
`dst-port|src-port <0-65535>`	Specifies the destination port or the source port. The value ranges from 0 to 65535.
`mltID <1-512>`	Specifies the MLT ID. The value ranges from 1 to 512.
`src-val WORD<1-1536>`	Specifies the source address in the range from 1-1536. The source and destination addresses cannot have the same value.
`traffic-type {ipv4|ipv6|non-ip}`	Specifies the type of traffic: ipv4, ipv6 or non-ip.

Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

help

Use this command to see parameters for a particular command. You can use this command in any mode. You can also request Help at any point by entering a question mark after a command, which shows the available options.

Syntax

- `help`
- `help WORD<1-255>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
WORD<1-255>	Enters a command to see the options for that command.

©Avaya Inc. 2015 All Rights Reserved.

high-secure enable

Protect Virtual Services Platform 9000 against IP packets with illegal IP addresses such as loopback addresses or a source IP address of ones, or Class D or Class E addresses from being routed.

Syntax

- `default high-secure`
- `default high-secure enable`
- `default high-secure port {slot/port[-slot/port][,...]}`
- `default high-secure port {slot/port[-slot/port][,...]} enable`
- `high-secure`
- `high-secure enable`
- `high-secure port {slot/port[-slot/port][,...]}`
- `high-secure port {slot/port[-slot/port][,...]} enable`
- `no high-secure`
- `no high-secure enable`
- `no high-secure port {slot/port[-slot/port][,...]}`
- `no high-secure port {slot/port[-slot/port][,...]} enable`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables the high secure feature that blocks packets with illegal IP addresses. This flag is disabled by default.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

host-route

Use host routes when the Virtual Services Platform 9000 resides in a network that uses routing protocols other than OSPF.

Syntax

- `default host-route {A.B.C.D}`
- `default host-route {A.B.C.D} metric`
- `host-route {A.B.C.D}`
- `host-route {A.B.C.D} metric <0-65535>`
- `no host-route {A.B.C.D}`

Default

None

Command mode

OSPF Router Configuration

Command parameters

Parameter	Description
`<A.B.C.D>`	Specifies the IP address of the host router in a.b.c.d format.
`metric <0-65535>`	Configures the metric (cost) for the host route.

©Avaya Inc. 2015 All Rights Reserved.

ibgp-report-import-rt

Configure BGP to advertise imported routes to an interior BGP (IBGP) peer. This command Enable or disables the advertisement of nonBGP imported routes to other IBGP neighbors.

Syntax

- `default ibgp-report-import-rt`
- `default ibgp-report-import-rt enable`
- `ibgp-report-import-rt enable`
- `no ibgp-report-import-rt`
- `no ibgp-report-import-rt enable`

Default

`The default value is enable.`

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
`enable`	Enables advertisement of non BGP imported routes to other IBGP neighbors.

©Avaya Inc. 2015 All Rights Reserved.

ignore-illegal-rtrid

Overlook an illegal router id after enabling BGP.

Syntax

- `default ignore-illegal-rtrid`
- `default ignore-illegal-rtrid enable`
- `ignore-illegal-rtrid enable`
- `no ignore-illegal-rtrid`
- `no ignore-illegal-rtrid enable`

Default

`The default value is enable.`

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
`enable`	Enables or disables the acceptance of a connection from a peer that sends an open message using a router ID of 0 (zero).

©Avaya Inc. 2015 All Rights Reserved.

interface GigabitEthernet

Use this command to enter Interface Configuration mode for a GigabitEthernet slot and port.

Syntax

- `interface GigabitEthernet {slot/port[-slot/port][,...]}`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

interface Loopback

Use this command to enter Interface Configuration mode for a loopback interface.

Syntax

- `interface Loopback <1-256>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-256>	Specifies the loopback ID.

©Avaya Inc. 2015 All Rights Reserved.

interface mgmtEthernet

Use this command to enter Interface Configuration mode for a management interface on the CP module.

Syntax

- `interface mgmtEthernet {slot/port[-slot/port][,...]}`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Specifies the slot and port, either 1/1 or 2/1.

©Avaya Inc. 2015 All Rights Reserved.

interface mlt

Use this command to enter Interface Configuration mode for an MLT.

Syntax

- `interface mlt <1-512>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-512>	Specifies the MLT ID.

©Avaya Inc. 2015 All Rights Reserved.

interface vlan

Use this command to enter Interface Configuration mode for a VLAN.

Syntax

- `interface Vlan <1-4084>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-4084>	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

ip address (for the management port)

Configure the IP address for the Ethernet management port.

Syntax

- `ip address {A.B.C.D A.B.C.D|A.B.C.D/X}`
- `ip address port {slot/port} {A.B.C.D/X}`
- `ip address port {slot/port} {A.B.C.D} {A.B.C.D}`
- `no ip address {A.B.C.D}`

Default

None

Command mode

mgmtEthernet Interface Configuration

Command parameters

Parameter	Description
`{A.B.C.D A.B.C.D|A.B.C.D/X}`	Assigns an IP address and mask for the management port. Important: You cannot assign an address of 0.0.0.0/0. You can specify the mask in either dotted decimal notation or as a decimal number.

©Avaya Inc. 2015 All Rights Reserved.

ip address (loopback)

Configure a circuitless IP interface (CLIP) when you want to provide a virtual interface that is not associated with a physical port. You can use a CLIP interface to provide uninterrupted connectivity to your switch. You can configure a maximum of 256 CLIP interfaces on each device.

Syntax

- `ip address <1-256> {A.B.C.D/X}`
- `ip address <1-256> {A.B.C.D/X} vrf WORD<1-16>`
- `ip address <1-256> {A.B.C.D} {A.B.C.D}`
- `ip address {A.B.C.D/X}`
- `ip address {A.B.C.D/X} vrf WORD<1-16>`
- `ip address {A.B.C.D} {A.B.C.D}`
- `no ip address <1-256> {A.B.C.D}`
- `no ip address <1-256> {A.B.C.D} vrf WORD<1-16>`
- `no ip address {A.B.C.D}`
- `no ip address {A.B.C.D} vrf WORD<1-16>`

Default

None

Command mode

Loopback Interface Configuration

Command parameters

Parameter	Description
[vrf WORD<1-16>]	Specifies an associated VRF by name.
{A.B.C.D/X}	Specifies the IP address and subnet mask.
{A.B.C.D}	Specifies the IP address.
<1-256>	Specifies the interface identification number for the circuitless IP (CLIP).
no	Deletes the address for a particular VRF.

©Avaya Inc. 2015 All Rights Reserved.

ip address (on a VLAN)

Assign an IP address to a VLAN to configure the VLAN.

Syntax

- `ip address {A.B.C.D/X}`
- `ip address {A.B.C.D} {A.B.C.D}`
- `ip address {A.B.C.D} {A.B.C.D} <0-1535>`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`<0-1535>`	Specifies the Mac-offset value. The value is in the range of 0-1535.
`<A.B.C.D/X>|<A.B.C.D> <A.B.C.D>`	Specifies the IP address and subnet mask in the format A.B.C.D/X or A.B.C.D A.B.C.D.

©Avaya Inc. 2015 All Rights Reserved.

ip alternative-route (globally)

Enable the alternative route feature globally.

Syntax

- `default ip alternative-route`
- `ip alternative-route`
- `no ip alternative-route`

Default

`The default is enabled.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`alternative-route`	Enables or disables the Alternative Route feature. The default value is enabled. If the alternative-route parameter is disabled, all existing alternative routes are removed. When the parameter is enabled, all alternative routes are re-added.

©Avaya Inc. 2015 All Rights Reserved.

ip alternative-route (on a VRF)

Enable the alternative route feature for a VRF context.

Syntax

- `default ip alternative-route`
- `ip alternative-route`
- `no ip alternative-route`

Default

`The default is enabled.`

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
`alternative-route`	Enables or disables the Alternative Route feature. The default value is enabled. If the alternative-route parameter is disabled, all existing alternative routes are removed. When the parameter is enabled, all alternative routes are re-added.

©Avaya Inc. 2015 All Rights Reserved.

ip area (loopback)

Designate an area for the circuitless IP (CLIP) interface.

Syntax

- `default ip area`
- `default ip area <1-256>`
- `default ip area vrf WORD<1-16>`
- `ip area <1-256> {A.B.C.D}`
- `ip area <1-256> {A.B.C.D} vrf WORD<1-16>`
- `ip area {A.B.C.D}`
- `ip area {A.B.C.D} vrf WORD<1-16>`
- `no ip area`
- `no ip area <1-256>`
- `no ip area vrf WORD<1-16>`

Default

None

Command mode

Loopback Interface Configuration

Command parameters

Parameter	Description
{A.B.C.D}	Specifies the IP address of the OSPF area that is associated with the CLIP.
<1-256>	Specifies the interface identification number for the CLIP.
default	Sets the loopback area for a particular VRF to the default value of none.
no	Deletes the loopback area for a particular VRF.
vrf WORD<1-16>	Specifies an associated VRF by name.

©Avaya Inc. 2015 All Rights Reserved.

ip arp

Configure ARP static entries to modify the ARP parameters on the device. The only way to change a static ARP is to delete the static ARP entry and create a new entry with new information.

Syntax

- `ip arp {A.B.C.D} 0x00:0x00:0x00:0x00:0x00:0x00 {slot/port}`
- `ip arp {A.B.C.D} 0x00:0x00:0x00:0x00:0x00:0x00 {slot/port} vid <1-4084>`
- `ip arp timeout <1-32767>`
- `no ip arp {A.B.C.D}`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
{A.B.C.D}	Specifies the IP address.
{slot/port}	Specifies the port that receives the flooding.
0x00:0x00:0x00:0x00:0x00:0x00	Specifies the MAC address in hexadecimal format. The MAC address parameter does not accept MAC addresses beginning with 01:00:5e (01:00:5e:00:00:00 to 01:00:5e:ff:ff:ff inclusive).
timeout <1-32767>	Configures the timeout value.
vid <1-4084>	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

ip arp (for a VRF)

Configure ARP static entries to modify the ARP parameters on the device. The only way to change a static ARP is to delete the static ARP entry and create a new entry with new information.

Syntax

- `ip arp {A.B.C.D} 0x00:0x00:0x00:0x00:0x00:0x00 {slot/port}`
- `ip arp {A.B.C.D} 0x00:0x00:0x00:0x00:0x00:0x00 {slot/port} vid <1-4084>`
- `ip arp timeout <1-32767>`
- `no ip arp {A.B.C.D}`

Default

None

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
{A.B.C.D}	Specifies the IP address.
{slot/port}	Specifies the port that receives the flooding.
0x00:0x00:0x00:0x00:0x00:0x00	Specifies the MAC address in hexadecimal format. The MAC address parameter does not accept MAC addresses beginning with 01:00:5e (01:00:5e:00:00:00 to 01:00:5e:ff:ff:ff inclusive).
timeout <1-32767>	Configures the timeout value.
vid <1-4084>	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

ip arp multicast-mac-flooding

Determine whether ARP entries for multicast MAC addresses are associated with the VLAN or the port interface on which they were learned. Links the ARP entry for the Network Load Balancer (NLB) cluster to the multicast group ID (MGID) of the VLAN.

Syntax

- `default ip arp multicast-mac-flooding`
- `ip arp multicast-mac-flooding`
- `no ip arp multicast-mac-flooding`

Default

`The default is disabled.`

Command mode

Global Configuration

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

ip arp-proxy enable (for a port)

Configure an ARP proxy to allow a router to answer a local ARP request for a remote destination.

Syntax

- `default ip arp-proxy`
- `default ip arp-proxy enable`
- `ip arp-proxy enable`
- `no ip arp-proxy`
- `no ip arp-proxy enable`

Default

`The default is disabled.`

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip arp-proxy enable (for a VLAN)

Configure an ARP proxy to allow a router to answer a local ARP request for a remote destination.

Syntax

- `ip arp-proxy enable`
- `no ip arp-proxy`
- `no ip arp-proxy enable`

Default

`The default is disabled.`

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip arp-response (for a port)

Enable Address Resolution Protocol (ARP) on the switch to allow a router to answer a local ARP request.

Syntax

- `default ip arp-response`
- `ip arp-response`
- `no ip arp-response`

Default

None

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip arp-response (for a VLAN)

Enable Address Resolution Protocol (ARP) on the switch to allow a router to answer a local ARP request.

Syntax

- `ip arp-response`
- `no ip arp-response`

Default

None

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip arp static-mcast

Configure Layer 3 multicast MAC filtering to route an IP frame to a unicast IP address and flood it with a destination multicast MAC address. You must manually define a static ARP entry that associates an IP address with a multicast MAC address, flooding ports, and a multilink trunk.

Syntax

- `default ip arp static-mcast {A.B.C.D}`
- `ip arp static-mcast {A.B.C.D} <0x00:0x00:0x00:0x00:0x00:0x00> vid <1-4084> [mlt WORD<1-16>][port {slot/port[-slot/port][,...]}] [WORD<1-16>]`
- `no ip arp static-mcast {A.B.C.D}`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<0x00:0x00:0x00:0x00:0x00:0x00>	Specifies the MAC address in hexadecimal format. The MAC address parameter does not accept MAC addresses beginning with 01:00:5e (01:00:5e:00:00:00 to 01:00:5e:ff:ff:ff inclusive).
A.B.C.D	Specifies the IP address.
mlt WORD<1-16>	Specifies the multilink trunking ID.
port {slot/port[-slot/port][,...]}	Specifies the port that receives the multicast flooding. Type the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
vid <1-4084>	Specifies the VLAN ID.
WORD<1-16>	Specifies the multilink trunking ID.

©Avaya Inc. 2015 All Rights Reserved.

ip as-list

Use an asynchronous (AS) path list to restrict the routing information a router learns or advertises to and from a neighbor. The AS path list acts as a filter that Match AS paths.

Syntax

- `ip as-list <1-1024> memberId <0-65535> <permit|deny> as-path WORD<0-1536>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`<permit|deny>`	Permits or denies access for matching conditions.
`as-list <1-1024>`	Creates the specified AS-path list entry.
`as-path WORD <0-1536>`	Specifies an integer value between 0 and 1536 placed within quotation marks " ."
`memberid <0-65535>`	Adds a regular expression entry to the specified AS-path list. It is an integer value between 0 and 65 535.

©Avaya Inc. 2015 All Rights Reserved.

ip as-list (for a VRF)

Use an asynchronous (AS) path list to restrict the routing information a router learns or advertises to and from a neighbor. The AS path list acts as a filter that Match AS paths.

Syntax

- `ip as-list <1-1024> memberid <0-65535> { permit | deny } as-path WORD<0-1536>`
- `no ip as-list <1-1024> as-path WORD<0-1536>`
- `no ip as-list <1-1024> memberid <0-65535>`

Default

None

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
`{ permit | deny }`	Permits or denies access for matching conditions.
`<1-1024>`	Creates the specified AS-path list entry.
`as-path WORD<0-1536>`	Specifies an integer value between 0 and 1536 placed within quotation marks " ."
`memberid <0-65535>`	Adds a regular expression entry to the specified AS-path list.

©Avaya Inc. 2015 All Rights Reserved.

ip bgp

Enables BGP on the VRF.

Syntax

- `default ip bgp`
- `ip bgp`
- `no ip bgp`

Default

`The default value is disabled.`

Command mode

VRF Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip bgp aggregate-address

Add or delete an aggregate address in a BGP routing table.

Syntax

- default ip bgp aggregate-address <prefix/len>
- default ip bgp aggregate-address <prefix/len> advertise-map
- default ip bgp aggregate-address <prefix/len> as-set
- default ip bgp aggregate-address <prefix/len> attribute-map
- default ip bgp aggregate-address <prefix/len> summary-only
- default ip bgp aggregate-address <prefix/len> suppress-map
- ip bgp aggregate-address <prefix/len>
- ip bgp aggregate-address <prefix/len> advertise-map WORD<0-1536>
- ip bgp aggregate-address <prefix/len> as-set
- ip bgp aggregate-address <prefix/len> attribute-map WORD<0-1536>
- ip bgp aggregate-address <prefix/len> summary-only
- ip bgp aggregate-address <prefix/len> suppress-map WORD<0-1536>
- no ip bgp aggregate-address <prefix/len>
- no ip bgp aggregate-address <prefix/len> advertise-map
- no ip bgp aggregate-address <prefix/len> as-set
- no ip bgp aggregate-address <prefix/len> attribute-map
- no ip bgp aggregate-address <prefix/len> summary-only
- no ip bgp aggregate-address <prefix/len> suppress-map

Default

The default is disabled.

Command mode

VRF Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip bgp aggregation

Enable or disable automatic route aggregation on the port. When enabled, the router automatically aggregates routes to their natural mask when they are advertised on an interface in a different class network.

Syntax

- `default ip bgp aggregation`
- `default ip bgp aggregation enable`
- `ip bgp aggregation`
- `ip bgp aggregation enable`
- `no ip bgp aggregation`
- `no ip bgp aggregation enable`

Default

`The default is disabled.`

Command mode

VRF Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip bgp always-compare-med

When enabled, compares multiexit discriminator (MED) attributes from neighbors in different autonomous systems.

Syntax

- `default ip bgp always-compare-med`
- `ip bgp always-compare-med`
- `no ip bgp always-compare-med`

Default

`The default is enabled.`

Command mode

VRF Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip bgp apply redistribute

Configure a redistribute entry to announce routes of a certain source protocol type into the Border Gateway Protocol (BGP) domain, for example, static, Routing Information Protocol (RIP), or direct routes.

Syntax

- `ip bgp apply redistribute`
- `ip bgp apply redistribute direct`
- `ip bgp apply redistribute direct vrf WORD<1-16>`
- `ip bgp apply redistribute direct vrf-src WORD<1-16>`
- `ip bgp apply redistribute isis`
- `ip bgp apply redistribute isis vrf WORD<1-16>`
- `ip bgp apply redistribute isis vrf-src WORD<1-16>`
- `ip bgp apply redistribute ospf`
- `ip bgp apply redistribute ospf vrf WORD<1-16>`
- `ip bgp apply redistribute ospf vrf-src WORD<1-16>`
- `ip bgp apply redistribute rip`
- `ip bgp apply redistribute rip vrf WORD<1-16>`
- `ip bgp apply redistribute rip vrf-src WORD<1-16>`
- `ip bgp apply redistribute static`
- `ip bgp apply redistribute static vrf WORD<1-16>`
- `ip bgp apply redistribute static vrf-src WORD<1-16>`
- `ip bgp apply redistribute vrf WORD<1-16>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF instance by name.
`vrf-src`	Specifies the source VRF instance. This parameter is not required for redistribution

WORD<1-16>	within the same VRF.

©Avaya Inc. 2015 All Rights Reserved.

ip bgp auto-peer-restart enable

Enable the process that automatically restarts a connection to a BGP neighbor.

Syntax

- `default ip bgp auto-peer-restart`
- `default ip bgp auto-peer-restart enable`
- `ip bgp auto-peer-restart enable`
- `no ip bgp auto-peer-restart`
- `no ip bgp auto-peer-restart enable`

Default

`The default is enabled.`

Command mode

VRF Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip bgp auto-summary

Summarize the networks based on class limits after BGP is enabled. (For example, Class A, B, C networks).

Syntax

- `default ip bgp auto-summary`
- `ip bgp auto-summary`
- `no ip bgp auto-summary`

Default

`The default is enabled.`

Command mode

VRF Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip bgp debug-screen

Display debug messages on the console, or saves them in a log file.

Syntax

- `default ip bgp debug-screen`
- `ip bgp debug-screen { off | on }`
- `no ip bgp debug-screen`

Default

`The default is off.`

Command mode

VRF Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip bgp default-information

Enable the advertisement of a default route to peers, if it is present in the routing table.

Syntax

- `default ip bgp default-information originate`
- `ip bgp default-information originate`
- `no ip bgp default-information originate`

Default

`The default is disabled.`

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
`originate`	Enables the origination default route.

©Avaya Inc. 2015 All Rights Reserved.

ip bgp default local-preference

Specifies the default value of the local preference attribute.

Syntax

- `default ip bgp default local-preference`
- `ip bgp default local-preference <0-2147483647>`
- `no ip bgp default local-preference`

Default

`The default is 0.`

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
`<0-2147483647>`	Specifies the preference value.

©Avaya Inc. 2015 All Rights Reserved.

ip bgp default-metric

Configure a value that is sent to a BGP neighbor to determine the cost of a route a neighbor is using.

Syntax

- `default ip bgp default-metric`
- `ip bgp default-metric <-1-2147483647>`
- `no ip bgp default-metric`

Default

`The default value is -1.`

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
`<-1-2147483647>`	Specifies the range of the default metric. A default metric value helps solve the problems associated with redistributing routes that have incompatible metrics.

©Avaya Inc. 2015 All Rights Reserved.

ip bgp deterministic-med enable

Enables deterministic MED. Deterministic MED, when enabled, means that the first AS of the multiple paths must be the same.

Syntax

- `default ip bgp deterministic-med`
- `default ip bgp deterministic-med enable`
- `ip bgp deterministic-med enable`
- `no ip bgp deterministic-med`
- `no ip bgp deterministic-med enable`

Default

`The default is disabled.`

Command mode

VRF Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip bgp enable

Enabled BGP on the VRF.

Syntax

- `default ip bgp enable`
- `ip bgp enable`
- `no ip bgp enable`

Default

`The default is disabled.`

Command mode

VRF Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip bgp flap-dampening

Enable route suppression for routes that flap on and off.

Syntax

- `default ip bgp flap-dampening`
- `default ip bgp flap-dampening enable`
- `ip bgp flap-dampening`
- `ip bgp flap-dampening enable`
- `no ip bgp flap-dampening`
- `no ip bgp flap-dampening enable`

Default

`The default is enabled.`

Command mode

VRF Router Configuration

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

ip bgp global-debug mask

Display specific debug messages for your global BGP configuration.

Syntax

- `default ip bgp global-debug mask`
- `ip bgp global-debug mask WORD<1-100>`
- `no ip bgp global-debug mask`

Default

None

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
WORD<1-100>	Specifies one or more mask choices that you enter, separated by commas with no space between choices. For example,[<mask>,<mask>,<mask>...]. Options include: none, all, error, packet, event, trace, warning, state, init, filter, update.

©Avaya Inc. 2015 All Rights Reserved.

ip bgp ibgp-report-import-rt enable

Configure BGP to advertise imported routes to an interior BGP (IBGP) peer. This command enable or disables the advertisement of non-BGP imported routes to other IBGP neighbors.

Syntax

- `default ip bgp ibgp-report-import-rt enable`
- `ip bgp ibgp-report-import-rt enable`
- `no ip bgp ibgp-report-import-rt enable`

Default

`The default is enabled.`

Command mode

VRF Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip bgp ignore-illegal-rtrid enable

Overlook an illegal router id after enabling BGP.

Syntax

- `default ip bgp ignore-illegal-rtrid`
- `default ip bgp ignore-illegal-rtrid enable`
- `ip bgp ignore-illegal-rtrid enable`
- `no ip bgp ignore-illegal-rtrid`
- `no ip bgp ignore-illegal-rtrid enable`

Default

`The default is enabled.`

Command mode

VRF Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip bgp in-route-map

Apply a route policy to all incoming routes.

Syntax

- `default ip bgp in-route-map`
- `ip bgp in-route-map WORD<0-256>`
- `no ip bgp in-route-map WORD<0-256>`

Default

None

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
WORD<0-256>	An alphanumeric string length (0–256 characters) that indicates the name of the route map or policy.

©Avaya Inc. 2015 All Rights Reserved.

ip bgp multiple-paths <1-8>

Configures the maximum number of equal-cost-paths that are available to a BGP router by limiting the number of equal-cost-paths the routing table can store.

Syntax

- `default ip bgp multiple-paths`
- `ip bgp multiple-paths <1-8>`

Default

`The default is 1.`

Command mode

VRF Router Configuration

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

ip bgp neighbor

Configure BGP neighbors for a VRF context.

Syntax

- default ip bgp neighbor <nbr_ipaddr|peer-group-name>
- default ip bgp neighbor <nbr_ipaddr|peer-group-name> advertisement-interval
- default ip bgp neighbor <nbr_ipaddr|peer-group-name> allow-as-in
- default ip bgp neighbor <nbr_ipaddr|peer-group-name> as-override
- default ip bgp neighbor <nbr_ipaddr|peer-group-name> default-originate
- default ip bgp neighbor <nbr_ipaddr|peer-group-name> ebgp-multihop
- default ip bgp neighbor <nbr_ipaddr|peer-group-name> enable
- default ip bgp neighbor <nbr_ipaddr|peer-group-name> in-route-map
- default ip bgp neighbor <nbr_ipaddr|peer-group-name> max-prefix
- default ip bgp neighbor <nbr_ipaddr|peer-group-name> MD5-authentication enable
- default ip bgp neighbor <nbr_ipaddr|peer-group-name> neighbor-debug-mask
- default ip bgp neighbor <nbr_ipaddr|peer-group-name> next-hop-self
- default ip bgp neighbor <nbr_ipaddr|peer-group-name> out-route-map
- default ip bgp neighbor <nbr_ipaddr|peer-group-name> remote-as
- default ip bgp neighbor <nbr_ipaddr|peer-group-name> remove-private-as enable
- default ip bgp neighbor <nbr_ipaddr|peer-group-name> retry-interval
- default ip bgp neighbor <nbr_ipaddr|peer-group-name> send-community
- default ip bgp neighbor <nbr_ipaddr|peer-group-name> site-of-origin
- default ip bgp neighbor <nbr_ipaddr|peer-group-name> soft-reconfiguration-in enable
- default ip bgp neighbor <nbr_ipaddr|peer-group-name> timers
- default ip bgp neighbor <nbr_ipaddr|peer-group-name> update-source
- default ip bgp neighbor <nbr_ipaddr|peer-group-name> weight
- ip bgp neighbor <nbr_ipaddr|peer-group-name>
- ip bgp neighbor <nbr_ipaddr|peer-group-name> advertisement-interval <5-120>
- ip bgp neighbor <nbr_ipaddr|peer-group-name> allow-as-in <0-10>
- ip bgp neighbor <nbr_ipaddr|peer-group-name> as-override

- ip bgp neighbor <nbr_ipaddr|peer-group-name> default-originate
- ip bgp neighbor <nbr_ipaddr|peer-group-name> ebgp-multihop
- ip bgp neighbor <nbr_ipaddr|peer-group-name> enable
- ip bgp neighbor <nbr_ipaddr|peer-group-name> in-route-map WORD<0-256>
- ip bgp neighbor <nbr_ipaddr|peer-group-name> max-prefix <0-2147483647>
- ip bgp neighbor <nbr_ipaddr|peer-group-name> MD5-authentication enable
- ip bgp neighbor <nbr_ipaddr|peer-group-name> neighbor-debug-mask WORD<1-100>
- ip bgp neighbor <nbr_ipaddr|peer-group-name> next-hop-self
- ip bgp neighbor <nbr_ipaddr|peer-group-name> out-route-map WORD<0-256>
- ip bgp neighbor <nbr_ipaddr|peer-group-name> peer-group WORD<0-1536>
- ip bgp neighbor <nbr_ipaddr|peer-group-name> remote-as WORD<0-11>
- ip bgp neighbor <nbr_ipaddr|peer-group-name> remove-private-as enable
- ip bgp neighbor <nbr_ipaddr|peer-group-name> retry-interval <1-65535>
- ip bgp neighbor <nbr_ipaddr|peer-group-name> send-community
- ip bgp neighbor <nbr_ipaddr|peer-group-name> site-of-origin <0-65535> <0-2147483647>
- ip bgp neighbor <nbr_ipaddr|peer-group-name> site-of-origin {A.B.C.D} <0-65535>
- ip bgp neighbor <nbr_ipaddr|peer-group-name> soft-reconfiguration-in enable
- ip bgp neighbor <nbr_ipaddr|peer-group-name> timers <0-21845> <0-65535>
- ip bgp neighbor <nbr_ipaddr|peer-group-name> update-source {A.B.C.D}
- ip bgp neighbor <nbr_ipaddr|peer-group-name> weight <0-65535>
- no ip bgp neighbor <nbr_ipaddr|peer-group-name>
- no ip bgp neighbor <nbr_ipaddr|peer-group-name> as-override
- no ip bgp neighbor <nbr_ipaddr|peer-group-name> default-originate
- no ip bgp neighbor <nbr_ipaddr|peer-group-name> ebgp-multihop
- no ip bgp neighbor <nbr_ipaddr|peer-group-name> enable
- no ip bgp neighbor <nbr_ipaddr|peer-group-name> in-route-map
- no ip bgp neighbor <nbr_ipaddr|peer-group-name> MD5-authentication enable
- no ip bgp neighbor <nbr_ipaddr|peer-group-name> neighbor-debug-mask
- no ip bgp neighbor <nbr_ipaddr|peer-group-name> next-hop-self
- no ip bgp neighbor <nbr_ipaddr|peer-group-name> out-route-map
- no ip bgp neighbor <nbr_ipaddr|peer-group-name> peer-group
- no ip bgp neighbor <nbr_ipaddr|peer-group-name> remove-private-as enable
- no ip bgp neighbor <nbr_ipaddr|peer-group-name> send-community
- no ip bgp neighbor <nbr_ipaddr|peer-group-name> site-of-origin
- no ip bgp neighbor <nbr_ipaddr|peer-group-name> soft-reconfiguration-in enable

- `no ip bgp neighbor <nbr_ipaddr|peer-group-name> update-source`

Default

None

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
`<nbr_ipaddr|peer-group-name>`	Specifies the neighbor IP address or the neighbor group name.
`advertisement-interval <5-120>`	Specifies the IP Border Gateway Protocol (BGP) route advertisement interval.
`allow-as-in <0-10>`	Specifies the IP Border Gateway Protocol (BGP) neighbor allow-as-in.
`as-override`	Specifies the as-override.
`default-originate`	Specifies the default-originate.
`ebgp-multihop`	Specifies EBGP-multihop.
`enable`	Enables the command.
`in-route-map WORD<0-256>`	Specifies the in-route-map.
`max-prefix <0-2147483647>`	Specifies the max-prefix.
`MD5-authentication enable`	Enables the Message Digest 5 (MD5)-authentication.
`neighbor-debug-mask WORD<1-100>`	Specifies the neighbor-debug-mask.
`next-hop-self`	Specifies the next-hop-self.
`out-route-map WORD<0-256>`	Specifies the out-route-map.
`peer-group WORD<0-1536>`	Specifies the peer group.
`remote-as WORD<0-11>`	Specifies the remote-as.
`remove-private-as enable`	Enables the remote-private-as enable.
`retry-interval <1-65535>`	Specifies the retry-interval.
`send-community`	Specifies the send-community.
`site-of-origin {A.B.C.D} <0-65535>`	Specifies the site-of-origin.
`site-of-origin <0-65535> <0-2147483647>`	Specifies the site-of-origin.
`timers <0-21845> <0-65535>`	Specifies the timers.
`update-source {A.B.C.D}`	Specifies the update-source.
`weight <0-65535>`	Specifies the weight.

©Avaya Inc. 2015 All Rights Reserved.

ip bgp neighbor password

Specify the password for IP BGP.

Syntax

- `default ip bgp neighbor password <nbr_ipaddr|peer-group-name> WORD<0-1536>`
- `ip bgp neighbor password <nbr_ipaddr|peer-group-name> WORD<0-1536>`
- `no ip bgp neighbor password <nbr_ipaddr|peer-group-name> WORD<0-1536>`

Default

None

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
`<nbr_ipaddr|peer-group-name>`	Specifies the peer IP address or the peer group name.
`password`	Configures the IP BGP neighbor password.
`WORD<0-1536>`	Specifies a password for IP BGP.

©Avaya Inc. 2015 All Rights Reserved.

ip bgp network

Specify the Interior Gateway Protocol (IGP) network prefixes for Border Gateway Protocol (BGP) to advertise for redistribution.

Syntax

- `default ip bgp network <prefix/len>`
- `ip bgp network <prefix/len>`
- `ip bgp network <prefix/len> metric <0-65535>`
- `no ip bgp network <prefix/len>`

Default

None

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
`<prefix/len>`	Specifies IGP network prefixes for Border Gateway Protocol (BGP) to advertise for redistribution. This command imports routes into BGP. WORD <1-256> is the IPv4 or the IPv6 network address and mask.
`metric <0-65535>`	Corresponds to the multiexit discriminator (MED) BGP attribute for the route.

©Avaya Inc. 2015 All Rights Reserved.

ip bgp no-med-path-is-worst enable

Enable Border Gateway Protocol (BGP) to treat an update without a multiexit discriminator (MED) attribute as the worst path.

Syntax

- `default ip bgp no-med-path-is-worst`
- `default ip bgp no-med-path-is-worst enable`
- `ip bgp no-med-path-is-worst enable`
- `no ip bgp no-med-path-is-worst`
- `no ip bgp no-med-path-is-worst enable`

Default

`The default value is enable.`

Command mode

VRF Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip bgp out-route-map WORD<0-256>

Applies a route policy rule to all outgoing routes that are learned from, or sent to, the local peers or peer groups, of the BGP router. The local BGP router is the BGP router that allows or disallows routes, and sets attributes in incoming or outgoing updates.

Syntax

- `default ip bgp out-route-map`
- `ip bgp out-route-map WORD<0-256>`
- `no ip bgp out-route-map WORD<0-256>`

Default

None

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
WORD<0-256>	Specifies the route map or policy name in an alphanumeric string.

©Avaya Inc. 2015 All Rights Reserved.

ip bgp quick-start enable

Enables the quick-start flag for exponential backoff.

Syntax

- `default ip bgp quick-start`
- `default ip bgp quick-start enable`
- `ip bgp quick-start enable`
- `no ip bgp quick-start`
- `no ip bgp quick-start enable`

Default

`The default value is enable.`

Command mode

VRF Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip bgp redistribute

Configure and enable redistribution entries to allow a protocol to announce routes of a certain source type, for example, static, RIP, or direct.

Syntax

- `default ip bgp redistribute WORD<0-32>`
- `default ip bgp redistribute WORD<0-32> enable`
- `default ip bgp redistribute WORD<0-32> metric`
- `default ip bgp redistribute WORD<0-32> route-map`
- `default ip bgp redistribute WORD<0-32> vrf-src WORD<1-16>`
- `ip bgp redistribute WORD<0-32>`
- `ip bgp redistribute WORD<0-32> enable`
- `ip bgp redistribute WORD<0-32> metric <0-65535>`
- `ip bgp redistribute WORD<0-32> route-map WORD<0-64>`
- `ip bgp redistribute WORD<0-32> vrf-src WORD<1-16>`
- `no ip bgp redistribute WORD<0-32>`
- `no ip bgp redistribute WORD<0-32> enable`
- `no ip bgp redistribute WORD<0-32> route-map`
- `no ip bgp redistribute WORD<0-32> vrf-src WORD<1-16>`

Default

None

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
`enable`	Enables the route redistribution instance.
`metric <0-65535>`	Configures the metric to apply to redistributed routes.
`route-map WORD<0-64>`	Configures the route map to apply to redistributed routes.
`vrf-src WORD<1-16>`	Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.
`WORD<0-32>`	Specifies the type of routes to redistribute-the protocol source.

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

ip bgp restart-bgp

Restart BGP for a particular peer.

Syntax

- `ip bgp restart-bgp`
- `ip bgp restart-bgp neighbor WORD<0-1536>`
- `ip bgp restart-bgp neighbor WORD<0-1536> soft-reconfiguration {in|out}`
- `ip bgp restart-bgp neighbor WORD<0-1536> vrf WORD<1-16>`
- `ip bgp restart-bgp vrf WORD<1-16>`
- `ip bgp restart-bgp vrf WORD<1-16> soft-reconfiguration {in|out}`

Default

`The default for soft-reconfiguration is: in`

Command mode

User EXEC

Command parameters

Parameter	Description
`soft-configuration {in|out}`	Enables or disables soft-reconfiguration. If peer soft-reconfiguration is enabled in the in-bound direction, the policy can be changed and routes can be re-learned without having to reset the BGP connection. Enabling soft-reconfiguration, using the in parameter, causes the system to store all BGP routes in local memory. Even non-best routes will be stored if soft-configuration in is enabled. Setting the value to out forces the neighbor to send out all the updates to the remote neighbor without resetting the connection.
`vrf WORD<1-16>`	Applies the BGP configuration for a particular VRF.
`WORD<1-1536>`	Specifies the neighbor IP address or the neighbor group name.

©Avaya Inc. 2015 All Rights Reserved.

ip bgp router-id {A.B.C.D}

Specify the BGP router ID in IP address format.

Syntax

- `default ip bgp router-id`
- `ip bgp router-id {A.B.C.D}`
- `no ip bgp router-id`

Default

None

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
{A.B.C.D}	Identifies the router IP address.

©Avaya Inc. 2015 All Rights Reserved.

ip bgp stats-clear-counters

Clears the BGP configuration statistics.

Syntax

- `ip bgp stats-clear-counters`
- `ip bgp stats-clear-counters neighbor <nbr_ipaddr|peer-group-name>`
- `ip bgp stats-clear-counters vrf WORD<1-16>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`neighbor <nbr_ipaddress|peer-group-name>`	Clears the BGP configuration statistics for the peer IP address or the peer group name.
`vrf WORD<1-16>`	Clears the statistics for the BGP configuration for a particular VRF.

©Avaya Inc. 2015 All Rights Reserved.

ip bgp synchronization

Enables the router to accept routes from BGP peers without waiting for an update from the IGP.

Syntax

- `default ip bgp synchronization`
- `ip bgp synchronization`
- `no ip bgp synchronization`

Default

`The default value is enable.`

Command mode

VRF Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip bgp traps enable

Enables BGP traps.

Syntax

- `default ip bgp traps`
- `default ip bgp traps enable`
- `ip bgp traps enable`
- `no ip bgp traps`
- `no ip bgp traps enable`

Default

`The default value is disable.`

Command mode

VRF Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip community-list

Use community lists to specify permitted routes by using their BGP community. This list acts as a filter that Match communities or AS numbers

Syntax

- `ip community-list <1-1024> memberId <0-65535> <permit|deny> community-string WORD<0-256>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<permit|deny>	Sets the access mode, which permits or denies access for matching conditions.
community-list <1-1024>	Creates the specified community list entry. <1-1024> specifies the list id.
community-string WORD<0-256>	Specifies an alphanumeric string value with a string length of 0 to 1536 characters. This string value is either an AS num: community-value or a well-known community string. Well known communities include: internet no-export no-advertise local-as (known as NO_EXPORT_SUBCONFED).
memberId <0-65535>	Adds an entry to the community list. <0-65535> is an integer value that represents the member ID in the community list.

©Avaya Inc. 2015 All Rights Reserved.

ip dhcp-relay (for an MLT)

Configure Dynamic Host Configuration Protocol (DHCP) Relay on an interface. The command no ip dhcp-relay disables DHCP Relay but does not delete the DHCP entry.

Syntax

- default ip dhcp-relay broadcast
- default ip dhcp-relay circuitId
- default ip dhcp-relay fwd-path {A.B.C.D}
- default ip dhcp-relay fwd-path {A.B.C.D} mode
- default ip dhcp-relay fwd-path {A.B.C.D} vrid <1-255>
- default ip dhcp-relay max-hop
- default ip dhcp-relay min-sec
- default ip dhcp-relay mode
- default ip dhcp-relay remoteId
- default ip dhcp-relay trusted
- ip dhcp-relay broadcast
- ip dhcp-relay circuitId
- ip dhcp-relay fwd-path {A.B.C.D}
- ip dhcp-relay fwd-path {A.B.C.D} disable
- ip dhcp-relay fwd-path {A.B.C.D} enable
- ip dhcp-relay fwd-path {A.B.C.D} mode bootp
- ip dhcp-relay fwd-path {A.B.C.D} mode bootp_dhcp
- ip dhcp-relay fwd-path {A.B.C.D} mode dhcp
- ip dhcp-relay fwd-path {A.B.C.D} vrid <1-255>
- ip dhcp-relay max-hop <1-16>
- ip dhcp-relay min-sec <0-65535>
- ip dhcp-relay mode { bootp | dhcp | bootp_dhcp }
- ip dhcp-relay remoteId
- ip dhcp-relay trusted
- no ip dhcp-relay

- `no ip dhcp-relay broadcast`
- `no ip dhcp-relay circuitId`
- `no ip dhcp-relay fwd-path {A.B.C.D}`
- `no ip dhcp-relay fwd-path {A.B.C.D} vrid <1-255>`
- `no ip dhcp-relay remoteId`
- `no ip dhcp-relay trusted`

Default

None

Command mode

MLT Interface Configuration

Command parameters

Parameter	Description
`{A.B.C.D}`	Creates a forwarding path to the DHCP server with a mode and a state. A.B.C.D is the IP address of the server. The default IP address of the relay is the address of the interface. Tip: If the relay is a Virtual Router configured on this interface, you must set the vrid.
`broadcast`	Enables the device to send the server reply as a broadcast to the end station. After you disable this variable, the device sends the server reply as a unicast to the end station.
`circuitId`	Enables the device to insert the Option 82 Circuit ID into the packets sent to the server (enables DHCP Option 82).
`max-hop <1-16>`	Configures the maximum number of hops before a BootP/DHCP packet is discarded (1-16). The default is 4.
`min-sec <0-65535>`	Configures the minimum seconds count for DHCP. If the secs field in the BootP/DHCP packet header is greater than this value, the device relays or forwards the packet; otherwise, the packet is dropped (0-65535). The default is 0 seconds.
`mode <bootp|dhcp|bootp_dhcp>`	Configures DHCP mode to forward BootP messages only, DHCP messages only, or both. The default is both.
`remoteId`	Enables the device to insert the Option 82 Remote ID into the packets sent to the server (enables DHCP Option 82).
`trusted`	Configures the circuit as trusted in an Option 82 context.

©Avaya Inc. 2015 All Rights Reserved.

ip dhcp-relay (for a port)

Configure Dynamic Host Configuration Protocol (DHCP) Relay on an interface. The command no ip dhcp-relay disables DHCP Relay but does not delete the DHCP entry.

Syntax

- `default ip dhcp-relay`
- `default ip dhcp-relay broadcast`
- `default ip dhcp-relay circuitId`
- `default ip dhcp-relay max-hop`
- `default ip dhcp-relay min-sec`
- `default ip dhcp-relay mode`
- `default ip dhcp-relay remoteId`
- `default ip dhcp-relay trusted`
- `ip dhcp-relay`
- `ip dhcp-relay broadcast`
- `ip dhcp-relay circuitId`
- `ip dhcp-relay max-hop <1-16>`
- `ip dhcp-relay min-sec <0-65535>`
- `ip dhcp-relay mode { bootp | dhcp | bootp_dhcp }`
- `ip dhcp-relay remoteId`
- `ip dhcp-relay trusted`
- `no ip dhcp-relay`
- `no ip dhcp-relay broadcast`
- `no ip dhcp-relay circuitId`
- `no ip dhcp-relay remoteId`
- `no ip dhcp-relay trusted`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
broadcast	Enables the device to send the server reply as a broadcast to the end station. After you disable this variable, the device sends the server reply as a unicast to the end station.
circuitId	Enables the device to insert the Option 82 Circuit ID into the packets sent to the server (enables DHCP Option 82). The default is disabled.
max-hop <1-16>	Configures the maximum number of hops before a BootP/DHCP packet is discarded (1-16). The default is 4.
min-sec <0-65535>	Configures the minimum seconds count for Dynamic Host Configuration Protocol (DHCP). If the secs field in the BootP/DHCP packet header is greater than this value, the device relays or forwards the packet; otherwise, the packet is dropped (0- 65535). The default is 0 seconds.
mode <bootp|dhcp|bootp_dhcp>	Configures DHCP mode to forward BootP messages only, Dynamic Host Configuration Protocol (DHCP) messages only, or both. The default is both.
remoteId	Enables the device to insert the Option 82 Remote ID into the packets sent to the server (enables DHCP Option 82). The default is disabled.
trusted	Configures the circuit as trusted in an Option 82 context.

©Avaya Inc. 2015 All Rights Reserved.

ip dhcp-relay (for a VLAN)

Configure Dynamic Host Configuration Protocol (DHCP) Relay on an interface. The command no ip dhcp-relay disables DHCP Relay but does not delete the DHCP entry.

Syntax

- default ip dhcp-relay broadcast
- default ip dhcp-relay circuitId
- default ip dhcp-relay fwd-path {A.B.C.D}
- default ip dhcp-relay fwd-path {A.B.C.D} mode
- default ip dhcp-relay fwd-path {A.B.C.D} vrid <1-255>
- default ip dhcp-relay max-hop
- default ip dhcp-relay min-sec
- default ip dhcp-relay mode
- default ip dhcp-relay remoteId
- default ip dhcp-relay trusted
- ip dhcp-relay broadcast
- ip dhcp-relay circuitId
- ip dhcp-relay fwd-path {A.B.C.D}
- ip dhcp-relay fwd-path {A.B.C.D} disable
- ip dhcp-relay fwd-path {A.B.C.D} enable
- ip dhcp-relay fwd-path {A.B.C.D} mode bootp
- ip dhcp-relay fwd-path {A.B.C.D} mode bootp_dhcp
- ip dhcp-relay fwd-path {A.B.C.D} mode dhcp
- ip dhcp-relay fwd-path {A.B.C.D} vrid <1-255>
- ip dhcp-relay max-hop <1-16>
- ip dhcp-relay min-sec <0-65535>
- ip dhcp-relay mode { bootp | dhcp | bootp_dhcp }
- ip dhcp-relay remoteId
- ip dhcp-relay trusted
- no ip dhcp-relay

- `no ip dhcp-relay broadcast`
- `no ip dhcp-relay circuitId`
- `no ip dhcp-relay fwd-path {A.B.C.D}`
- `no ip dhcp-relay fwd-path {A.B.C.D} vrid <1-255>`
- `no ip dhcp-relay remoteId`
- `no ip dhcp-relay trusted`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`{A.B.C.D}`	Creates a forwarding path to the DHCP server with a mode and a state. A.B.C.D is the IP address of the server. The default IP address of the relay is the address of the interface. Tip: If the relay is a Virtual Router configured on this interface, you must set the vrid.
`broadcast`	Enables the device to send the server reply as a broadcast to the end station. After you disable this variable, the device sends the server reply as a unicast to the end station.
`circuitId`	Enables the device to insert the Option 82 Circuit ID into the packets sent to the server (enables DHCP Option 82).
`max-hop <1-16>`	Configures the maximum number of hops before a BootP/DHCP packet is discarded (1-16). The default is 4.
`min-sec <0-65535>`	Configures the minimum seconds count for DHCP. If the secs field in the BootP/DHCP packet header is greater than this value, the device relays or forwards the packet; otherwise, the packet is dropped (0-65535). The default is 0 seconds.
`mode <bootp|dhcp|bootp_dhcp>`	Configures DHCP mode to forward BootP messages only, DHCP messages only, or both. The default is both.
`remoteId`	Enables the device to insert the Option 82 Remote ID into the packets sent to the server (enables DHCP Option 82).
`trusted`	Configures the circuit as trusted in an Option 82 context.

©Avaya Inc. 2015 All Rights Reserved.

ip dhcp-relay fwd-path

Create the forwarding path from the client to the server.

Syntax

- `ip dhcp-relay fwd-path <A.B.C.D> <A.B.C.D>`
- `no ip dhcp-relay fwd-path <A.B.C.D> <A.B.C.D>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`fwd-path <A.B.C.D> <A.B.C.D>`	Configures the forwarding path from the client to the server. A.B.C.D is the IP address configured on an interface (a locally configured IP address) to forward or relay BootP or Dynamic Host Configuration Protocol (DHCP). The relay can also be a VRRP address. A.B.C.D is the IP address of the DHCP server in the network. If this IP address corresponds to the locally configured IP network, the DHCP packet is broadcast out from the interface.

©Avaya Inc. 2015 All Rights Reserved.

ip dhcp-relay fwd-path enable

Enable the forwarding path from the client to the server.

Syntax

- `ip dhcp-relay fwd-path <A.B.C.D> <A.B.C.D> enable`

Default

`The ip dhcp-relay fwd-path default state is disabled.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`disable`	Disables Dynamic Host Configuration Protocol (DHCP) relaying on the path from the IP address to the server.
`fwd-path <A.B.C.D> <A.B.C.D> enable`	Enables Dynamic Host Configuration Protocol (DHCP) relaying on the path from the IP address to the server. A.B.C.D is the IP address configured on an interface (a locally configured IP address). A.B.C.D is the IP address of the DHCP server in the network. If this IP address corresponds to the locally configured IP network, the DHCP packet is broadcast out from the interface.

©Avaya Inc. 2015 All Rights Reserved.

ip dhcp-relay fwd-path (for a port)

Create the forwarding path from the client to the server.

Syntax

- `default ip dhcp-relay fwd-path {A.B.C.D}`
- `default ip dhcp-relay fwd-path {A.B.C.D} vrid <1-255>`
- `ip dhcp-relay fwd-path {A.B.C.D}`
- `ip dhcp-relay fwd-path {A.B.C.D} disable`
- `ip dhcp-relay fwd-path {A.B.C.D} enable`
- `ip dhcp-relay fwd-path {A.B.C.D} vrid <1-255>`
- `no ip dhcp-relay fwd-path {A.B.C.D}`
- `no ip dhcp-relay fwd-path {A.B.C.D} vrid <1-255>`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`{A.B.C.D}`	Creates a forwarding path to the Dynamic Host Configuration Protocol (DHCP) server. A.B.C.D is the IP address of the server. The default IP address of the relay is the address of the interface. Tip: If the relay is a virtual router configured on this interface, you must set the vrid.
`disable`	Disables the forwarding path.
`enable`	Enables the forwarding path.
`vrid <1-255>`	Specifies the virtual router ID. The virtual router acts as the default router for one or more associated addresses.

©Avaya Inc. 2015 All Rights Reserved.

ip dhcp-relay fwd-path mode

Modify Dynamic Host Configuration Protocol (DHCP) mode to forward BootP messages only, DHCP messages only, or both.

Syntax

- `ip dhcp-relay fwd-path <A.B.C.D> <A.B.C.D> mode <bootp|bootp-dhcp|dhcp>`

Default

`The default mode is both.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`fwd-path <A.B.C.D> <A.B.C.D> mode <bootp|bootp-dhcp|dhcp>`	Modifies Dynamic Host Configuration Protocol (DHCP) mode to forward BootP messages only, DHCP messages only, or both. The default is both. mode is {bootp | bootp_dhcp | dhcp}.

©Avaya Inc. 2015 All Rights Reserved.

ip dhcp-relay fwd-path mode (for a port)

Modify Dynamic Host Configuration Protocol (DHCP) mode to forward BootP messages only, DHCP messages only, or both.

Syntax

- `default ip dhcp-relay fwd-path {A.B.C.D} mode`
- `ip dhcp-relay fwd-path {A.B.C.D} mode bootp`
- `ip dhcp-relay fwd-path {A.B.C.D} mode bootp_dhcp`
- `ip dhcp-relay fwd-path {A.B.C.D} mode dhcp`

Default

`The default mode is both.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`mode <bootp|dhcp|bootp_dhcp>`	Configures DHCP mode to forward BootP messages only, Dynamic Host Configuration Protocol (DHCP) messages only, or both. The default is both.

©Avaya Inc. 2015 All Rights Reserved.

ip dhcp-relay (loopback)

Configure Dynamic Host Configuration Protocol (DHCP) Relay on an interface. The command no ip dhcp-relay disables DHCP Relay but does not delete the DHCP entry.

Syntax

- `default ip dhcp-relay broadcast`
- `default ip dhcp-relay circuitId`
- `default ip dhcp-relay fwd-path {A.B.C.D}`
- `default ip dhcp-relay fwd-path {A.B.C.D} mode`
- `default ip dhcp-relay fwd-path {A.B.C.D} vrid <1-255>`
- `default ip dhcp-relay max-hop`
- `default ip dhcp-relay min-sec`
- `default ip dhcp-relay mode`
- `default ip dhcp-relay remoteId`
- `default ip dhcp-relay trusted`
- `ip dhcp-relay broadcast`
- `ip dhcp-relay circuitId`
- `ip dhcp-relay fwd-path {A.B.C.D}`
- `ip dhcp-relay fwd-path {A.B.C.D} disable`
- `ip dhcp-relay fwd-path {A.B.C.D} enable`
- `ip dhcp-relay fwd-path {A.B.C.D} mode bootp`
- `ip dhcp-relay fwd-path {A.B.C.D} mode bootp_dhcp`
- `ip dhcp-relay fwd-path {A.B.C.D} mode dhcp`
- `ip dhcp-relay fwd-path {A.B.C.D} vrid <1-255>`
- `ip dhcp-relay max-hop <1-16>`
- `ip dhcp-relay min-sec <0-65535>`
- `ip dhcp-relay mode { bootp | dhcp | bootp_dhcp }`
- `ip dhcp-relay remoteId`
- `ip dhcp-relay trusted`
- `no ip dhcp-relay`

- `no ip dhcp-relay broadcast`
- `no ip dhcp-relay circuitId`
- `no ip dhcp-relay fwd-path {A.B.C.D}`
- `no ip dhcp-relay fwd-path {A.B.C.D} vrid <1-255>`
- `no ip dhcp-relay remoteId`
- `no ip dhcp-relay trusted`

Default

None

Command mode

Loopback Interface Configuration

Command parameters

Parameter	Description
`{A.B.C.D}`	Creates a forwarding path to the DHCP server with a mode and a state. A.B.C.D is the IP address of the server. The default IP address of the relay is the address of the interface. Tip: If the relay is a Virtual Router configured on this interface, you must set the vrid.
`broadcast`	Enables the device to send the server reply as a broadcast to the end station. After you disable this variable, the device sends the server reply as a unicast to the end station.
`circuitId`	Enables the device to insert the Option 82 Circuit ID into the packets sent to the server (enables DHCP Option 82).
`max-hop <1-16>`	Configures the maximum number of hops before a BootP/DHCP packet is discarded (1-16). The default is 4.
`min-sec <0-65535>`	Configures the minimum seconds count for DHCP. If the secs field in the BootP/DHCP packet header is greater than this value, the device relays or forwards the packet; otherwise, the packet is dropped (0-65535). The default is 0 seconds.
`mode <bootp|dhcp|bootp_dhcp>`	Configures DHCP mode to forward BootP messages only, DHCP messages only, or both. The default is both.
`remoteId`	Enables the device to insert the Option 82 Remote ID into the packets sent to the server (enables DHCP Option 82).
`trusted`	Configures the circuit as trusted in an Option 82 context.

©Avaya Inc. 2015 All Rights Reserved.

ip directed-broadcast (for a port)

Configure the device to forward directed broadcasts for a VLAN.

Syntax

- `default ip directed-broadcast`
- `default ip directed-broadcast enable`
- `ip directed-broadcast`
- `ip directed-broadcast enable`
- `no ip directed-broadcast`
- `no ip directed-broadcast enable`

Default

`The default is enabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Allows the device to forward directed broadcast frames to the specified VLAN. The default setting for this feature is enabled.

©Avaya Inc. 2015 All Rights Reserved.

ip directed-broadcast (for a VLAN)

Configure the device to forward directed broadcasts for a VLAN.

Syntax

- `default ip directed-broadcast`
- `default ip directed-broadcast enable`
- `ip directed-broadcast`
- `ip directed-broadcast enable`
- `no ip directed-broadcast`
- `no ip directed-broadcast enable`

Default

`The default is enabled.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`enable`	Allows the device to forward directed broadcast frames to the specified VLAN. The default setting for this feature is enabled.

©Avaya Inc. 2015 All Rights Reserved.

ip domain-name

Configure the Domain Name Service (DNS) to establish the mapping between a name and an IP address.

Syntax

- `default ip domain-name`
- `ip domain-name WORD<0-255>`
- `no ip domain-name`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
WORD<0-255>	Configures the default domain name.

©Avaya Inc. 2015 All Rights Reserved.

ip ecmp

Enable Equal Cost Multipath protocol (ECMP). If the ECMP parameter is disabled, all existing ECMP routes are removed. When ECMP is enabled, all ECMP routes are re-added.

Syntax

- `default ip ecmp`
- `default ip ecmp max-path`
- `ip ecmp`
- `ip ecmp max-path <1-8>`
- `ip ecmp pathlist-1 WORD<0-64>`
- `ip ecmp pathlist-2 WORD<0-64>`
- `ip ecmp pathlist-3 WORD<0-64>`
- `ip ecmp pathlist-4 WORD<0-64>`
- `ip ecmp pathlist-5 WORD<0-64>`
- `ip ecmp pathlist-6 WORD<0-64>`
- `ip ecmp pathlist-7 WORD<0-64>`
- `ip ecmp pathlist-8 WORD<0-64>`
- `no ip ecmp`
- `no ip ecmp pathlist-1`
- `no ip ecmp pathlist-2`
- `no ip ecmp pathlist-3`
- `no ip ecmp pathlist-4`
- `no ip ecmp pathlist-5`
- `no ip ecmp pathlist-6`
- `no ip ecmp pathlist-7`
- `no ip ecmp pathlist-8`

Default

`The default is disabled.`

Command mode

Global Configuration

Command parameters

Parameter	Description
max-path <1-8>	Configures the maximum number of Equal Cost Multipath (ECMP) paths.
pathlist-1 WORD<0-64>	Configures one equal-cost path to the same destination prefix. To remove the policy, enter a blank string. To configure this parameter, you must globally enable Equal Cost Multipath (ECMP).
pathlist-2 WORD<0-64>	Configures up to two equal-cost paths to the same destination prefix. To remove the policy, enter a blank string. To configure this parameter, you must globally enable Equal Cost Multipath (ECMP).
pathlist-3 WORD<0-64>	Configures up to three equal-cost paths to the same destination prefix. To remove the policy, enter a blank string. To configure this parameter, you must globally enable Equal Cost Multipath (ECMP).
pathlist-4 WORD<0-64>	Configures up to four equal-cost paths to the same destination prefix. To remove the policy, enter a blank string. To configure this parameter, you must globally enable Equal Cost Multipath (ECMP).
pathlist-5 WORD<0-64>	Configures up to five equal-cost paths to the same destination prefix. To remove the policy, enter a blank string. To configure this parameter, you must globally enable Equal Cost Multipath (ECMP).
pathlist-6 WORD<0-64>	Configures up to six equal-cost paths to the same destination prefix. To remove the policy, enter a blank string. To configure this parameter, you must globally enable Equal Cost Multipath (ECMP).
pathlist-7 WORD<0-64>	Configures up to seven equal-cost paths to the same destination prefix. To remove the policy, enter a blank string. To configure this parameter, you must globally enable Equal Cost Multipath (ECMP).
pathlist-8 WORD<0-64>	Configures up to eight equal-cost paths to the same destination prefix. To remove the policy, enter a blank string. To configure this parameter, you must globally enable Equal Cost Multipath (ECMP).

©Avaya Inc. 2015 All Rights Reserved.

ip ecmp pathlist-apply

Apply changes to all Equal Cost Multipath (ECMP) pathlist configurations.

Syntax

- `ip ecmp pathlist-apply`
- `ip ecmp pathlist-apply vrf WORD<1-16>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`pathlist-apply`	Apply changes to all Equal Cost Multipath (ECMP) pathlist configurations.
`vrf WORD<1-16>`	Apply changes to all Equal Cost Multipath (ECMP) pathlist configurations for a particular VRF.

©Avaya Inc. 2015 All Rights Reserved.

ip extcommunity-list

Use community lists to specify permitted routes by BGP extended community attributes, including route targets and sites of origin (SOO). This list acts as a filter that Match route targets and SOO.

Syntax

- `ip extcommunity-list <1-1024> memberid <0-65535>`
- `ip extcommunity-list <1-1024> memberid <0-65535> rt <0-65535> <0-2147483647>`
- `ip extcommunity-list <1-1024> memberid <0-65535> rt {A.B.C.D} <0-65535>`
- `ip extcommunity-list <1-1024> memberid <0-65535> soo <0-65535> <0-2147483647>`
- `ip extcommunity-list <1-1024> memberid <0-65535> soo {A.B.C.D} <0-65535>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`memberId <0-65535>`	Specifies an integer value between 0 and 65535 that represents the member ID in the community list.
`rt <0-65536> <0-2147483647> rt <A.B.C.D> <0-65535>`	Specifies the route target in the format {AS number: assigned number} (that is, {0 to 65535}:{0 to 2147483647}) or {ipaddress: assigned number} (that is, {a.b.c.d}:{0 to 65535}).
`soo <0-65535> <0-2147483647> soo <A.B.C.D> <0-65535>`	Specifies the site of origin in the format {AS number: assigned number} (that is, {0 to 65535}:{0 to 2147483647}) or {ipaddress: assigned number} (that is, {a.b.c.d}:{0 to 65535}).

©Avaya Inc. 2015 All Rights Reserved.

ip forward-protocol udp

Configure UDP protocols to determine which UDP broadcasts are forwarded

Syntax

- `default ip forward-protocol udp`
- `ip forward-protocol udp`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-65535>	Creates a new UDP protocol. <1-65535> is the UDP protocol port number.
WORD<1-15>	Specifies the UDP protocol name as a string.

©Avaya Inc. 2015 All Rights Reserved.

ip forward-protocol udp broadcastmask

Configure the broadcast mask on the IP forwarding list.

Syntax

- `default ip forward-protocol udp broadcastmask`
- `default ip forward-protocol udp broadcastmask {A.B.C.D}`
- `ip forward-protocol udp broadcastmask {A.B.C.D}`
- `ip forward-protocol udp vlan <1-4084> broadcastmask {A.B.C.D}`
- `no ip forward-protocol udp broadcastmask`
- `no ip forward-protocol udp broadcastmask {A.B.C.D}`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`<A.B.C.D>`	Sets the interface broadcast mask (the interface broadcast mask can be different from the interface mask). A.B.C.D is an IP address in a.b.c.d format.

©Avaya Inc. 2015 All Rights Reserved.

ip forward-protocol udp maxttl

Set the maximum time to live.

Syntax

- `default ip forward-protocol udp maxttl`
- `default ip forward-protocol udp maxttl <1-16>`
- `ip forward-protocol udp maxttl <1-16>`
- `ip forward-protocol udp vlan <1-4084> maxttl <1-16>`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`maxttl <1-16>`	Sets the maximum time-to-live value (TTL) for the UDP broadcast forwarded by the interface. The range is 1 to 16.

©Avaya Inc. 2015 All Rights Reserved.

ip forward-protocol udp (on a VLAN)

Configure UDP protocols to determine which UDP broadcasts are forwarded

Syntax

- `default ip forward-protocol udp`
- `default ip forward-protocol udp vlan <1-4084>`
- `ip forward-protocol udp`
- `no ip forward-protocol udp`
- `no ip forward-protocol udp vlan <1-4084>`

Default

None

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip forward-protocol udp portfwd

Configure a UDP port forward entry to add or remove a port forward entry.

Syntax

- `ip forward-protocol udp portfwd <1-65535> {A.B.C.D}`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
{A.B.C.D}	A.B.C.D is an IP address in a.b.c.d format.
<1-65535>	Adds a UDP protocol port to the specified port forwarding list. 1-65535 is a UDP protocol port in the range of 1 to 65535.

©Avaya Inc. 2015 All Rights Reserved.

ip forward-protocol udp portfwdlist

Configure the UDP port forwarding list.

Syntax

- `ip forward-protocol udp portfwdlist <1-1000>`
- `ip forward-protocol udp portfwdlist <1-1000> <1-65535>`
- `ip forward-protocol udp portfwdlist <1-1000> <1-65535> {A.B.C.D}`
- `ip forward-protocol udp portfwdlist <1-1000> name WORD<0-15>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
{A.B.C.D}	A.B.C.D is an IP address in a.b.c.d format.
<1-1000>	Creates a UDP port forwarding list in the range of 1 to 1000.
<1-65535>	Adds a UDP protocol port to the specified port forwarding list. 1-65535 is a UDP protocol port in the range of 1 to 65535.
name WORD<0-15>	Specifies a name.

©Avaya Inc. 2015 All Rights Reserved.

ip forward-protocol udp portfwdlist (on a VLAN)

Configure the UDP port forwarding list.

Syntax

- `ip forward-protocol udp portfwdlist <1-1000>`
- `ip forward-protocol udp portfwdlist <1-1000> broadcastmask {A.B.C.D}`
- `ip forward-protocol udp portfwdlist <1-1000> broadcastmask {A.B.C.D} maxttl <1-16>`
- `ip forward-protocol udp portfwdlist <1-1000> maxttl <1-16>`
- `no ip forward-protocol udp portfwdlist`
- `no ip forward-protocol udp portfwdlist <1-1000>`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`<1-1000>`	Creates a UDP port forwarding list in the range of 1 to 1000.
`broadcastmask {A.B.C.D}`	Configures the broadcast mask, which may be different from the interface mask. A.B.C.D is an IP address in a.b.c.d format.
`maxttl <1-16>`	Configures the maximum time-to-live (TTL) for this interface.
`name WORD<0-15>`	Specifies a name.

©Avaya Inc. 2015 All Rights Reserved.

ip icmp

Enable Internet Control Message Protocol (ICMP) redirect and unreachable messages.

Syntax

- `default ip icmp redirect`
- `default ip icmp unreachable`
- `ip icmp redirect`
- `ip icmp unreachable`
- `no ip icmp redirect`
- `no ip icmp unreachable`

Default

`The default is disabled.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`redirect`	Enables the switch to send Internet Control Message Protocol (ICMP) destination redirect messages.
`unreachable`	Enables the switch to send Internet Control Message Protocol (ICMP) unreachable messages. When enabled, generates Internet Control Message Protocol (ICMP) network unreachable messages if the destination network is not reachable from this router. These messages help determine if the routing switch is reachable over the network. The default is disabled.

©Avaya Inc. 2015 All Rights Reserved.

ip igmp access-list (for a port)

Configure multicast access control for a Internet Group Management Protocol (IGMP) Ethernet port to restrict access to certain multicast streams and to protect multicast streams from spoofing (injecting data to the existing streams).

Syntax

- `default ip igmp access-list WORD<1-64> {A.B.C.D/X}`
- `ip igmp access-list WORD<1-64> {A.B.C.D/X} { deny-tx | deny-rx | deny-both | allow-only-tx | allow-only-rx | allow-only-both }`
- `no ip igmp access-list WORD<1-64> {A.B.C.D/X}`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
{A.B.C.D/X}	Creates an access control group entry for a specific Internet Group Management Protocol (IGMP) interface. Specifies the IP address of the host and the subnet mask used to determine the host or hosts covered by this configuration. You can use the host subnet mask to restrict access to a portion of the network for the host.
deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both	Indicates the action for the specified Internet Group Management Protocol (IGMP) interface. For example, if you specify deny-both, the interface denies both transmitted and received traffic
WORD<1-64>	Specifies the name of the access list from 1-64 characters.

©Avaya Inc. 2015 All Rights Reserved.

ip igmp access-list (for a VLAN)

Configure multicast access control for a VLAN to restrict access to certain multicast streams and to protect multicast streams from spoofing (injecting data to the existing streams).

Syntax

- `default ip igmp access-list WORD<1-64> {A.B.C.D/X}`
- `ip igmp access-list WORD<1-64> {A.B.C.D/X} <deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both>`
- `no ip igmp access-list WORD<1-64> {A.B.C.D/X}`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
{A.B.C.D/X}	Creates an access control group entry for a specific Internet Group Management Protocol (IGMP) interface. Specify the IP address of the host and the subnet mask used to determine the host or hosts covered by this configuration. You can use the host subnet mask to restrict access to a portion of the network for the host.
deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both	Indicates the action for the specified Internet Group Management Protocol (IGMP) interface. For example, if you specify deny-both, the interface denies both transmitted and received traffic.
WORD<1-64>	Specifies the name of the access list from 1-64 characters.

©Avaya Inc. 2015 All Rights Reserved.

ip igmp access-list mode (for a port)

Change an existing access list on the Ethernet port.

Syntax

- `default ip igmp access-list WORD<1-64> {A.B.C.D/X}`
- `ip igmp access-list WORD<1-64> {A.B.C.D/X} mode { deny-tx | deny-rx | deny-both | allow-only-tx | allow-only-rx | allow-only-both }`
- `no ip igmp access-list WORD<1-64> {A.B.C.D/X}`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
{A.B.C.D/X}	Creates an access control group entry for a specific Internet Group Management Protocol (IGMP) interface. Specify the IP address of the host and the subnet mask used to determine the host or hosts covered by this configuration. You can use the host subnet mask to restrict access to a portion of the network for the host.
deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both	Indicates the action for the specified Internet Group Management Protocol (IGMP) interface. For example, if you specify deny-both, the interface denies both transmitted and received traffic
WORD<1-64>	Specifies the name of the access list from 1-64 characters.

©Avaya Inc. 2015 All Rights Reserved.

ip igmp access-list mode (for a VLAN)

Change an existing access list on the VLAN interface.

Syntax

- `default ip igmp access-list WORD<1-64> {A.B.C.D/X}`
- `ip igmp access-list WORD<1-64> {A.B.C.D/X} mode <deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both`
- `no ip igmp access-list WORD<1-64> {A.B.C.D/X}`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
{A.B.C.D/X}	Creates an access control group entry for a specific Internet Group Management Protocol (IGMP) interface. Specify the IP address of the host and the subnet mask used to determine the host or hosts covered by this configuration. You can use the host subnet mask to restrict access to a portion of the network for the host.
deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both	Indicates the action for the specified Internet Group Management Protocol (IGMP) interface. For example, if you specify deny-both, the interface denies both transmitted and received traffic
WORD<1-64>	Specifies the name of the access list from 1-64 characters.

©Avaya Inc. 2015 All Rights Reserved.

ip igmp flush port

Use this command to flush Internet Group Management Protocol (IGMP) group members on a port.

Syntax

- `ip igmp flush port {slot/port [-slot/port] [,...]} grp-member`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port] [,...]}`	Specifies the port list.
`grp-member`	Specifies a group member.

©Avaya Inc. 2015 All Rights Reserved.

ip igmp flush vlan

Use this command to flush Internet Group Management Protocol (IGMP) group members, the multicast router and senders.

Syntax

- `ip igmp flush vlan <1-4084> grp-member`
- `ip igmp flush vlan <1-4084> mrouter`
- `ip igmp flush vlan <1-4084> sender`
- `ip igmp flush vlan <1-4084> sender {A.B.C.D}`
- `ip igmp flush vlan <1-4084>sender {A.B.C.D} {A.B.C.D}`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<1-4084>`	Specifies the VLAN ID.
`grp-member`	Specifies a group member.
`mrouter`	Specifies a multicast router.
`sender {A.B.C.D}`	Specifies a sender. The first IP address specifies the source IP address of the sender.
`sender {A.B.C.D} {A.B.C.D}`	Specifies a sender. The first IP address specifies the source IP address of the sender. The second IP address specifies the group IP address of the sender.

©Avaya Inc. 2015 All Rights Reserved.

ip igmp (for an port)

Configure Internet Group Management Protocol (IGMP) for each interface to change default multicasting operations.

Syntax

- `default ip igmp`
- `default ip igmp compatibility-mode`
- `default ip igmp dynamic-downgrade-version`
- `default ip igmp last-member-query-interval`
- `default ip igmp port {slot/port[-slot/port][,...]}`
- `default ip igmp query-interval`
- `default ip igmp query-max-response`
- `default ip igmp robust-value`
- `default ip igmp router-alert`
- `default ip igmp version`
- `ip igmp compatibility-mode`
- `ip igmp dynamic-downgrade-version`
- `ip igmp last-member-query-interval <0-255>`
- `ip igmp port {slot/port[-slot/port][,...]}`
- `ip igmp query-interval <1-65535>`
- `ip igmp query-max-response <0-255>`
- `ip igmp robust-value <2-255>`
- `ip igmp router-alert`
- `ip igmp version <1-3>`
- `no ip igmp`
- `no ip igmp compatibility-mode`
- `no ip igmp dynamic-downgrade-version`
- `no ip igmp port {slot/port[-slot/port][,...]}`
- `no ip igmp router-alert`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
compatibility-mode	Activates v2-v3 compatibility mode. The default value is disabled, which means IGMPv3 is not compatible with IGMPv2.
dynamic-downgrade-version	Configures if the system downgrades the version of Internet Group Management Protocol (IGMP) to handle older query messages. If the system downgrades, the host with IGMPv3 only capability does not work. If you do not configure the system to downgrade the version of IGMP, the system logs a warning. The default is enabled.
last-member-query-interval <0-255>	Configures the maximum response time (in tenths of a second) inserted into group-specific queries sent in response to leave group messages. This value is also the time between group-specific query messages. You cannot configure this value for IGMPv1. Decreasing the value reduces the time to detect the loss of the last member of a group. Avaya recommends that you configure this value between 3-10 (equal to 0.3 - 1.0 seconds). The default is 10 tenths of a second.
port {slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
query-interval <1-65535>	Configures the frequency (in seconds) at which the VLAN transmits host query packets. The default is 125 seconds.
query-max-response <0-255>	Configures the maximum response time (in tenths of a second) advertised in IGMPv2 general queries on this interface. You cannot configure this value for IGMPv1. Smaller values allow a router to prune groups faster. Important: You must configure this value lower than the query-interval. The default is 100 tenths of a second (equal to 10 seconds).
robust-value <2-255>	Configures the expected packet loss of a network. Increase the value if you expect the network to experience packet loss. The default is 2 seconds.
router-alert	Instructs the router to ignore Internet Group Management Protocol (IGMP) packets that do not contain the router alert IP option. When disabled (default configuration), the router processes IGMP packets regardless of the status of the router alert IP option. Important To maximize network performance, Avaya recommends that you configure this parameter according to the version of IGMP currently in use: IGMPv1-Disable IGMPv2-Enable IGMPv3-Enable. The default is disabled.
version <1-3>	Configures the version of IGMP that you want to configure on this interface. For IGMP to function correctly, all routers on a LAN must use the same version. The default is 2 (IGMPv2).

©Avaya Inc. 2015 All Rights Reserved.

ip igmp (for a VLAN)

Configure Internet Group Management Protocol (IGMP) for each interface to change default multicasting operations.

Syntax

- `default ip igmp compatibility-mode`
- `default ip igmp dynamic-downgrade-version`
- `default ip igmp last-member-query-interval`
- `default ip igmp mrouter`
- `default ip igmp proxy`
- `default ip igmp query-interval`
- `default ip igmp query-max-response`
- `default ip igmp robust-value`
- `default ip igmp router-alert`
- `default ip igmp snooping`
- `default ip igmp ssm-snoop`
- `default ip igmp version`
- `ip igmp compatibility-mode`
- `ip igmp dynamic-downgrade-version`
- `ip igmp last-member-query-interval <0-255>`
- `ip igmp mrouter {slot/port[-slot/port][,...]}`
- `ip igmp proxy`
- `ip igmp query-interval <1-65535>`
- `ip igmp query-max-response <0-255>`
- `ip igmp robust-value <2-255>`
- `ip igmp router-alert`
- `ip igmp snooping`
- `ip igmp ssm-snoop`
- `ip igmp version <1-3>`
- `no ip igmp compatibility-mode`
- `no ip igmp dynamic-downgrade-version`

- `no ip igmp mrouter {slot/port[-slot/port][,...]}`
- `no ip igmp proxy`
- `no ip igmp router-alert`
- `no ip igmp snooping`
- `no ip igmp ssm-snoop`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`compatibility-mode`	Activates v2-v3 compatibility mode. The default value is disabled, which means IGMPv3 is not compatible with IGMPv1 or IGMPv2.
`dynamic-downgrade-version`	Configures if the system downgrades the version of Internet Group Management Protocol (IGMP) to handle older query messages. If the system downgrades, the host with IGMPv3 only capability does not work. If you do not configure the system to downgrade the version of IGMP, the system logs a warning. The default is enabled.
`last-member-query-interval <0-255>`	Configures the maximum response time (in tenths of a second) inserted into group-specific queries sent in response to leave group messages. This value is also the time between group-specific query messages. You cannot configure this value for IGMPv1. Decreasing the value reduces the time to detect the loss of the last member of a group. Avaya recommends that you configure this value between 3-10 (equal to 0.3 - 1.0 seconds). The default is 10 tenths of a second.
`mrouter {slot/port[-slot/port][,...]}`	Adds multicast router ports. {slot/port[-slot/port][,...]} identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`proxy`	Activates the proxy-snoop option globally for the VLAN. The default is disabled.
`query-interval <1-65535>`	Configures the frequency (in seconds) at which the VLAN transmits host query packets. The default is 125 seconds.
`query-max-response <0-255>`	Configures the maximum response time (in tenths of a second) advertised in IGMPv2 general queries on this interface. You cannot configure this value for IGMPv1. Smaller values allow a router to prune groups faster. Important: You must configure this value lower than the query-interval.
`robust-value <2-255>`	Configures the expected packet loss of a network. Increase the value if you expect the network to experience packet loss. The default is 2 seconds.
`router-alert`	Instructs the router to ignore Internet Group Management Protocol (IGMP) packets that do not contain the router alert IP option. When disabled (default configuration), the router processes IGMP packets regardless of the status of the router alert IP option. Important: To maximize network performance, Avaya recommends that you configure this parameter according to the version of IGMP currently in use: IGMPv1-Disable IGMPv2-Enable IGMPv3-Enable. The default is disabled.
`snooping`	Activates the snoop option for the VLAN. The default is disabled.
`ssm-snoop`	Activates support for PIM-SSM on the snoop interface. The default is disabled.
`version <1-3>`	Configures the version of IGMP that you want to configure on this interface. For IGMP to function correctly, all routers on a LAN must use the same

version. The default is 2 (IGMPv2).

©Avaya Inc. 2015 All Rights Reserved.

ip igmp generate-log (for a VRF)

Enables the generation of IGMP log messages.

Syntax

- `default ip igmp generate-log`
- `ip igmp generate-log`
- `no ip igmp generate-log`

Default

`The default is disabled.`

Command mode

VRF Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip igmp generate-trap (for a VRF)

Enables the generation of IGMP traps.

Syntax

- `default ip igmp generate-trap`
- `ip igmp generate-trap`
- `no ip igmp generate-trap`

Default

`The default is disabled.`

Command mode

VRF Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip igmp (globally)

Configure the Internet Group Management Protocol (IGMP) commands to establish and manage the multicast groups.

Syntax

- `default ip igmp ssm-map {A.B.C.D} {A.B.C.D}`
- `default ip igmp ssm-map {A.B.C.D} {A.B.C.D} [enable]`
- `ip igmp generate-log`
- `ip igmp generate-trap`
- `ip igmp immediate-leave-mode <multiple-user|one-user>`
- `ip igmp ssm [dynamic-learning] [group-range {A.B.C.D/X}]`
- `ip igmp ssm-map {A.B.C.D} {A.B.C.D} [enable]`
- `ip igmp ssm-map all`
- `no ip igmp ssm-map {A.B.C.D} {A.B.C.D}`
- `no ip igmp ssm-map {A.B.C.D} {A.B.C.D} [enable]`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`generate-log`	Sets the Internet Group Management Protocol (IGMP) log.
`generate-trap`	Sets the Internet Group Management Protocol (IGMP) trap.
`immediate-leave-mode <multiple-user|one-user`	Enables immediate leave mode to users which is either a single user or multiple users.
`ssm [dynamic-learning] [group-range {A.B.C.D/X}]`	Enables and sets the Source Specific Multicast (SSM) features. The parameter, dynamic-learning enables SSM dynamic learning. The parameter, group range {A.B.C.D/X} configures the range group address and mask. The SSM range parameter extends the default SSM range of 232/8 to include an IP multicast address. You can configure existing applications without having to change their group configurations. This parameter specifies an IP multicast address within the range of 224.0.0.0 and 239.255.255.255. The default is 232.0.0.0. The address mask is the IP address mask of the multicast group. The default is 255.0.0.0.
`ssm-map all`	Enables the Source Specific Multicast (SSM) map table for all static entries.

ssm-map{A.B.C.D} {A.B.C.D}[enable]	Enables the Source Specific Multicast (SSM) map table for a specific entry or creates a static entry for a specific group. The parameter, {A.B.C.D} {A.B.C.D} creates a static SSM channel table entry by specifying the group and source IP addresses. The first IP address is an IP multicast address within the SSM range. The second IP address is the source IP address and it is an IP host address that sends traffic to the group. The default for {A.B.C.D}{A.B.C.D} enable is enable for each entry. The default is enable for each entry.
ssm-map{A.B.C.D}[enable]	Enables the administrative state for a specific entry (group). This variable does not affect the dynamically-learned entries. This state determines whether the switch uses the static entry or saves it for future use. The default is enable for each entry.

©Avaya Inc. 2015 All Rights Reserved.

ip igmp igmpv3-explicit-host-tracking (for an Ethernet port)

Track all the source and group members. You must enable explicit-host-tracking to use fast leave for IGMPv3.

Syntax

- `default ip igmp igmpv3-explicit-host-tracking`
- `ip igmp igmpv3-explicit-host-tracking`
- `no ip igmp igmpv3-explicit-host-tracking`

Default

The default is disabled.

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip igmp igmpv3-explicit-host-tracking (for a VLAN)

Track all the source and group members. You must enable explicit-host-tracking to use fast leave for IGMPv3.

Syntax

- `default ip igmp igmpv3-explicit-host-tracking`
- `ip igmp igmpv3-explicit-host-tracking`
- `no ip igmp igmpv3-explicit-host-tracking`

Default

The default is disabled.

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip igmp immediate-leave (for an Ethernet port)

Enable fast (immediate) leave mode to specify if a port receives a leave message from a member of a group.

Syntax

- `default ip igmp immediate-leave`
- `ip igmp immediate-leave`
- `no ip igmp immediate-leave`

Default

None

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip igmp immediate-leave (for a VLAN)

Enable fast (immediate) leave mode to specify if a VLAN receives a leave message from a member of a group.

Syntax

- `default ip igmp immediate-leave`
- `ip igmp immediate-leave`
- `no ip igmp immediate-leave`

Default

None

Command mode

VLAN Interface Configuration

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

Home | Command modes | Alphabetical listing

ip igmp immediate-leave-members

Configure fast leave members on a VLAN to specify fast leave capable ports.

Syntax

- `default ip igmp immediate-leave-members {slot/port[-slot/port][,...]}`
- `ip igmp immediate-leave-members {slot/port[-slot/port][,...]}`
- `no ip igmp immediate-leave-members {slot/port[-slot/port][,...]}`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

ip igmp immediate-leave-mode (for a VRF)

Configures the fast leave mode.

Syntax

- `default ip igmp immediate-leave-mode multiple-user`
- `default ip igmp immediate-leave-mode one-user`
- `ip igmp immediate-leave-mode multiple-user`
- `ip igmp immediate-leave-mode one-user`
- `no ip igmp immediate-leave-mode multiple-user`
- `no ip igmp immediate-leave-mode one-user`

Default

`The default is multiple-user.`

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
`multiple-user`	Removes from the group only the IGMP member who sent the leave message. Traffic does not stop if other receivers exist on the interface port.
`one-user`	Removes all group members on a fast leave enabled interface port after receiving the first leave message from a member. This behavior is the same as the conventional fast leave process.

©Avaya Inc. 2015 All Rights Reserved.

ip igmp mrdisc

Configure the multicast route discovery options to enable the automatic discovery of multicast-capable routers.

Syntax

- `default ip igmp mrdisc`
- `default ip igmp mrdisc maxadvertinterval`
- `default ip igmp mrdisc maxinitadvertinterval`
- `default ip igmp mrdisc maxinitadvertisements`
- `default ip igmp mrdisc minadvertinterval`
- `default ip igmp mrdisc neighdeadinterval`
- `ip igmp mrdisc`
- `ip igmp mrdisc maxadvertinterval <2-180>`
- `ip igmp mrdisc maxinitadvertinterval <2-180>`
- `ip igmp mrdisc maxinitadvertisements <2-15>`
- `ip igmp mrdisc minadvertinterval <3-180>`
- `ip igmp mrdisc neighdeadinterval <2-180>`
- `no ip igmp mrdisc`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`maxadvertinterval <2-180>`	Configures the maximum number (in seconds) between successive advertisements. For this change to take effect, you must save the configuration, and then reset the switch. The default is 20.
`maxinitadvertinterval <2-180>`	Configures the maximum number (in seconds) between successive initial advertisements. For this change to take effect, you must save the configuration, and then reset the switch. The default is 2.
`maxinitadvertisements <2-15>`	Configures the maximum number of initial multicast advertisements after initialization. For this change to take effect, you must save the configuration, and then reset the switch. The default is 3.
`minadvertinterval`	Configures the minimum number (in seconds) between successive

<3-180>	advertisements. For this change to take effect, you must save the configuration, and then reset the switch. The default is 15.
neighdeadinterval <2-180>	Configures the multicast router discovery dead interval-the number of seconds the multicast route neighbors for the switch must wait before assuming that the multicast router is down. The default is 60.

©Avaya Inc. 2015 All Rights Reserved.

ip igmp snoop-querier

Enables the Layer 2 querier on a VLAN interface.

Syntax

- `default ip igmp snoop-querier`
- `ip igmp snoop-querier`
- `no ip igmp snoop-querier`

Default

`The default is disabled.`

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip igmp snoop-querier-addr

Configures the address of the IGMP snoop querier.

Syntax

- `default ip igmp snoop-querier-addr`
- `ip igmp snoop-querier-addr {A.B.C.D}`
- `no ip igmp snoop-querier-addr`

Default

`The default value is 0.0.0.0.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`{A.B.C.D}`	Specifies the IP address.

©Avaya Inc. 2015 All Rights Reserved.

ip igmp ssm dynamic-learning (for a VRF)

Enables SSM dynamic learning for the VRF.

Syntax

- `default ip igmp ssm dynamic-learning`
- `ip igmp ssm dynamic-learning`
- `ip igmp ssm dynamic-learning group-range {A.B.C.D/X}`
- `no ip igmp ssm dynamic-learning`

Default

`The default is enabled.`

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
`group-range {A.B.C.D/X}`	Extends the default SSM range of 232/8 to include an IP multicast address. You can configure existing applications without changing their group configuration.

©Avaya Inc. 2015 All Rights Reserved.

ip igmp ssm group-range (for a VRF)

Extends the default SSM range of 232/8 to include an IP multicast address. You can configure existing applications without changing their group configuration.

Syntax

- `default ip igmp ssm`
- `ip igmp ssm group-range {A.B.C.D/X}`
- `no ip igmp ssm`

Default

`The default IP address is 0.0.0.232. The default mask is 0.0.0.255.`

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
`{A.B.C.D/X}`	Specifies the IP address. The IP address must be within the range of 224.0.0.0 and 239.255.255.255.

©Avaya Inc. 2015 All Rights Reserved.

ip igmp ssm-map (for a VRF)

Configures the SSM map table to map groups to their sending source.

Syntax

- `default ip igmp ssm-map {A.B.C.D} {A.B.C.D}`
- `default ip igmp ssm-map {A.B.C.D} {A.B.C.D} enable`
- `default ip igmp ssm-map all`
- `ip igmp ssm-map {A.B.C.D} {A.B.C.D}`
- `ip igmp ssm-map {A.B.C.D} {A.B.C.D} enable`
- `ip igmp ssm-map all`
- `no ip igmp ssm-map {A.B.C.D} {A.B.C.D}`
- `no ip igmp ssm-map {A.B.C.D} {A.B.C.D} enable`
- `no ip igmp ssm-map all`

Default

`The default is disabled.`

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
`{A.B.C.D} {A.B.C.D}`	Enables the SSM map table for a specific entry or creates a static entry for a specific group. {A.B.C.D} {A.B.C.D} creates a static SSM channel table entry by specifying the group and source IP address. The first IP address is an IP multicast address within the SSM range. The second IP address is the source IP address. The source address is an IP host address that sends traffic to the group.
`all`	Enables the SSM map table for all static entries.
`enable`	Enables the static entry.

©Avaya Inc. 2015 All Rights Reserved.

ip igmp static-group

Configure IGMP static members to add members to a snoop group.

Syntax

- `default ip igmp static-group {A.B.C.D}`
- `default ip igmp static-group {A.B.C.D} {A.B.C.D}`
- `default ip igmp static-group {A.B.C.D} {A.B.C.D} {slot/port[-slot/port][,...]} { static | blocked }`
- `default ip igmp static-group {A.B.C.D} {slot/port[-slot/port][,...]} { static | blocked }`
- `ip igmp static-group {A.B.C.D} {A.B.C.D} {slot/port[-slot/port][,...]} { static | blocked }`
- `ip igmp static-group {A.B.C.D} {A.B.C.D} port {slot/port[-slot/port][,...]} { static | blocked }`
- `ip igmp static-group {A.B.C.D} {slot/port[-slot/port][,...]} { static | blocked }`
- `ip igmp static-group {A.B.C.D} port {slot/port[-slot/port][,...]} { static | blocked }`
- `no ip igmp static-group {A.B.C.D}`
- `no ip igmp static-group {A.B.C.D} {A.B.C.D}`
- `no ip igmp static-group {A.B.C.D} {A.B.C.D} {slot/port[-slot/port][,...]} { static | blocked }`
- `no ip igmp static-group {A.B.C.D} {slot/port[-slot/port][,...]} { static | blocked }`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`[static|blocked]`	Adds a static-member entry to the Internet Group Management Protocol (IGMP) interface. value is the port or list of ports to which you want to redirect the multicast stream for this multicast group. static|blocked configures the route to static or blocked.
`{slot/port [-slot/port][,...]}`	Creates static members on the interface. Specifies the port or list of ports to which you want to redirect the multicast stream for this multicast group. Use the format {slot/port[-slot/port][,...]}. Use the no operator to later remove this configuration.
`<A.B.C.D> <A.B.C.D>`	Indicates the IP address range from <A.B.C.D> to <A.B.C.D> of the selected multicast group.

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

ip igmp stream-limit (for a port)

Configure multicast stream limitation on an Ethernet port to limit the number of concurrent multicast streams on the port.

Syntax

- `default ip igmp stream-limit`
- `default ip igmp stream-limit stream-limit-max-streams`
- `ip igmp stream-limit`
- `ip igmp stream-limit stream-limit-max-streams <0-65535>`
- `no ip igmp stream-limit`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`stream-limit`	Enables the stream limit on the specifies Ethernet port.
`stream-limit-max-streams <0-65535>`	Sets the maximum number of streams allowed on an interface. The value ranges from 0 to 65535.

©Avaya Inc. 2015 All Rights Reserved.

ip igmp stream-limit (for a VLAN)

Configure multicast stream limitation on a VLAN to limit the number of concurrent multicast streams on the VLAN.

Syntax

- `ip igmp stream-limit [stream-limit-max-streams <0-65535>]`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`stream-limit`	Enables the stream limit on the specific VLAN port.
`stream-limit-max-streams <0-65535>`	Sets the maximum number of streams allowed on an interface. The value ranges from 0 to 65535.

©Avaya Inc. 2015 All Rights Reserved.

ip igmp stream-limit-group

Configure multicast stream limitation members on ports of a specific VLAN to limit the number of multicast groups that can join a VLAN.

Syntax

- `default ip igmp stream-limit-group {slot/port[-slot/port][,...]}`
- `default ip igmp stream-limit-group {slot/port[-slot/port][,...]} enable`
- `ip igmp stream-limit-group {slot/port[-slot/port][,...]} enable max-streams <0-65535>`
- `ip igmp stream-limit-group {slot/port[-slot/port][,...]} max-streams <0-65535>`
- `no ip igmp stream-limit-group {slot/port[-slot/port][,...]}`
- `no ip igmp stream-limit-group {slot/port[-slot/port][,...]} enable`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Specifies the slot and the port number.
`max-streams <0-65535>`	Configures the maximum number of allowed streams for the specified ports on this VLAN. The range is from 0-65535 and the default is 4. To use the default configuration, use the default option in the command: default ip igmp stream-limit-group <ports>

©Avaya Inc. 2015 All Rights Reserved.

ip ipfix collector

Configure collector parameters to determine to which collector a slot exports flow information. You can configure up to two collectors for each slot. Specify an exporter IP address to configure the source address in the IPFIX packets the interface module sends to the collectors. If you do not specify an exporter IP address, the source IP address is chosen from virtual IP, management IP, or outgoing interface IP based on the collector IP reachability.

Syntax

- `ip ipfix collector {slot[-slot][,...]} {A.B.C.D} dest-port <1-65535>`
- `ip ipfix collector {slot[-slot][,...]} {A.B.C.D} enable`
- `ip ipfix collector {slot[-slot][,...]} {A.B.C.D} exporter-ip {A.B.C.D}`
- `ip ipfix collector {slot[-slot][,...]} {A.B.C.D} protocol udp`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
{A.B.C.D}	Specifies the IP address of the collector.
{slot[-slot][,...]}	Identifies the slot in one of the following formats: a single slot (3), a range of slots (3-4), or a series of slots (3,5,6).
dest-port <1-65535>	Specifies the destination port.
enable	Enables the collector status.
exporter-ip {A.B.C.D}	Specifies the IP address for the exported traffic.
protocol udp	Specifies the protocol.

©Avaya Inc. 2015 All Rights Reserved.

ip ipfix enable

Enable Internet Protocol Flow Information eXport (IPFIX) to use IPFIX in filters or on a port.

Syntax

- `default ip ipfix enable`
- `ip ipfix enable`
- `no ip ipfix enable`

Default

`The default is disabled.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`enable`	Enables Internet Protocol Flow Information eXport (IPFIX) globally.

©Avaya Inc. 2015 All Rights Reserved.

ip ipfix flush

Flush Internet Protocol Flow Information eXport (IPFIX) flow information to delete all records that correspond to the port number you specify.

Syntax

- `ip ipfix flush port {slot/port[-slot/port][,...]}`
- `ip ipfix flush port {slot/port[-slot/port][,...]} export-and-flush`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot[-slot][,...]}`	Identifies the slot in one of the following formats: a single slot (3), a range of slots (3-4), or a series of slots (3,5,6).
`export-and-flush`	Optionally, initiates an export of all records, and then deletes the database after the export finishes. in UDP-based transport, the exporter sends out the flow database once, but there is no guarantee that the export reaches the collector. In TCP/SCTP-based transport, the receipt of the export by the collector is guaranteed.

©Avaya Inc. 2015 All Rights Reserved.

ip ipfix (on a port)

Configure IPFIX on a port to meter IP flows on the port. Note: For second generation I/O modules with IPFIX enabled, traffic loss can occur at high traffic rates. If you configure IPFIX for second generation modules, ensure you configure the sample rate to a value of at least 50.

Syntax

- `default ip ipfix`
- `default ip ipfix enable`
- `default ip ipfix port {slot/port[-slot/port][,...]} enable`
- `default ip ipfix port {slot/port[-slot/port][,...]} sampling-rate`
- `default ip ipfix sampling-rate`
- `ip ipfix enable`
- `ip ipfix port {slot/port[-slot/port][,...]} enable`
- `ip ipfix port {slot/port[-slot/port][,...]} sampling-rate <1-100000>`
- `ip ipfix sampling-rate <1-100000>`
- `no ip ipfix`
- `no ip ipfix enable`
- `no ip ipfix port {slot/port[-slot/port][,...]}`
- `no ip ipfix port {slot/port[-slot/port][,...]} enable`

Default

`The default sampling rate for second generation I/O modules is 50. The default sampling rate for first generation I/O modules is 1.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`enable`	Enables IPFIX on the port.
`sampling-rate <1-100000>`	Configures the sampling rate for metering on the port, as one in every n packets. The default sampling-rate value for first generation I/O modules is 1, which configures continuous monitoring. The default sampling-rate value for second generation I/O modules is 50. Note: For second generation I/O

modules with IPFIX enabled, traffic loss can occur at high traffic rates. If you configure IPFIX for second generation modules, ensure you configure the sampling rate to a value of at least 50.

©Avaya Inc. 2015 All Rights Reserved.

ip ipfix slot

Configure Internet Protocol Flow Information eXport (IPFIX) on an interface module to specify active flow parameters.

Syntax

- `default ip ipfix slot {slot[-slot][,...]} active-timeout`
- `default ip ipfix slot {slot[-slot][,...]} aging-interval`
- `default ip ipfix slot {slot[-slot][,...]} exporter-enable`
- `default ip ipfix slot {slot[-slot][,...]} export-interval`
- `default ip ipfix slot {slot[-slot][,...]} template-refresh-interval`
- `default ip ipfix slot {slot[-slot][,...]} template-refresh-packets`
- `ip ipfix slot {slot[-slot][,...]} active-timeout <1-60>`
- `ip ipfix slot {slot[-slot][,...]} aging-interval <10-3600>`
- `ip ipfix slot {slot[-slot][,...]} exporter-enable`
- `ip ipfix slot {slot[-slot][,...]} export-interval <10-3600>`
- `ip ipfix slot {slot[-slot][,...]} template-refresh-interval <60-3600>`
- `ip ipfix slot {slot[-slot][,...]} template-refresh-packets <1-600>`
- `no ip ipfix slot {slot[-slot][,...]}`
- `no ip ipfix slot {slot[-slot][,...]} exporter-enable`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`{slot[-slot][,...]}`	Identifies the slot in one of the following formats: a single slot (3), a range of slots (3- 4), or a series of slots (3,5,6). Valid slots are 3-12.
`active-timeout <1-60>`	Configures the flow active timeout. The default is 30 minutes.
`aging-interval <10-3600>`	Configures the flow record aging interval. The default is 15 seconds.
`exporter-enable`	Enables the exporter state for the slot. The default is enable.
`export-interval <10-3600>`	Configures the interval at which to export flow information. The default is 50 seconds.

`template-refresh-interval <60-3600>`	Configures the template refresh timeout. The template is sent to the collector every x seconds or after x exported packets, whichever occurs first. The default is 60 seconds.
`template-refresh-packets <1-600>`	Configures the template refresh timeout. The template is sent to the collector every x seconds or after x exported packets, whichever occurs first. The default is 20 packets.

©Avaya Inc. 2015 All Rights Reserved.

ip irdp

Enable Router Discovery globally so that the switch supports Router Discovery.

Syntax

- `default ip irdp`
- `ip irdp enable`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
enable	Enables the router discovery protocol on the switch.

©Avaya Inc. 2015 All Rights Reserved.

ip irdp address (for a port)

Configure Internet Control Message Protocol (ICMP) Router Discovery to enable hosts attached to multicast or broadcast networks to discover the IP addresses of their neighboring routers.

Syntax

- `default ip irdp`
- `default ip irdp address`
- `ip irdp address {A.B.C.D}`

Default

`The default address is 255.255.255.255.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`address <A.B.C.D>`	Specifies the IP destination address use for broadcast or multicast router advertisements sent from the interface. The address is the all-systems multicast address, 224.0.0.1, or the limited-broadcast address, 255.255.255.255.

©Avaya Inc. 2015 All Rights Reserved.

ip irdp address (for a VLAN)

Configure Internet Control Message Protocol (ICMP) Router Discovery to enable hosts attached to multicast or broadcast networks to discover the IP addresses of their neighboring routers.

Syntax

- `default ip irdp address <A.B.C.D>`
- `default ip irdp vlan <1-4084> address`
- `ip irdp address <A.B.C.D>`
- `ip irdp vlan <1-4084> address {A.B.C.D}`

Default

`The default address is 255.255.255.255.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`address <A.B.C.D>`	Specifies the IP destination address use for broadcast or multicast router advertisements sent from the interface. The address is the all-systems multicast address, 224.0.0.1, or the limited-broadcast address, 255.255.255.255.

©Avaya Inc. 2015 All Rights Reserved.

ip irdp holdtime (for a port)

Configure the lifetime for advertisements.

Syntax

- `default ip irdp holdtime`
- `ip irdp holdtime <4-9000>`

Default

`The default is 1800.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
<4-9000>	Specifies the lifetime.

©Avaya Inc. 2015 All Rights Reserved.

ip irdp holdtime (for a VLAN)

Configure the lifetime for advertisements.

Syntax

- `default ip irdp holdtime`
- `default ip irdp vlan <1-4084> holdtime`
- `ip irdp holdtime <4-9000>`
- `ip irdp vlan <1-4084> holdtime <4-9000>`

Default

`The default is 1800.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`<4-9000>`	Specifies the lifetime.

©Avaya Inc. 2015 All Rights Reserved.

ip irdp maxadvertinterval (for a port)

Specify the maximum time (in seconds) that elapses between unsolicited broadcast or multicast router advertisement transmissions from the router interface.

Syntax

- `default ip irdp maxadvertinterval`
- `ip irdp maxadvertinterval <4-1800>`

Default

`The default is 600 seconds.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<4-1800>`	Specifies the maximum time in seconds.

©Avaya Inc. 2015 All Rights Reserved.

ip irdp maxadvertinterval (for a VLAN)

Specify the maximum time (in seconds) that elapses between unsolicited broadcast or multicast router advertisement transmissions from the router interface.

Syntax

- `default ip irdp maxadvertinterval`
- `default ip irdp vlan <1-4084> maxadvertinterval`
- `ip irdp maxadvertinterval <4-1800>`
- `ip irdp vlan <1-4084> maxadvertinterval <4-1800>`

Default

`The default is 600 seconds.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`<4-1800>`	Specifies the maximum time in seconds.

©Avaya Inc. 2015 All Rights Reserved.

ip irdp minadvertinterval (for a port)

Specify the minimum time (in seconds) that elapses between unsolicited broadcast or multicast router advertisement transmissions from the interface. The range is 3 seconds to maxadvertinterval.

Syntax

- `default ip irdp minadvertinterval`
- `ip irdp minadvertinterval <3-1800>`

Default

`The default is 450 seconds.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
<3-1800>	Specifies the minimum time in seconds.

©Avaya Inc. 2015 All Rights Reserved.

ip irdp minadvertinterval (for a VLAN)

Specify the minimum time (in seconds) that elapses between unsolicited broadcast or multicast router advertisement transmissions from the interface. The range is 3 seconds to maxadvertinterval.

Syntax

- `default ip irdp minadvertinterval`
- `default ip irdp vlan <1-4084> minadvertinterval`
- `ip irdp minadvertinterval <3-1800>`
- `ip irdp vlan <1-4084> minadvertinterval <3-1800>`

Default

`The default is 450 seconds.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`<3-1800>`	Specifies the minimum time in seconds.

©Avaya Inc. 2015 All Rights Reserved.

ip irdp multicast (for a port)

Specify if multicast advertisements are sent.

Syntax

- `default ip irdp multicast`
- `ip irdp multicast`
- `no ip irdp multicast`

Default

`The default is enabled (true).`

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip irdp multicast (for a VLAN)

Specify if multicast advertisements are sent.

Syntax

- `default ip irdp multicast`
- `default ip irdp vlan <1-4084> multicast`
- `ip irdp multicast`
- `ip irdp vlan <1-4084> multicast`
- `no ip irdp multicast`
- `no ip irdp vlan <1-4084> multicast`

Default

`The default is enabled (true).`

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip irdp preference (for a port)

Specify the preference (a higher number indicates more preferred) of the address as a default router address relative to other router addresses on the same subnet.

Syntax

- `default ip irdp preference`
- `ip irdp preference <-2147483648-2147483647>`

Default

`The default is 0.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<-2147483648-2147483647>`	Specifies the preference value.

©Avaya Inc. 2015 All Rights Reserved.

ip irdp preference (for a VLAN)

Specify the preference (a higher number indicates more preferred) of the address as a default router address relative to other router addresses on the same subnet.

Syntax

- `default ip irdp preference`
- `default ip irdp vlan <1-4084> preference`
- `ip irdp preference <-2147483648-2147483647>`
- `ip irdp vlan <1-4084> preference <-2147483648-2147483647>`

Default

`The default is 0.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`<-2147483648-2147483647>`	Specifies the preference value.

©Avaya Inc. 2015 All Rights Reserved.

ip isid-list (for a VRF)

Create an I-SID list to use with IS-IS accept policies.

Syntax

- `ip isid-list WORD<1-32> <0-16777215>`
- `ip isid-list WORD<1-32> list WORD<1-1024>`
- `no ip isid-list WORD<1-32> <0-16777215>`
- `no ip isid-list WORD<1-32> list WORD<1-1024>`

Default

None

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
`<0-16777215>`	Specifies an I-SID value.
`list WORD<1-1024>`	Specifies a list of I-SID values in one of the following formats (1,3,5,8-10).
`WORD<1-32>`	Specifies a name for the I-SID list.

©Avaya Inc. 2015 All Rights Reserved.

ip isid-list (for the GRT)

Create an I-SID list to use with IS-IS accept policies.

Syntax

- `ip isid-list WORD<1-32> <1-16777215>`
- `ip isid-list WORD<1-32> list WORD<1-1024>`
- `no ip isid-list WORD<1-32> <1-16777215>`
- `no ip isid-list WORD<1-32> list WORD<1-1024>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`<1-16777215>`	Specifies an I-SID value.
`list WORD<1-1024>`	Specifies a list of I-SID values in one of the following formats (1,3,5,8-10).
`WORD<1-32>`	Specifies a name for the I-SID list.

©Avaya Inc. 2015 All Rights Reserved.

ip max-routes-trap enable

Enable the switch to send a trap when the maximum number of routes is exceeded.

Syntax

- `default ip max-routes-trap enable`
- `ip max-routes-trap enable`
- `no ip max-routes-trap enable`

Default

`The default is disabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip more-specific-non-local-route

Enable the more-specific-non-local-route feature. If enabled, the switch can enter a more-specific nonlocal route into the routing table.

Syntax

- `default ip more-specific-non-local-route`
- `default ip more-specific-non-local-route enable`
- `ip more-specific-non-local-route`
- `ip more-specific-non-local-route enable`
- `no ip more-specific-non-local-route`
- `no ip more-specific-non-local-route enable`

Default

`The default is disabled.`

Command mode

Global Configuration

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

ip mroute (for a port)

Limit the number of multicast streams to protect a CPU from multicast data packet bursts generated by malicious applications.

Syntax

- `default ip mroute max-allowed-streams`
- `default ip mroute max-allowed-streams-timer-check`
- `default ip mroute port {slot/port[-slot/port][,...]}`
- `default ip mroute stream-limit`
- `ip mroute max-allowed-streams <1-32768>`
- `ip mroute max-allowed-streams-timer-check <1-3600>`
- `ip mroute port {slot/port[-slot/port][,...]} max-allowed-streams <1-32768>`
- `ip mroute port {slot/port[-slot/port][,...]} max-allowed-streams-timer-check <1-3600>`
- `ip mroute port {slot/port[-slot/port][,...]} stream-limit`
- `ip mroute stream-limit`
- `no ip mroute port {slot/port[-slot/port][,...]}`
- `no ip mroute stream-limit`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`max-allowed-streams <1-32768>`	Configures the maximum number of streams on the specified port. The port is shut down if the number of streams exceeds this limit. The value is a number between 1-32768. The default value is 1984 streams. To set this option to the default value, use the default operator with the command.
`max-allowed-streams-timer-check <1-3600>`	Configures the sampling interval, which is used to check if the number of ingress multicast streams to the CPU is under a configured limit or if the port needs to shut down. The range is between 1-3600. The default value is 10 seconds. To set this option to the default value, use the default operator with the command.
`port {slot/port[-slot/port][,...]}`	Specifies the port or range of ports in slot/port notation. Use the no operator to later remove this configuration.

`stream-limit` Enables stream limit on a particular interface.

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

ip mroute resource-usage egress-threshold

Configure the resource usage counters to query the number of ingress and egress IP multicast streams traversing your switch.

Syntax

- `ip mroute resource-usage egress-threshold <0-32767> ingress-threshold <0-32767>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`egress-threshold <0-32767>`	Configures the egress record threshold (S,G). A notification message is sent if this value is exceeded. integer is a value between 0-32767. To set this option to the default value, use the default operator with the command. The default is 0.
`ingress-threshold <0-32767>`	Configures the ingress record threshold (peps). A notification message is sent if this value is exceeded. integer is a value between 0-32767. To set this option to the default value, use the default operator with the command. The default is 0.

©Avaya Inc. 2015 All Rights Reserved.

ip mroute resource-usage (for a VRF)

Configures the resource usage counters.

Syntax

- `default ip mroute resource-usage egress-threshold <0-32767>`
- `default ip mroute resource-usage ingress-threshold <0-32767>`
- `default ip mroute resource-usage log-msg`
- `default ip mroute resource-usage trap-msg`
- `ip mroute resource-usage egress-threshold <0-32767>`
- `ip mroute resource-usage ingress-threshold <0-32767>`
- `ip mroute resource-usage log-msg`
- `ip mroute resource-usage trap-msg`
- `no ip mroute resource-usage egress-threshold <0-32767>`
- `no ip mroute resource-usage ingress-threshold <0-32767>`
- `no ip mroute resource-usage log-msg`
- `no ip mroute resource-usage trap-msg`

Default

None

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
`egress-threshold <0-32767>`	Configures the egress record threshold (S,G). A notification message is sent if this value is exceeded. The default is 0.
`ingress-threshold <0-32767>`	Configures the ingress record threshold (peps). A notification message is sent if this value is exceeded. The default is 0.
`log-msg`	Configures the notification method for sending only a log message after the threshold level is exceeded. The default is disabled.
`trap-msg`	Configures the notification method for sending only a trap message after the threshold level is exceeded. The default is disabled

©Avaya Inc. 2015 All Rights Reserved.

ip mroute resource-usage log-msg trap-msg

Enable traps and log messages on the console.

Syntax

- `ip mroute resource-usage log-msg trap-msg`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`log-msg`	Configures the notification method for sending only a log message after the threshold level is exceeded. Use the no operator to later remove this configuration. To set this option to the default value, use the default operator with the command. The default is disabled.
`trap-msg`	Configures the notification method for sending only a trap message after the threshold level is exceeded. Use the no operator to later remove this configuration. To set this option to the default value, use the default operator with the command. The default is disabled.

©Avaya Inc. 2015 All Rights Reserved.

ip mroute static-source-group

Configure static source-group entries in the Protocol Independent Multicast (PIM) multicast routing table.

Syntax

- `ip mroute static-source-group <A.B.C.D> <A.B.C.D/X>`
- `np ip mroute static-source-group <A.B.C.D> <A.B.C.D/X>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
A.B.C.D	Specifies the IP address of the multicast group. Use the no operator to remove this configuration.
A.B.C.D/X	Specifies the multicast source IP address and subnet mask for the static source group entry. You cannot create duplicate groups. How you configure the source address depends on the protocol and mode you use. Use the no operator to remove this configuration.

©Avaya Inc. 2015 All Rights Reserved.

ip mroute stats enable

Enable the collection of multicast routing process statistics.

Syntax

- `default ip mroute stats enable`
- `ip mroute stats enable`
- `no ip mroute stats enable`

Default

`The default is disabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip mroute stream-limit (globally)

Limit the number of multicast streams to protect a Central Processor Unit (CPU) from multicast data packet bursts generated by malicious applications.

Syntax

- `ip mroute stream-limit`

Default

None

Command mode

Global Configuration

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

ip name-server

Add addresses for DNS servers.

Syntax

- `default ip name-server <primary|secondary|tertiary>`
- `ip name-server <primary|secondary|tertiary> WORD<0-46>`
- `no ip name-server <primary|secondary|tertiary>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`<primary|secondary|tertiary>WORD<0-46>`	Configures the primary, secondary, or tertiary DNS server address. Enter the IP address in a.b.c.d format for IPv4 (string length 0-46). You can specify the IP address for only one server at a time; you cannot specify all three servers in one command.

©Avaya Inc. 2015 All Rights Reserved.

ip ospf advertise-when-down enable (for a port)

Enable or disable AdvertiseWhenDown. If enabled, the network on this interface is advertised as up, even if the port is down. When you configure a port with no link and enable advertise-when-down, the route is not advertised until the port is active. Then the route is advertised even when the link is down. To disable advertising based on link status, this parameter must be disabled.

Syntax

- `default ip ospf advertise-when-down enable`
- `ip ospf advertise-when-down enable`
- `ip ospf port {slot/port[-slot/port][,...]} advertise-when-down enable`
- `no ip ospf advertise-when-down enable`

Default

`The default is disabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

ip ospf advertise-when-down enable (for a VLAN)

Enable or disable AdvertiseWhenDown. If enabled, the network on this interface is advertised as up, even if the port is down. When you configure a VLAN with no link and enable advertise-when-down, the route is not advertised until the VLAN is active. Then the route is advertised even when the link is down. To disable advertising based on link status, this parameter must be disabled.

Syntax

- `default ip ospf advertise-when-down enable`
- `ip ospf advertise-when-down enable`
- `no ip ospf advertise-when-down enable`

Default

`The default is disabled.`

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip ospf apply accept

Apply OSPF accept policy changes to allow the configuration changes in the policy to take effect in an OSPF Accept context (and to prevent the switch from attempting to apply the changes one by one after each configuration change).

Syntax

- `ip ospf apply accept`
- `ip ospf apply accept vrf WORD<1-16>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`apply`	Commits entered changes. Issue this command after modifying any policy configuration that affects an OSPF accept policy.
`vrf WORD<1-16>`	Specifies the name of the VRF.

©Avaya Inc. 2015 All Rights Reserved.

ip ospf apply accept adv-rtr

Apply the OSPF accept policy change to accept external routes from a specified advertising route.

Syntax

- `ip ospf apply accept adv-rtr {A.B.C.D}`
- `ip ospf apply accept adv-rtr {A.B.C.D} vrf WORD<1-16>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`adv-rtr <A.B.C.D>`	Specifies the advertising router IP address.
`vrf WORD<1-16>`	Specifies the configuration for a particular VRF. WORD<1-16> specifies the VRF name.

©Avaya Inc. 2015 All Rights Reserved.

ip ospf apply redistribute

Apply the OSPF redistribution.

Syntax

- `ip ospf apply redistribute`
- `ip ospf apply redistribute vrf WORD<1-16>`
- `ip ospf apply redistribute WORD<1-32>`
- `ip ospf apply redistribute WORD<1-32> vrf WORD<1-16>`
- `ip ospf apply redistribute WORD<1-32> vrf-src WORD<1-16>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies the VRF instance by name. When applying a redistribution instance that redistributes from a nonzero VRF to VRF 0 (the global router), do not specify the destination VRF; only specify the source VRF.
`vrf-src WORD<1-16>`	Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.
`WORD<1-32>`	Specifies the type of routes to be redistributed (the protocol source), including RIP, OSPF, BGP, ISIS, static, and direct.

©Avaya Inc. 2015 All Rights Reserved.

ip ospf area (for a port)

Configure OSPF parameters on a port to control how OSPF behaves.

Syntax

- `default ip ospf area`
- `ip ospf area {A.B.C.D}`
- `ip ospf port {slot/port[-slot/port][,...]} area {A.B.C.D}`
- `no ip ospf area`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
<A.B.C.D>	Configures the OSPF identification number for the area, typically formatted as an IP address.
port {slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

ip ospf area (for a VLAN)

Configure OSPF parameters on a VLAN to control how OSPF behaves.

Syntax

- `default ip ospf area`
- `ip ospf area {A.B.C.D}`
- `no ip ospf area`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
<A.B.C.D>	Configures the OSPF identification number for the area, typically formatted as an IP address.

©Avaya Inc. 2015 All Rights Reserved.

ip ospf authentication-key WORD<0-8> (for a port)

Configure the eight-character simple password authentication key for the port.

Syntax

- `ip ospf authentication-key WORD<0-8>`
- `ip ospf port {slot/port[-slot/port][,...]} authentication-key WORD<0-8>`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

ip ospf authentication-key WORD<0-8> (for a VLAN)

Configure the eight-character simple password authentication key for the VLAN.

Syntax

- `ip ospf authentication-key WORD<0-8>`

Default

None

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip ospf authentication-type <none|message-digest|simple> (for a port)

Configure the OSPF authentication type for the port. If simple, all OSPF updates the interface receives must contain the authentication key specified by the area authentication-key command. If MD5, they must contain the MD5 key.

Syntax

- `default ip ospf authentication-type`
- `ip ospf authentication-type message-digest`
- `ip ospf authentication-type none`
- `ip ospf authentication-type simple`
- `ip ospf port {slot/port[-slot/port][,...]} authentication-type message-digest`
- `ip ospf port {slot/port[-slot/port][,...]} authentication-type none`
- `ip ospf port {slot/port[-slot/port][,...]} authentication-type simple`
- `no ip ospf authentication-type`

Default

`The default is none.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

ip ospf authentication-type <none|message-digest|simple> (for a VLAN)

Configure the OSPF authentication type for the VLAN. If simple, all OSPF updates the interface receives must contain the authentication key specified by the area authentication-key command. If MD5, they must contain the MD5 key.

Syntax

- `default ip ospf authentication-type`
- `ip ospf authentication-type message-digest`
- `ip ospf authentication-type none`
- `ip ospf authentication-type simple`
- `no ip ospf authentication-type`

Default

`The default is none.`

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip ospf cost <1-65535> (for a port)

Configure the OSPF cost associated with this interface and advertised in router link advertisements.

Syntax

- `default ip ospf cost`
- `ip ospf cost <0-65535>`
- `ip ospf port {slot/port[-slot/port][,...]} cost <0-65535>`

Default

`The default is 0.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

ip ospf cost <1-65535> (for a VLAN)

Configure the OSPF cost associated with this interface and advertised in router link advertisements.

Syntax

- `default ip ospf cost`
- `ip ospf cost <0-65535>`

Default

`The default is 0.`

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip ospf dead-interval <0-2147483647> (for a port)

Configure the router OSPF dead interval-the number of seconds the OSPF neighbors of a switch must wait before assuming that the OSPF router is down. The value must be at least four times the Hello interval.

Syntax

- `default ip ospf dead-interval`
- `ip ospf dead-interval <0-2147483647>`
- `ip ospf port {slot/port[-slot/port][,...]} dead-interval <0-2147483647>`

Default

`The default is 40.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

ip ospf dead-interval <0-2147483647> (for a VLAN)

Configure the router OSPF dead interval-the number of seconds the OSPF neighbors of a switch must wait before assuming that the OSPF router is down. The value must be at least four times the Hello interval.

Syntax

- `default ip ospf dead-interval`
- `ip ospf dead-interval <0-2147483647>`

Default

`The default is 40.`

Command mode

VLAN Interface Configuration

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

ip ospf default-cost (for a VRF)

Configure the OSPF default cost.

Syntax

- `default ip ospf default-cost ethernet`
- `default ip ospf default-cost fast-ethernet`
- `default ip ospf default-cost forty-gig-ethernet`
- `default ip ospf default-cost gig-ethernet`
- `default ip ospf default-cost ten-gig-ethernet`
- `ip ospf default-cost ethernet <1-65535>`
- `ip ospf default-cost fast-ethernet <1-65535>`
- `ip ospf default-cost forty-gig-ethernet <1-65535>`
- `ip ospf default-cost gig-ethernet <1-65535>`
- `ip ospf default-cost ten-gig-ethernet <1-65535>`

Default

`The default is none.`

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
`ethernet <1-65535>`	Configures the OSPF default cost for 10 Mb/s Ethernet. The default is 100.
`fast-ethernet <1-65535>`	Configures the OSPF default cost for 100 Mb/s (Fast) Ethernet. The default is 10.
`forty-gig-ethernet <1-65535>`	Configures the OSPF default cost for 40 Gigabit Ethernet. The default is 1.
`gig-ethernet <1-65535>`	Configures the OSPF default cost for Gigabit Ethernet. The default is 1.
`ten-gig-ethernet <1-65535>`	Configures the OSPF default cost for 10 Gigabit Ethernet. The default is 1.

©Avaya Inc. 2015 All Rights Reserved.

ip ospf enable (for a port)

Enable OSPF on the port.

Syntax

- `default ip ospf`
- `default ip ospf enable`
- `default ip ospf port {slot/port[-slot/port][,...]}`
- `ip ospf enable`
- `ip ospf port {slot/port[-slot/port][,...]} enable`
- `no ip ospf`
- `no ip ospf enable`
- `no ip ospf port {slot/port[-slot/port][,...]}`

Default

`The default is disabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

ip ospf enable (for a VLAN)

Enable OSPF on the VLAN.

Syntax

- `default ip ospf enable`
- `ip ospf enable`
- `no ip ospf`
- `no ip ospf enable`

Default

`The default is disabled.`

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip ospf hello-interval <1-65535> (for a port)

Configure the OSPF Hello interval, which is the number of seconds between Hello packets sent on this interface.

Syntax

- `default ip ospf hello-interval`
- `ip ospf hello-interval <1-65535>`
- `ip ospf port {slot/port[-slot/port][,...]} hello-interval <1-65535>`

Default

`The default is 10.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

ip ospf hello-interval <1-65535> (for a VLAN)

Configure the OSPF Hello interval, which is the number of seconds between Hello packets sent on this interface.

Syntax

- `default ip ospf hello-interval`
- `ip ospf hello-interval <1-65535>`

Default

`The default is 10.`

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip ospf (loopback)

Enable OSPF for the circuitless IP (CLIP) interface.

Syntax

- `default ip ospf`
- `default ip ospf <1-256>`
- `default ip ospf vrf WORD<1-16>`
- `ip ospf`
- `ip ospf <1-256>`
- `ip ospf vrf WORD<1-16>`
- `no ip ospf`
- `no ip ospf <1-256>`
- `no ip ospf vrf WORD<1-16>`

Default

`The default is disabled.`

Command mode

Loopback Interface Configuration

Command parameters

Parameter	Description
`<1-256>`	Specifies the interface identification number for the CLIP.
`default`	Sets the OSPF status on the loopback interface to the default of disabled.
`no`	Disables the loopback OSPF for a particular value.
`vrf WORD<1-16>`	Specifies an associated VRF by name.

©Avaya Inc. 2015 All Rights Reserved.

ip ospf message-digest-key <1-255> md5-key WORD<0-16> (for a port)

Configure the Message Digest 5 algorithm (MD5) key. At most, you can configure two MD5 keys for an interface.<1-255> is the ID for the message digest key WORD<0-16> is an alphanumeric password of up to 16 bytes {string length 0 to 16}

Syntax

- `default ip ospf message-digest-key <1-255>`
- `ip ospf message-digest-key <1-255> md5 WORD<0-16>`
- `no ip ospf message-digest-key <1-255>`

Default

None

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip ospf message-digest-key <1-255> md5-key WORD<0-16> (for a VLAN)

Configure the Message Digest 5 algorithm (MD5) key. At most, you can configure two MD5 keys for an interface.<1-255> is the ID for the message digest key WORD<0-16> is an alphanumeric password of up to 16 bytes {string length 0 to 16}

Syntax

- `default ip ospf message-digest-key <1-255>`
- `ip ospf message-digest-key <1-255> md5 WORD<0-16>`
- `no ip ospf message-digest-key <1-255>`

Default

None

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip ospf mtu-ignore enable (for a port)

Enable maximum transmission unit (MTU) ignore. To allow the VSP 9000 to accept OSPF database description (DBD) packets with a different MTU size, enable mtu-ignore. Incoming OSPF DBD packets are dropped if their MTU is greater than 1500 bytes.

Syntax

- `default ip ospf mtu-ignore enable`
- `ip ospf mtu-ignore enable`
- `ip ospf port {slot/port[-slot/port][,...]} mtu-ignore enable`
- `no ip ospf mtu-ignore enable`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

ip ospf mtu-ignore enable (for a VLAN)

Enable maximum transmission unit (MTU) ignore. To allow the VSP 9000 to accept OSPF database description (DBD) packets with a different MTU size, enable mtu-ignore. Incoming OSPF DBD packets are dropped if their MTU is greater than 1500 bytes.

Syntax

- `default ip ospf mtu-ignore enable`
- `ip ospf mtu-ignore enable`
- `no ip ospf mtu-ignore enable`

Default

None

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip ospf network <broadcast|nbma|passive> (for a port)

Specify the type of OSPF interface.

Syntax

- `default ip ospf network`
- `ip ospf network { broadcast | nbma | passive }`
- `ip ospf port {slot/port[-slot/port][,...]} network { broadcast | nbma | passive }`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

ip ospf network <broadcast|nbma|passive> (for a VLAN)

Specify the type of OSPF interface.

Syntax

- `default ip ospf network`
- `ip ospf network { broadcast | nbma | passive }`

Default

None

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip ospf poll-interval <0-2147483647> (for a port)

Configure the OSPF poll interval in seconds.

Syntax

- `default ip ospf poll-interval`
- `ip ospf poll-interval <0-2147483647>`
- `ip ospf port {slot/port[-slot/port][,...]} poll-interval <0-2147483647>`

Default

`The default is 120.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

ip ospf poll-interval <0-2147483647> (for a VLAN)

Configure the OSPF poll interval in seconds.

Syntax

- `default ip ospf poll-interval`
- `ip ospf poll-interval <0-2147483647>`

Default

The default is 120.

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip ospf primary-md5-key <1-255> (for a port)

Changes the primary key used to encrypt outgoing packets. <1-255> is the ID for the new message digest key.

Syntax

- `default ip ospf primary-md5-key`
- `ip ospf port {slot/port[-slot/port][,...]} primary-md5-key <1-255>`
- `ip ospf primary-md5-key <1-255>`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

ip ospf primary-md5-key <1-255> (for a VLAN)

Changes the primary key used to encrypt outgoing packets. <1-255> is the ID for the new message digest key.

Syntax

- `default ip ospf primary-md5-key`
- `ip ospf primary-md5-key <1-255>`

Default

None

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip ospf priority <0-255> (for a port)

Configure the OSPF priority for the port during the election process for the designated router. The port with the highest priority number is the best candidate for the designated router. If you configure the priority to 0, the port cannot become either the designated router or a backup designated router.

Syntax

- `default ip ospf priority`
- `ip ospf port {slot/port[-slot/port][,...]} priority <0-255>`
- `ip ospf priority <0-255>`

Default

`The default is 1.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

ip ospf priority <0-255> (for a VLAN)

Configure the OSPF priority for the VLAN during the election process for the designated router. The VLAN with the highest priority number is the best candidate for the designated router. If you configure the priority to 0, the VLAN cannot become either the designated router or a backup designated router.

Syntax

- `default ip ospf priority`
- `ip ospf priority <0-255>`

Default

`The default is 1.`

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip ospf redistribute

Configure and enable redistribution entries to allow a protocol to announce routes of a certain source type, for example, static, RIP, or direct.

Syntax

- `default ip ospf redistribute WORD<1-32>`
- `default ip ospf redistribute WORD<1-32> enable`
- `default ip ospf redistribute WORD<1-32> metric`
- `default ip ospf redistribute WORD<1-32> metric-type`
- `default ip ospf redistribute WORD<1-32> route-policy`
- `default ip ospf redistribute WORD<1-32> subnets`
- `default ip ospf redistribute WORD<1-32> vrf-src WORD<1-16>`
- `ip ospf redistribute WORD<1-32>`
- `ip ospf redistribute WORD<1-32> enable`
- `ip ospf redistribute WORD<1-32> metric <0-65535>`
- `ip ospf redistribute WORD<1-32> metric-type { type1 | type2 | any }`
- `ip ospf redistribute WORD<1-32> route-policy WORD<0-64>`
- `ip ospf redistribute WORD<1-32> subnets { allow | suppress }`
- `ip ospf redistribute WORD<1-32> vrf-src WORD<1-16>`
- `no ip ospf redistribute WORD<1-32>`
- `no ip ospf redistribute WORD<1-32> enable`
- `no ip ospf redistribute WORD<1-32> route-policy`
- `no ip ospf redistribute WORD<1-32> vrf-src WORD<1-16>`

Default

None

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
`enable`	Enables the route redistribution instance.
`metric <0-`	

65535>	Configures the metric to apply to redistributed routes.
metric-type { type1 | type2 | any }	Specifies a type 1 or a type 2 metric. For metric type 1, the cost of the external routes is equal to the sum of all internal costs and the external cost. For metric type 2, the cost of the external routes is equal to the external cost alone.
route-policy WORD<0-64>	Configures the route policy to apply to redistributed routes.
subnets { allow | suppress }	Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.
vrf WORD<1-16>	Specifies the VRF instance.
vrf-src WORD<1-16>	Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.
WORD<0-32>	Specifies the type of routes to redistribute-the protocol source.

©Avaya Inc. 2015 All Rights Reserved.

ip ospf retransmit-interval <0-3600> (for a port)

Configure the retransmit interval for the virtual interface, the number of seconds between link-state advertisement retransmissions.

Syntax

- `default ip ospf retransmit-interval`
- `ip ospf port {slot/port[-slot/port][,...]} retransmit-interval <0-3600>`
- `ip ospf retransmit-interval <0-3600>`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

ip ospf retransmit-interval <0-3600> (for a VLAN)

Configure the retransmit interval for the virtual interface, the number of seconds between link-state advertisement retransmissions.

Syntax

- `default ip ospf retransmit-interval`
- `ip ospf retransmit-interval <0-3600>`

Default

None

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip ospf spf-run

Force the switch to update its shortest-path calculations so that the switch uses the latest OSPF routing information.

Syntax

- `ip ospf spf-run`
- `ip ospf spf-run vrf WORD<1-16>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF instance by name.

©Avaya Inc. 2015 All Rights Reserved.

ip ospf transit-delay <0-3600> (for a port)

Configure the transit delay for the virtual interface, which is the estimated number of seconds required to transmit a link-state update over the interface.

Syntax

- `default ip ospf transit-delay`
- `ip ospf port {slot/port[-slot/port][,...]} transit-delay <0-3600>`
- `ip ospf transit-delay <0-3600>`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

ip ospf transit-delay <0-3600> (for a VLAN)

Configure the transit delay for the virtual interface, which is the estimated number of seconds required to transmit a link-state update over the interface.

Syntax

- `default ip ospf transit-delay`
- `ip ospf transit-delay <0-3600>`

Default

None

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip ospf vlan (for a VLAN)

Configure OSPF on a VLAN.

Syntax

- `default ip ospf vlan <1-4084>`
- `ip ospf vlan <1-4084> advertise-when-down enable`
- `ip ospf vlan <1-4084> area {A.B.C.D}`
- `ip ospf vlan <1-4084> authentication-key WORD<0-8>`
- `ip ospf vlan <1-4084> authentication-type message-digest`
- `ip ospf vlan <1-4084> authentication-type none`
- `ip ospf vlan <1-4084> authentication-type simple`
- `ip ospf vlan <1-4084> cost <0-65535>`
- `ip ospf vlan <1-4084> dead-interval <0-2147483647>`
- `ip ospf vlan <1-4084> enable`
- `ip ospf vlan <1-4084> hello-interval <1-65535>`
- `ip ospf vlan <1-4084> mtu-ignore enable`
- `ip ospf vlan <1-4084> network { broadcast | nbma | passive }`
- `ip ospf vlan <1-4084> poll-interval <0-2147483647>`
- `ip ospf vlan <1-4084> primary-md5-key <1-255>`
- `ip ospf vlan <1-4084> priority <0-255>`
- `ip ospf vlan <1-4084> retransmit-interval <0-3600>`
- `ip ospf vlan <1-4084> transit-delay <0-3600>`
- `no ip ospf vlan <1-4084>`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
<1-4084>	Specifies the VLAN ID.

advertise-when-down enable	Enables or disables AdvertiseWhenDown. If enabled, the network on this interface is advertised as up, even if the port is down. When you configure a VLAN with no link and enable advertise-when-down, the route is not advertised until the VLAN is active. Then the route is advertised even when the link is down. To disable advertising based on link status, this parameter must be disabled. The default is disabled.
area {A.B.C.D}	Configures OSPF parameters on a VLAN to control how OSPF behaves.
authentication-key WORD<0-8>	Configures the eight-character simple password authentication key for the VLAN.
authentication-type	Configures the OSPF authentication type for the VLAN. If simple, all OSPF updates the interface receives must contain the authentication key specified by the area authentication-key command. If MD5, they must contain the MD5 key. The default is none.
cost <0-65535>	Configures the OSPF cost associated with this interface and advertised in router link advertisements. The default is 0.
dead-interval <0-2147483647>	Configures the router OSPF dead interval-the number of seconds the OSPF neighbors of a switch must wait before assuming that the OSPF router is down. The value must be at least four times the Hello interval. The default is 40.
enable	Enables OSPF on the VLAN. The default is disabled.
hello-interval <1-65535>	Configures the OSPF Hello interval, which is the number of seconds between Hello packets sent on this interface. The default is 10.
mtu-ignore enable	Enables maximum transmission unit (MTU) ignore. To allow the VSP 9000 to accept OSPF database description (DBD) packets with a different MTU size, enable mtu-ignore. Incoming OSPF DBD packets are dropped if their MTU is greater than 1500 bytes.
network { broadcast | nbma | passive }	Specifies the type of OSPF interface.
poll-interval <0-2147483647>	Configures the OSPF poll interval in seconds. The default is 120.
primary-md5-key <1-255>	Changes the primary key used to encrypt outgoing packets. <1-255> is the ID for the new message digest key.
priority <0-255>	Configures the OSPF priority for the VLAN during the election process for the designated router. The VLAN with the highest priority number is the best candidate for the designated router. If you configure the priority to 0, the VLAN cannot become either the designated router or a backup designated router. The default is 1.
retransmit-interval <0-3600>	Configures the retransmit interval for the virtual interface, the number of seconds between link-state advertisement retransmissions.
transit-delay <0-3600>	Configures the transit delay for the virtual interface, which is the estimated number of seconds required to transmit a link-state update over the interface.

©Avaya Inc. 2015 All Rights Reserved.

ip pim active (for a port)

Enable PIM and configure the interface type to active to perform multicasting operations.

Syntax

- `ip pim active`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
active	Enables PIM and sets interface type to active.
passive	Enables PIM and sets interface type to passive.

©Avaya Inc. 2015 All Rights Reserved.

ip pim active (for a VLAN)

Enable PIM and configure the interface type to active or passive to perform multicasting operations.

Syntax

- `ip pim <active|passive>`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
active	Enables PIM and sets interface type to active.
passive	Enables PIM and sets interface type to passive.

©Avaya Inc. 2015 All Rights Reserved.

ip pim bootstrap-period <5-32757>

Specify the interval (in seconds) that the elected bootstrap router (BSR) waits between originating bootstrap messages.

Syntax

- `default ip pim bootstrap-period`
- `ip pim bootstrap-period <5-32757>`

Default

`The default is 60.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip pim bsr-candidate preference (for a port)

Configure additional routers as candidate BSRs (C-BSR) to provide backup protection in the event that the primary BSR fails.

Syntax

- `default ip pim bsr-candidate`
- `ip pim bsr-candidate preference <0-255>`
- `no ip pim bsr-candidate`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`preference <0-255>`	Enables the C-BSR on this interface and configures its preference value, from 0-255, to become a BootStrap Router (BSR). The C-BSR with the highest BSR preference and address is the preferred BSR.

©Avaya Inc. 2015 All Rights Reserved.

ip pim bsr-candidate preference (for a VLAN)

Configure additional routers as candidate BSRs (C-BSR) to provide backup protection in the event that the primary BSR fails.

Syntax

- `default ip pim bsr-candidate`
- `ip pim bsr-candidate preference <0-255>`
- `no ip pim bsr-candidate`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`preference <0-255>`	Enables the C-BSR on this interface and configures its preference value, from 0-255, to become a BSR. The C-BSR with the highest BSR preference and address is the preferred BSR.

©Avaya Inc. 2015 All Rights Reserved.

ip pim disc-data-timeout <5-65535>

Specify how long (in seconds) to discard data until the join is received from the rendezvous point (RP). An IP multicast discard record is created after a register packet is sent, until the timer expires or a join is received.

Syntax

- `default ip pim disc-data-timeout`
- `ip pim disc-data-timeout <5-65535>`

Default

`The default is 60.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip pim enable (for a port)

Configure PIM for each interface to enable the interface to perform multicasting operations.

Syntax

- `default ip pim enable`
- `ip pim enable`
- `no ip pim enable`

Default

`The default is disabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables PIM on the local switch interface. The default is disabled.

©Avaya Inc. 2015 All Rights Reserved.

ip pim enable (for a VLAN)

Configure PIM for each interface to enable the interface to perform multicasting operations.

Syntax

- `default ip pim enable`
- `ip pim enable`
- `no ip pim enable`

Default

`The default is disabled.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables PIM on the local switch interface. The default is disabled.

©Avaya Inc. 2015 All Rights Reserved.

ip pim fast-joinprune

Enable the fast join prune interval.

Syntax

- `default ip pim fast-joinprune`
- `ip pim fast-joinprune`
- `no ip pim fast-joinprune`

Default

`The default is disabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip pim fwd-cache-timeout <10-86400>

Specify the forward cache timeout value.

Syntax

- `default ip pim fwd-cache-timeout`
- `ip pim fwd-cache-timeout <10-86400>`

Default

`The default is 210.`

Command mode

Global Configuration

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

ip pim (globally)

Configure PIM to create a PIM instance, and enable or disable PIM globally on the switch and change default global parameters.

Syntax

- `default ip pim`
- `default ip pim enable`
- `ip pim`
- `ip pim enable`
- `no ip pim`
- `no ip pim enable`

Default

`The default is disabled.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`enable`	Activates PIM on the switch globally.

©Avaya Inc. 2015 All Rights Reserved.

ip pim hello-interval <0-18724> (for a port)

Specify how long to wait (in seconds) before the PIM switch sends out the next hello message to neighboring switches.

Syntax

- `default ip pim hello-interval`
- `ip pim hello-interval <0-18724>`

Default

The default is 30 seconds.

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip pim hello-interval <0-18724> (for a VLAN)

Specify how long to wait (in seconds) before the PIM switch sends out the next hello message to neighboring switches.

Syntax

- `default ip pim hello-interval`
- `ip pim hello-interval <0-18724>`

Default

The default is 30 seconds.

Command mode

VLAN Interface Configuration

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

ip pim interface-type <active|passive> (for a port)

Specify whether the selected interface is active or passive. You can change the state of a PIM interface after you create the interface but only if you disable PIM on the interface. An active interface accepts PIM control transmitted and received traffic. A passive interface prevents PIM control traffic from transmitting or receiving, thereby reducing the load on a system. Use this feature when a high number of PIM interfaces exist and connect to end users, not to other switches.

Syntax

- `default ip pim interface-type`
- `ip pim interface-type active`
- `ip pim interface-type passive`

Default

`The default is active.`

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip pim interface-type <active|passive> (for a VLAN)

Specify whether the selected interface is active or passive. You can change the state of a PIM interface after you create the interface but only if you disable PIM on the interface. An active interface accepts PIM control transmitted and received traffic. A passive interface prevents PIM control traffic from transmitting or receiving, thereby reducing the load on a system. Use this feature when a high number of PIM interfaces exist and connect to end users, not to other switches.

Syntax

- `default ip pim interface-type`
- `ip pim interface-type active`
- `ip pim interface-type passive`

Default

`The default is active.`

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip pim join-prune-interval <1-18724> (for a port)

Specify how long to wait (in seconds) before the PIM router sends out the next join/prune message to its upstream neighbors.

Syntax

- `default ip pim join-prune-interval`
- `ip pim join-prune-interval <1-18724>`

Default

`The default is 60.`

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip pim join-prune-interval <1-18724> (for a VLAN)

Specify how long to wait (in seconds) before the PIM router sends out the next join/prune message to its upstream neighbors.

Syntax

- `default ip pim join-prune-interval`
- `ip pim join-prune-interval <1-18724>`

Default

`The default is 60.`

Command mode

VLAN Interface Configuration

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

ip pim join-prune-interval <1-18724> (globally)

Specify how long to wait (in seconds) before the PIM router sends out the next join/prune message to its upstream neighbors.

Syntax

- `default ip pim join-prune-interval`
- `ip pim join-prune-interval <1-18724>`

Default

`The default is 60.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip pim (loopback)

Enable PIM for the circuitless IP (CLIP) interface.

Syntax

- `default ip pim`
- `default ip pim <1-256>`
- `default ip pim <1-256> bsr-candidate vrf WORD<1-16>`
- `default ip pim bsr-candidate`
- `default ip pim bsr-candidate vrf WORD<1-16>`
- `default ip pim vrf WORD<1-16>`
- `ip pim`
- `ip pim <1-256>`
- `ip pim <1-256> bsr-candidate preference <0-255> vrf WORD<1-16>`
- `ip pim bsr-candidate preference <0-255>`
- `ip pim bsr-candidate preference <0-255> vrf WORD<1-16>`
- `ip pim vrf WORD<1-16>`
- `no ip pim`
- `no ip pim <1-256>`
- `no ip pim <1-256> bsr-candidate vrf WORD<1-16>`
- `no ip pim bsr-candidate`
- `no ip pim bsr-candidate vrf WORD<1-16>`
- `no ip pim vrf WORD<1-16>`

Default

The default is -1, which indicates that the current interface is not a C-BSR.

Command mode

Loopback Interface Configuration

Command parameters

Parameter	Description
<0-255>	Specifies the preference value.
<1-256>	Specifies the interface ID.

bsr-candidate preference	Enables the CLIP interface as a candidate bootstrap router and configure a preference value. The C-BSR with the highest BSR preference and address is the preferred BootStrap Router (BSR).
vrf WORD<1-16>	Specifies the VRF name.

©Avaya Inc. 2015 All Rights Reserved.

ip pim mode

Configure the mode of this interface globally. After you change from one mode to another, an information message appears to remind you that traffic does not stop immediately.

Syntax

- `default ip pim mode`
- `ip pim mode sparse`
- `ip pim mode ssm`

Default

`The default is sparse.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<ssm|sparse>`	Specifies the mode. Configures Source Specific Multicast (SSM) to optimize PIM-SM by simplifying the many-to-many model (servers-to-receivers).

©Avaya Inc. 2015 All Rights Reserved.

ip pim passive (for a port)

Enable PIM and configure the interface type to passive simultaneously. By default, an enabled interface is active.

Syntax

- `ip pim passive`

Default

`The default status is disabled.`

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip pim passive (for a VLAN)

Enable PIM and Configure the interface type to passive simultaneously. By default, an enabled interface is active.

Syntax

- `ip pim passive`

Default

`The default status is disabled.`

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip pim register-suppression-timeout <6-65535>

Specify how long (in seconds) the designated router (DR) suppresses sending registers to the RP. The timer starts after the DR receives a register-stop message from the RP.

Syntax

- `default ip pim register-suppression-timeout`
- `ip pim register-suppression-timeout <6-65535>`

Default

`The default is 60.`

Command mode

Global Configuration

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

ip pim rp-c-adv-timeout <5-26214>

Specify how often (in seconds) a router configured as a candidate RP (C-RP) sends C-RP advertisement messages. After this timer expires, the C-RP router sends an advertisement message to the elected BSR.

Syntax

- `default ip pim rp-c-adv-timeout`
- `ip pim rp-c-adv-timeout <5-26214>`

Default

`The default is 60.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip pim rp-candidate group

Configure a candidate rendezvous point (C-RP) to serve as backup to the RP router.

Syntax

- `default ip pim rp-candidate group <A.B.C.D> <A.B.C.D>`
- `ip pim rp-candidate group <A.B.C.D> <A.B.C.D> rp <A.B.C.D>`
- `no ip pim rp-candidate group <A.B.C.D> <A.B.C.D>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
{A.B.C.D} {A.B.C.D}	Specifies the IP address and group mask of the multicast group. When combined, they identify the prefix that the local router uses to advertise itself as a C-RP router.
rp {A.B.C.D}	Specifies the IP address of the C-RP router. This address must be one of the local PIM-SM enabled interfaces.

©Avaya Inc. 2015 All Rights Reserved.

ip pim static-rp

Adds a static rendezvous point (RP) entry and activates static RP.

Syntax

- `default ip pim static-rp`
- `ip pim static-rp <A.B.C.D/X> <A.B.C.D>`
- `no ip pim static-rp`

Default

The default is disabled.

Command mode

Global Configuration

Command parameters

Parameter	Description
<A.B.C.D/X>	Specifies the IP address and address mask of the multicast group. When combined, the IP address and address mask identify the range of the multicast addresses that the RP handles.
<A.B.C.D>	Specifies the IP address of the static RP.

©Avaya Inc. 2015 All Rights Reserved.

ip pim unicast-route-change-timeout <2-65535>

Specify how often (in seconds) the switch polls the routing table manager (RTM) for unicast routing information updates for PIM. Lowering this value increases how often the switch polls the RTM. This can affect the performance of the switch, especially when a high volume of traffic flows through the switch.

Syntax

- `default ip pim unicast-route-change-timeout`
- `ip pim unicast-route-change-timeout <2-65535>`

Default

`The default is 5.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip pim virtual-neighbor

Configure a virtual neighbor when the next hop for a static route cannot run PIM.

Syntax

- `ip pim virtual-neighbor <A.B.C.D> <A.B.C.D>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<A.B.C.D>	The first IP address indicates the IP address of the selected interface.
<A.B.C.D>	The second IP address Indicates the IP address of the neighbor.

©Avaya Inc. 2015 All Rights Reserved.

ip prefix-list

Allows or denies specific route updates. A prefix list policy specifies route prefixes to match. When there is a match, the route is used. Configure a prefix list and apply the list to any IP route policy.

Syntax

- `ip prefix-list WORD<1-64> {A.B.C.D/X}`
- `ip prefix-list WORD<1-64> {A.B.C.D/X} ge <0-32>`
- `ip prefix-list WORD<1-64> {A.B.C.D/X} le <0-32>`
- `ip prefix-list WORD<1-64> name WORD<1-64>`
- `no ip prefix-list WORD<1-64>`
- `no ip prefix-list WORD<1-64> {A.B.C.D/X}`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<A.B.C.D/X> [<ge|le> <0-32>]	Adds a prefix entry to the prefix list. A.B.C.D/X is the IP address and mask. <ge|le> <0-32> Lower bound and higher bound mask lengths together can define a range of networks. Use the no operator to remove a prefix entry from the prefix list: no ip prefix-list WORD<1-64> <A.B.C.D/X>
name WORD<1-64>	Renames the specified prefix list. The name length is from 1 to 64 characters.

©Avaya Inc. 2015 All Rights Reserved.

ip prefix-list (for a VRF)

Allows or denies specific route updates. A prefix list policy specifies route prefixes to match. When there is a match, the route is used. Configure a prefix list and apply the list to any IP route policy.

Syntax

- `ip prefix-list WORD<1-64> {A.B.C.D/X}`
- `ip prefix-list WORD<1-64> {A.B.C.D/X} ge <0-32>`
- `ip prefix-list WORD<1-64> {A.B.C.D/X} le <0-32>`
- `ip prefix-list WORD<1-64> name WORD<1-64>`
- `no ip prefix-list WORD<1-64>`
- `no ip prefix-list WORD<1-64> {A.B.C.D/X}`

Default

None

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
<A.B.C.D/X> [<ge|le> <0-32>]	Adds a prefix entry to the prefix list. A.B.C.D/X is the IP address and mask. <ge|le> <0-32> Lower bound and higher bound mask lengths together can define a range of networks. Use the no operator to remove a prefix entry from the prefix list: no ip prefix-list WORD<1-64> <A.B.C.D/X>
name WORD<1-64>	Renames the specified prefix list. The name length is from 1 to 64 characters.

©Avaya Inc. 2015 All Rights Reserved.

ip rip advertise-when-down enable (for a port)

Enable or disable AdvertiseWhenDown. If enabled, the network on this interface is advertised as up, even if the port is down. The default is disabled. When you configure a port with no link and enable advertise-when-down, it does not advertise the route until the port is active. Then the route is advertised even when the link is down. To disable advertising based on link status, this parameter must be disabled.

Syntax

- `default ip rip advertise-when-down enable`
- `ip rip advertise-when-down enable`
- `no ip rip advertise-when-down enable`

Default

`The default is disabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<enable|disable>`	Enables or disables AdvertiseWhenDown. If enabled, the network on this interface is advertised as up, even if the port is down. The default is disabled. When you configure a port with no link and enable advertise-when-down, it does not advertise the route until the port is active. Then the route is advertised even when the link is down. To disable advertising based on link status, this parameter must be disabled.

©Avaya Inc. 2015 All Rights Reserved.

ip rip advertise-when-down enable (for a VLAN)

Enable or disable AdvertiseWhenDown. If enabled, the network on this interface is advertised as up, even if the port is down. The default is disabled. When you configure a port with no link and enable advertise-when-down, it does not advertise the route until the port is active. Then the route is advertised even when the link is down. To disable advertising based on link status, this parameter must be disabled.

Syntax

- `default ip rip advertise-when-down enable`
- `ip rip advertise-when-down enable`
- `no ip rip advertise-when-down enable`

Default

`The default is disabled.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`<enable|disable>`	Enables or disables AdvertiseWhenDown. If enabled, the network on this interface is advertised as up, even if the port is down. The default is disabled. When you configure a port with no link and enable advertise-when-down, it does not advertise the route until the port is active. Then the route is advertised even when the link is down. To disable advertising based on link status, this parameter must be disabled.

©Avaya Inc. 2015 All Rights Reserved.

ip rip apply redistribute

Apply the RIP redistribution.

Syntax

- `ip rip apply redistribute`
- `ip rip apply redistribute vrf WORD<1-16>`
- `ip rip apply redistribute WORD<0-32>`
- `ip rip apply redistribute WORD<0-32> vrf WORD<1-16>`
- `ip rip apply redistribute WORD<0-32> vrf WORD<1-16> vrf-src WORD<1-16>`
- `ip rip apply redistribute WORD<0-32> vrf-src WORD<1-16>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies the VRF instance by name. When applying a redistribution instance that redistributes from a nonzero VRF to VRF 0 (the global router), do not specify the destination VRF; only specify the source VRF.
`vrf-src WORD<1-16>`	Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.
`WORD<0-32>`	Specifies the type of routes to be redistributed (the protocol source), including OSPF, BGP, static, direct, RIP.

©Avaya Inc. 2015 All Rights Reserved.

ip rip auto-aggregation enable (for a port)

Enable or disable automatic route aggregation on the port. When enabled, the router switch automatically aggregates routes to their natural mask when they are advertised on an interface in a different class network. The default is disabled.

Syntax

- `default ip rip auto-aggregation enable`
- `ip rip auto-aggregation enable`
- `no ip rip auto-aggregation enable`

Default

`The default is disabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables or disables automatic route aggregation on the port. When enabled, the router switch automatically aggregates routes to their natural mask when they are advertised on an interface in a different class network. The default is disabled.

©Avaya Inc. 2015 All Rights Reserved.

ip rip auto-aggregation enable (for a VLAN)

Enable or disable automatic route aggregation on the port. When enabled, the router switch automatically aggregates routes to their natural mask when they are advertised on an interface in a different class network. The default is disabled.

Syntax

- `default ip rip auto-aggregation enable`
- `ip rip auto-aggregation enable`
- `no ip rip auto-aggregation enable`

Default

`The default is disabled.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables or disables automatic route aggregation on the port. When enabled, the router switch automatically aggregates routes to their natural mask when they are advertised on an interface in a different class network. The default is disabled.

©Avaya Inc. 2015 All Rights Reserved.

ip rip cost (for a port)

Configure the RIP cost for this port (link).

Syntax

- `default ip rip cost`
- `ip rip cost <1-15>`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
<1-15>	Configures the RIP cost for this port (link).

©Avaya Inc. 2015 All Rights Reserved.

ip rip cost (for a VLAN)

Configure the RIP cost for this port (link).

Syntax

- `ip rip cost <1-15>`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
<1-15>	Configures the RIP cost for this interface.

©Avaya Inc. 2015 All Rights Reserved.

ip rip default-listen enable (for a port)

Enable default listen: the switch accepts the default route learned through RIP on this interface. The default is disabled.

Syntax

- `default ip rip default-listen enable`
- `ip rip default-listen enable`
- `no ip rip default-listen enable`

Default

`The default is disabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables DefaultListen: the switch accepts the default route learned through RIP on this interface. The default is disabled.

©Avaya Inc. 2015 All Rights Reserved.

ip rip default-listen enable (for a VLAN)

Enable default listen: the switch accepts the default route learned through RIP on this interface. The default is disabled.

Syntax

- `default ip rip default-listen enable`
- `ip rip default-listen enable`
- `no ip rip default-listen enable`

Default

`The default is disabled.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables DefaultListen: the switch accepts the default route learned through RIP on this interface. The default is disabled.

©Avaya Inc. 2015 All Rights Reserved.

ip rip default-supply enable (for a port)

Enable default supply. If enabled, a default route must be advertised from this interface. The default route is advertised only if it exists in the routing table. The default route will not be advertised on RIP interfaces by default. You need to redistribute the default route, and then configure the default-supply at the interface for the default route to be advertised to the neighbor.

Syntax

- `default ip rip default-supply enable`
- `ip rip default-supply enable`
- `no ip rip default-supply enable`

Default

`The default is false.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables DefaultSupply. If enabled, a default route must be advertised from this interface. The default is false. The default route is advertised only if it exists in the routing table.

©Avaya Inc. 2015 All Rights Reserved.

ip rip default-supply enable (for a VLAN)

Enable default supply. If enabled, a default route must be advertised from this interface. The default is false. The default route is advertised only if it exists in the routing table. The default route will not be advertised on RIP interfaces by default. You need to redistribute the default route, and then configure the default-supply at the interface for the default route to be advertised to the neighbor.

Syntax

- `default ip rip default-supply enable`
- `ip rip default-supply enable`
- `no ip rip default-supply enable`

Default

`The default is false.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables DefaultSupply. If enabled, a default route must be advertised from this interface. The default is false. The default route is advertised only if it exists in the routing table.

©Avaya Inc. 2015 All Rights Reserved.

ip rip enable (for a port)

Enable RIP routing on the interface.

Syntax

- `default ip rip enable`
- `ip rip enable`
- `no ip rip enable`

Default

`The default is disabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables RIP routing on the interface.

©Avaya Inc. 2015 All Rights Reserved.

ip rip enable (for a VLAN)

Enable RIP routing on the interface.

Syntax

- `ip rip enable`
- `no ip rip enable`

Default

`The default is disabled.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables RIP routing on the interface.

©Avaya Inc. 2015 All Rights Reserved.

ip rip holddown (for a port)

Configure the RIP holddown timer value, the length of time (in seconds) that RIP continues to advertise a network after determining that it is unreachable. The default is 120.

Syntax

- `default ip rip holddown`
- `ip rip holddown <0-360>`

Default

`The default is 120.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<0-360>`	Configures the RIP holddown timer value, the length of time (in seconds) that RIP continues to advertise a network after determining that it is unreachable. The default is 120.

©Avaya Inc. 2015 All Rights Reserved.

ip rip holddown (for a VLAN)

Configure the RIP holddown timer value, the length of time (in seconds) that RIP continues to advertise a network after determining that it is unreachable. The default is 120.

Syntax

- `ip rip holddown <0-360>`

Default

`The default is 120.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`<0-360>`	Configures the RIP holddown timer value, the length of time (in seconds) that RIP continues to advertise a network after determining that it is unreachable. The default is 120.

©Avaya Inc. 2015 All Rights Reserved.

ip rip in-policy (for a port)

Configure the port RIP in-policy. The policy name for inbound filtering on this RIP interface. This policy determines whether to learn a route on this interface. It also Specify the parameters of the route when it is added to the routing table.

Syntax

- `default ip rip in-policy`
- `ip rip in-policy WORD<0-64>`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
WORD<0-64>	Configures the port RIP in-policy. The policy name for inbound filtering on this RIP interface. This policy determines whether to learn a route on this interface. It also specifies the parameters of the route when it is added to the routing table.

©Avaya Inc. 2015 All Rights Reserved.

ip rip in-policy (for a VLAN)

Configure the port RIP in-policy. The policy name for inbound filtering on this RIP interface. This policy determines whether to learn a route on this interface. It also Specify the parameters of the route when it is added to the routing table.

Syntax

- `ip rip in-policy WORD<0-64>`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
WORD<0-64>	Configures the port RIP in-policy. The policy name for inbound filtering on this RIP interface. This policy determines whether to learn a route on this interface. It also specifies the parameters of the route when it is added to the routing table.

©Avaya Inc. 2015 All Rights Reserved.

ip rip listen (for a port)

If enabled, the switch listens for a default route without listening for all routes. Specify that the routing switch learns RIP routes through this interface. The default is enable.

Syntax

- `default ip rip listen enable`
- `ip rip listen enable`
- `no ip rip listen enable`

Default

`The default is enabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	If enabled, the switch listens for a default route without listening for all routes. Specifies that the routing switch learns RIP routes through this interface. The default is enable.

©Avaya Inc. 2015 All Rights Reserved.

ip rip listen (for a VLAN)

If enabled, the switch listens for a default route without listening for all routes. Specify that the routing switch learns RIP routes through this interface. The default is enable.

Syntax

- `default ip rip listen enable`
- `ip rip listen enable`
- `no ip rip listen enable`

Default

`The default is enabled.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`enable`	If enabled, the switch listens for a default route without listening for all routes. Specifies that the routing switch learns RIP routes through this interface. The default is enable.

©Avaya Inc. 2015 All Rights Reserved.

ip rip out-policy (for a port)

Configure the port RIP out-policy. The policy name for outbound filtering on this RIP interface. This policy determines whether to advertise a route from the routing table on this interface. This policy also Specify the parameters of the advertisement. policy name is a string of length 0 to 64 characters.

Syntax

- `default ip rip out-policy`
- `ip rip out-policy WORD<0-64>`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
WORD<0-64>	Configures the port RIP out-policy. The policy name for outbound filtering on this RIP interface. This policy determines whether to advertise a route from the routing table on this interface. This policy also specifies the parameters of the advertisement. policy name is a string of length 0 to 64 characters.

©Avaya Inc. 2015 All Rights Reserved.

ip rip out-policy (for a VLAN)

Configure the port RIP out-policy. The policy name for outbound filtering on this RIP interface. This policy determines whether to advertise a route from the routing table on this interface. This policy also Specify the parameters of the advertisement. policy name is a string of length 0 to 64 characters.

Syntax

- `ip rip out-policy WORD<0-64>`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
WORD<0-64>	Configures the port RIP out-policy. The policy name for outbound filtering on this RIP interface. This policy determines whether to advertise a route from the routing table on this interface. This policy also specifies the parameters of the advertisement. policy name is a string of length 0 to 64 characters.

©Avaya Inc. 2015 All Rights Reserved.

ip rip poison enable (for a port)

Enable Poison Reverse. If you disable Poison Reverse (no poison enable), Split Horizon is enabled. By default, Split Horizon is enabled. If Split Horizon is enabled, IP routes learned from an immediate neighbor are not advertised back to the neighbor. If Poison Reverse is enabled, the RIP updates sent to a neighbor from which a route is learned are poisoned with a metric of 16. Therefore, the receiver neighbor ignores this route because the metric 16 indicates infinite hops in the network. These mechanisms prevent routing loops.

Syntax

- `default ip rip poison enable`
- `ip rip poison enable`
- `no ip rip poison enable`

Default

`The default is disabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables Poison Reverse. If you disable Poison Reverse (no poison enable), Split Horizon is enabled. By default, Split Horizon is enabled. If Split Horizon is enabled, IP routes learned from an immediate neighbor are not advertised back to the neighbor. If Poison Reverse is enabled, the RIP updates sent to a neighbor from which a route is learned are poisoned with a metric of 16. Therefore, the receiver neighbor ignores this route because the metric 16 indicates infinite hops in the network. These mechanisms prevent routing loops.

©Avaya Inc. 2015 All Rights Reserved.

ip rip poison enable (for a VLAN)

Enable Poison Reverse. If you disable Poison Reverse (no poison enable), Split Horizon is enabled. By default, Split Horizon is enabled. If Split Horizon is enabled, IP routes learned from an immediate neighbor are not advertised back to the neighbor. If Poison Reverse is enabled, the RIP updates sent to a neighbor from which a route is learned are poisoned with a metric of 16. Therefore, the receiver neighbor ignores this route because the metric 16 indicates infinite hops in the network. These mechanisms prevent routing loops.

Syntax

- `default ip rip poison enable`
- `ip rip poison enable`
- `no ip rip poison enable`

Default

`The default is disabled.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables Poison Reverse. If you disable Poison Reverse (no poison enable), Split Horizon is enabled. By default, Split Horizon is enabled. If Split Horizon is enabled, IP routes learned from an immediate neighbor are not advertised back to the neighbor. If Poison Reverse is enabled, the RIP updates sent to a neighbor from which a route is learned are poisoned with a metric of 16. Therefore, the receiver neighbor ignores this route because the metric 16 indicates infinite hops in the network. These mechanisms prevent routing loops.

©Avaya Inc. 2015 All Rights Reserved.

ip rip port

Configure RIP for a port.

Syntax

- `default ip rip port {slot/port[-slot/port][,...]}`
- `ip rip port {slot/port[-slot/port][,...]}`
- `no ip rip port {slot/port[-slot/port][,...]}`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`{slot/port [-slot/port][…]}`	Configures RIP for a port.

©Avaya Inc. 2015 All Rights Reserved.

ip rip receive version (for a port)

Indicate which RIP update version is accepted on this interface. The default is rip1orrip2.

Syntax

- `default ip rip receive version`
- `ip rip receive version { rip1 | rip2 | rip1orrip2 }`

Default

`The default is rip1orrip 2.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<rip1|rip2|rip1orrip2>`	Indicates which RIP update version is accepted on this interface. The default is rip1orrip2.

©Avaya Inc. 2015 All Rights Reserved.

ip rip receive version (for a VLAN)

Indicate which RIP update version is accepted on this interface. The default is rip1orrip2.

Syntax

- `ip rip receive version { rip1 | rip2 | rip1orrip2 }`

Default

`The default is rip1orrip 2.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`<rip1|rip2|rip1orrip2>`	Indicates which RIP update version is accepted on this interface. The default is rip1orrip2.

©Avaya Inc. 2015 All Rights Reserved.

ip rip redistribute

Configure and enable redistribution entries to allow a protocol to announce routes of a certain source type, for example, static, RIP, or direct.

Syntax

- `default ip rip redistribute WORD<0-32>`
- `default ip rip redistribute WORD<0-32> enable`
- `default ip rip redistribute WORD<0-32> enable vrf-src WORD<1-16>`
- `default ip rip redistribute WORD<0-32> metric`
- `default ip rip redistribute WORD<0-32> metric vrf-src WORD<1-16>`
- `default ip rip redistribute WORD<0-32> route-map`
- `default ip rip redistribute WORD<0-32> route-map vrf-src WORD<1-16>`
- `default ip rip redistribute WORD<0-32> vrf-src WORD<1-16>`
- `ip rip redistribute WORD<0-32>`
- `ip rip redistribute WORD<0-32> enable`
- `ip rip redistribute WORD<0-32> enable vrf-src WORD<1-16>`
- `ip rip redistribute WORD<0-32> metric <0-65535>`
- `ip rip redistribute WORD<0-32> metric <0-65535> vrf-src WORD<1-16>`
- `ip rip redistribute WORD<0-32> route-map WORD<0-64>`
- `ip rip redistribute WORD<0-32> route-map WORD<0-64> vrf-src WORD<1-16>`
- `ip rip redistribute WORD<0-32> vrf-src WORD<1-16>`
- `no ip rip redistribute WORD<0-32>`
- `no ip rip redistribute WORD<0-32> enable`
- `no ip rip redistribute WORD<0-32> enable vrf-src WORD<1-16>`
- `no ip rip redistribute WORD<0-32> route-map`
- `no ip rip redistribute WORD<0-32> route-map vrf-src WORD<1-16>`
- `no ip rip redistribute WORD<0-32> vrf-src WORD<1-16>`

Default

None

Command mode

Command parameters

Parameter	Description
`enable`	Enables the route redistribution instance.
`metric <0-65535>`	Configures the metric to apply to redistributed routes.
`route-map WORD<0-64>`	Configures the route map to apply to redistributed routes.
`vrf WORD<1-16>`	Specifies the VRF instance.
`vrf-src WORD<1-16>`	Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.
`WORD<0-32>`	Specifies the type of routes to redistribute-the protocol source.

©Avaya Inc. 2015 All Rights Reserved.

ip rip send (for a port)

Indicate which RIP update version the router sends from this interface. ripVersion1 implies sending RIP updates that comply with RFC 1058. rip1Compatible implies broadcasting RIP2 updates using RFC 1058 route subassumption rules. The default is rip1Compatible

Syntax

- `default ip rip send version`
- `ip rip send version { notsend | rip1 | rip1comp | rip2 }`

Default

`The default is rip1Compatible.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<notsend|rip1|rip2|rip1comp|rip2>`	Indicates which RIP update version the router sends from this interface. ripVersion1 implies sending RIP updates that comply with RFC 1058. rip1Compatible implies broadcasting RIP2 updates using RFC 1058 route subassumption rules. The default is rip1Compatible

©Avaya Inc. 2015 All Rights Reserved.

ip rip send (for a VLAN)

Indicate which RIP update version the router sends from this interface. ripVersion1 implies sending RIP updates that comply with RFC 1058. rip1Compatible implies broadcasting RIP2 updates using RFC 1058 route subassumption rules. The default is rip1Compatible

Syntax

- `ip rip send version { notsend | rip1 | rip1comp | rip2 }`
- `ip rip send version { notsend | rip1 | rip1comp | rip2 } timeout <15-259200>`

Default

`The default is rip1Compatible.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`<notsend|rip1|rip2|rip1comp|rip2>`	Indicates which RIP update version the router sends from this interface. ripVersion1 implies sending RIP updates that comply with RFC 1058. rip1Compatible implies broadcasting RIP2 updates using RFC 1058 route subassumption rules. The default is rip1Compatible

©Avaya Inc. 2015 All Rights Reserved.

ip rip supply (for a port)

Specify that the switch advertises RIP routes through the port. The default is enable.

Syntax

- `default ip rip supply enable`
- `ip rip supply enable`
- `no ip rip supply enable`

Default

`The default is enabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`ip rip supply <enable|disable>`	Specifies that the switch advertises RIP routes through the port. The default is enable.

©Avaya Inc. 2015 All Rights Reserved.

ip rip supply (for a VLAN)

Specify that the switch advertises RIP routes through the port. The default is enable.

Syntax

- `default ip rip supply enable`
- `ip rip supply enable`
- `no ip rip supply enable`

Default

`The default is enabled.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`<enable|disable>`	Specifies that the switch advertises RIP routes through the port. The default is enable.

©Avaya Inc. 2015 All Rights Reserved.

ip rip timeout (for a port)

Configure the RIP timeout interval in seconds.

Syntax

- `default ip rip timeout`
- `ip rip timeout <15-259200>`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
<15-259200>	Configures the RIP timeout interval in seconds.

©Avaya Inc. 2015 All Rights Reserved.

ip rip timeout (for a VLAN)

Configure the RIP timeout interval in seconds.

Syntax

- `ip rip timeout <15-259200>`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
<15-259200>	Configures the RIP timeout interval in seconds.

©Avaya Inc. 2015 All Rights Reserved.

ip rip triggered (for a port)

Enable automatic triggered updates for RIP.

Syntax

- `default ip rip triggered enable`
- `ip rip triggered enable`
- `no ip rip triggered enable`

Default

`The default is disabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<enable|disable>`	Enables automatic triggered updates for RIP.

©Avaya Inc. 2015 All Rights Reserved.

ip rip triggered (for a VLAN)

Enable automatic triggered updates for RIP.

Syntax

- `default ip rip triggered enable`
- `ip rip triggered enable`
- `no ip rip triggered enable`

Default

`The default is disabled.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`<enable|disable>`	Enables automatically triggered updates for RIP.

©Avaya Inc. 2015 All Rights Reserved.

ip route (for a VRF)

Configure a default route for a VRF. To assign a static route to specify a gateway address route for the management interface, configure the static route in the MgmtRouter VRF context. You can specify up to four static routes for the management interface.

Syntax

- default ip route {A.B.C.D} {A.B.C.D} {A.B.C.D}
- default ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} dynamic
- default ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} enable
- default ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} local-next-hop enable
- default ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} preference
- ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} enable
- ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} enable next-hop-vrf WORD<1-16>
- ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} local-next-hop enable
- ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} preference <1-255>
- ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} preference <1-255> next-hop-vrf WORD<1-16>
- ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} weight <1-65535>
- ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} weight <1-65535> local-next-hop enable
- ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} weight <1-65535> next-hop-vrf WORD<1-16>
- ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} weight <1-65535> preference <1-255>
- no ip route {A.B.C.D} {A.B.C.D} {A.B.C.D}
- no ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} dynamic
- no ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} dynamic next-hop-vrf WORD<1-16>
- no ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} enable
- no ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} enable next-hop-vrf WORD<1-16>
- no ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} local-next-hop enable
- no ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} next-hop-vrf WORD<1-16>
- no ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} preference

Default

None

Command mode

Command parameters

Parameter	Description
{A.B.C.D} {A.B.C.D} {A.B.C.D}	Specifies the IP address, subnet mask, and next-hop address for the route. The first {A.B.C.D} configures the destination IP address of this route. An entry with a value of 0.0.0.0 is the default route. Multiple routes to a single destination can appear in the table, but access to such multiple entries depends on the network management protocol table access mechanisms. The second {A.B.C.D} configures the route network mask with the destination address before the switch compares the mask to the destination value. The third {A.B.C.D} configures the IP address of the next hop of this route. In the case of a route bound to an interface realized through a broadcast media, the value of this box is the agent IP address on that interface.
<1-255>	Indicates the route preference of this entry. If you can use more than one route to forward IP traffic, the switch uses the route with the highest preference. The higher the number, the higher the preference.
<1-65535>	Specifies the static route cost.
dynamic	Specifies a dynamic route.
enable	Adds a static or default route to the router or VRF.
local-next-hop enable	Enables the local next hop for this static route.
next-hop-vrf WORD<1-16>	Specifies the next-hop VRF instance by name.
next-hop-vrf WORD<1-16>	Specifies the VRF ID in inter-VRF static-route configuration.
preference <1-255>	Specifies the route preference.
weight <1-65535>	Specifies the static route cost.

©Avaya Inc. 2015 All Rights Reserved.

ip route (globally)

You can configure routing switches with a static default route, or they can learn it through a dynamic routing protocol.

Syntax

- `ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} enable`
- `ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} enable next-hop-vrf WORD<1-16>`
- `ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} local-next-hop enable`
- `ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} preference <1-255>`
- `ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} preference <1-255> next-hop-vrf WORD<1-16>`
- `ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} weight <1-65535>`
- `ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} weight <1-65535> local-next-hop enable`
- `ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} weight <1-65535> next-hop-vrf WORD<1-16>`
- `ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} weight <1-65535> preference <1-255>`
- `no ip route {A.B.C.D} {A.B.C.D} {A.B.C.D}`
- `no ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} dynamic`
- `no ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} dynamic next-hop-vrf WORD<1-16>`
- `no ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} enable`
- `no ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} enable next-hop-vrf WORD<1-16>`
- `no ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} local-next-hop enable`
- `no ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} next-hop-vrf WORD<1-16>`
- `no ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} preference`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`{A.B.C.D}`	The first and second <A.B.C.D> specify the IP address and mask for the route destination. 255.255.255.255 is the black hole route. Configures a black hole static route to the destination a router advertises to avoid routing loops when aggregating or injecting routes to other routers. The default route specifies a route to all networks for

	which there are no explicit routes in the Forwarding Information Base or the routing table. The default route has a prefix length of zero (RFC 1812).
enable	Adds a static or default route to the router or VRF.
local-next-hop enable	Enables the local next hop for this static route.
next-hop-vrf WORD<1-16>	Specifies the next-hop VRF instance by name.
preference <1-255>	Specifies the route preference.
weight <1-65535>	Specifies the static route cost.

©Avaya Inc. 2015 All Rights Reserved.

ip route preference ebgp

Configure the global route preference.

Syntax

- `default ip route preference protocol ebgp`
- `ip route preference protocol ebgp <0-255>`

Default

`The default is 45.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<0-255>`	Configures the preference value for the specified protocol. If two protocols have the same configured value, the default value is used.

©Avaya Inc. 2015 All Rights Reserved.

ip route preference ibgp

Configure the global route preference.

Syntax

- `default ip route preference protocol ibgp`
- `ip route preference protocol ibgp <0-255>`

Default

`The default is 175.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<0-255>`	Configures the preference value for the specified protocol. If two protocols have the same configured value, the default value is used.

©Avaya Inc. 2015 All Rights Reserved.

ip route preference ospf-extern1

Configure the global route preference.

Syntax

- `default ip route preference protocol ospf-extern1`
- `ip route preference protocol ospf-extern1 <0-255>`

Default

`The default is 120.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<0-255>`	Configures the preference value for the specified protocol. If two protocols have the same configured value, the default value is used.

©Avaya Inc. 2015 All Rights Reserved.

ip route preference ospf-extern2

Configure the global route preference.

Syntax

- `default ip route preference protocol ospf-extern2`
- `ip route preference protocol ospf-extern2 <0-255>`

Default

`The default is 125.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<0-255>`	Configures the preference value for the specified protocol. If two protocols have the same configured value, the default value is used.

©Avaya Inc. 2015 All Rights Reserved.

ip route preference ospf-inter

Configure the global route preference.

Syntax

- `default ip route preference protocol ospf-inter`
- `ip route preference protocol ospf-inter <0-255>`

Default

`The default is 25.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<0-255>`	Configures the preference value for the specified protocol. If two protocols have the same configured value, the default value is used.

©Avaya Inc. 2015 All Rights Reserved.

ip route preference ospf-intra

Configure the global route preference.

Syntax

- `default ip route preference protocol ospf-intra`
- `ip route preference protocol ospf-intra <0-255>`

Default

`The default is 20.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<0-255>`	Configures the preference value for the specified protocol. If two protocols have the same configured value, the default value is used.

©Avaya Inc. 2015 All Rights Reserved.

ip route preference ospfv3-extern1

Configure the global route preference.

Syntax

- `default ip route preference protocol ospfv3-extern1`
- `ip route preference protocol ospfv3-extern1 <0-255>`

Default

`The default is 120.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<0-255>`	Configures the preference value for the specified protocol. If two protocols have the same configured value, the default value is used.

©Avaya Inc. 2015 All Rights Reserved.

ip route preference ospfv3-extern2

Configure the global route preference.

Syntax

- `default ip route preference protocol ospfv3-extern2`
- `ip route preference protocol ospfv3-extern2 <0-255>`

Default

`The default is 125.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<0-255>`	Configures the preference value for the specified protocol. If two protocols have the same configured value, the default value is used.

©Avaya Inc. 2015 All Rights Reserved.

ip route preference ospfv3-inter

Configure the global route preference.

Syntax

- `default ip route preference protocol ospfv3-inter`
- `ip route preference protocol ospfv3-inter <0-255>`

Default

`The default is 25.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<0-255>`	Configures the preference value for the specified protocol. If two protocols have the same configured value, the default value is used.

©Avaya Inc. 2015 All Rights Reserved.

ip route preference ospfv3-intra

Configure the global route preference.

Syntax

- `default ip route preference protocol ospfv3-intra`
- `ip route preference protocol ospfv3-intra <0-255>`

Default

`The default is 20.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<0-255>`	Configures the preference value for the specified protocol. If two protocols have the same configured value, the default value is used.

©Avaya Inc. 2015 All Rights Reserved.

ip route preference rip

Configure the global route preference.

Syntax

- `default ip route preference protocol rip`
- `ip route preference protocol rip <0-255>`

Default

`The default is 100.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<0-255>`	Configures the preference value for the specified protocol. If two protocols have the same configured value, the default value is used.

©Avaya Inc. 2015 All Rights Reserved.

ip route preference spbm-level1

Configure the global route preference.

Syntax

- `default ip route preference protocol spbm-level1`
- `ip route preference protocol spbm-level1 <0-255>`

Default

`The default is 7.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<0-255>`	Configures the preference value for the specified protocol. If two protocols have the same configured value, the default value is used.

©Avaya Inc. 2015 All Rights Reserved.

ip route preference static

Configure the global route preference.

Syntax

- `default ip route preference protocol static`
- `ip route preference protocol static <0-255>`

Default

`The default is 5.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<0-255>`	Configures the preference value for the specified protocol. If two protocols have the same configured value, the default value is used.

©Avaya Inc. 2015 All Rights Reserved.

ip route preference staticv6

Configure the global route preference.

Syntax

- `default ip route preference protocol staticv6`
- `ip route preference protocol staticv6 <0-255>`

Default

`The default is 5.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<0-255>`	Configures the preference value for the specified protocol. If two protocols have the same configured value, the default value is used.

©Avaya Inc. 2015 All Rights Reserved.

ip routing

Enable IP forwarding (routing) on a global level so that the router supports routing. You can use the IP address of any router interface for IP-based network management.

Syntax

- `ip routing`
- `no ip routing`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
routing	Enables IP routing.

©Avaya Inc. 2015 All Rights Reserved.

ip rsmlt

Configure Routed Split MultiLink Trunking (RSMLT) on an IPv4 or IPv6 VLAN interface.

Syntax

- `default ip rsmlt`
- `default ip rsmlt holddown-timer`
- `default ip rsmlt holdup-timer`
- `ip rsmlt`
- `ip rsmlt holddown-timer <0-3600>`
- `ip rsmlt holdup-timer <0-9999>`
- `no ip rsmlt`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`holddown-timer<0-3600>`	Defines how long the RSMLT switch does not participate in Layer 3 forwarding. <0-3600> is the timer value in seconds. Avaya recommends that you configure this value to be longer than the anticipated routing protocol convergence. The default holddown timer is 60.
`holdup-timer<0-3600|9999>`	Defines how long the RSMLT switch maintains forwarding for its peer. 0-3600 is the timer value in seconds. 9999 means infinity. The default holdup timer is 180.

©Avaya Inc. 2015 All Rights Reserved.

ip rsmlt edge-support

Configure Routed Split MultiLink trunking (RSMLT)-edge to store the RSMLT peer MAC/IP address-pair in its local config file and restore the configuration if the peer does not restore after a simultaneous reboot of both RSMLT-peer switches. The configuration applies to both IPv4 and IPv6.

Syntax

- `default ip rsmlt edge-support`
- `ip rsmlt edge-support`
- `no ip rsmlt edge-support`

Default

`The default is disabled.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`edge-support`	Enables RSMLT-edge support.

©Avaya Inc. 2015 All Rights Reserved.

ip rvs-path-chk (for a port)

You can enable, disable or reset the unicast reverse path checking feature to its default setting. The unicast reverse path checking feature can reduce problems associated with malformed or spoofed IP source addresses in a network.

Syntax

- `default ip rvs-path-chk`
- `ip rvs-path-chk`
- `no ip rvs-path-chk`

Default

`The default status is disabled.`

Command mode

GigabitEthernet Interface Configuration

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

ip rvs-path-chk (for a VLAN)

You can enable, disable or reset the unicast reverse path checking feature to its default setting. The unicast reverse path checking feature can reduce problems associated with malformed or spoofed IP source addresses in a network.

Syntax

- `default ip rvs-path-chk`
- `ip rvs-path-chk`
- `no ip rvs-path-chk`

Default

`The default status is disabled.`

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip rvs-path-chk mode (for a port)

Use the unicast reverse path checking feature to reduce the problems that are caused by the introduction of malformed or forged (spoofed) IP source addresses into a network.

Syntax

- `default ip rvs-path-chk mode`
- `ip rvs-path-chk mode exist-only`
- `ip rvs-path-chk mode strict`

Default

`The ip rvs-path-chk mode port default is exist-only.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`mode <exist-only|strict>`	Specifies the mode for reverse path checking. In exist-only mode, reverse path checking checks whether the source IP address of the incoming packet exists in the routing table. In strict mode, reverse path checking checks whether the source IP address of the incoming packet exists in the routing table.

©Avaya Inc. 2015 All Rights Reserved.

ip rvs-path-chk mode (for a VLAN)

Use the unicast reverse path checking feature to reduce the problems that are caused by the introduction of malformed or forged (spoofed) IP source addresses into a network.

Syntax

- `default ip rvs-path-chk mode`
- `ip rvs-path-chk mode exist-only`
- `ip rvs-path-chk mode strict`

Default

`The ip rvs-path-chk mode port default is exist-only.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`mode <exist-only|strict>`	Specifies the mode for reverse path checking. In exist-only mode, reverse path checking checks whether the source IP address of the incoming packet exists in the routing table. In strict mode, reverse path checking checks whether the source IP address of the incoming packet exists in the routing table.

©Avaya Inc. 2015 All Rights Reserved.

ip-source-address

Configure the circuitless IP (CLIP) interface as the source address for SPBM IP Shortcuts. Assigns a source IP address for locally generated IP packets whose egress port is an SPBM NNI port. The source-address value must be a locally configured loopback IP address. The IS-IS automatically advertises the source-address to other SPBM edge routers when you enable IP shortcuts. You must first configure a valid source-address before you enable IP shortcuts.

Syntax

- `ip-source-address {A.B.C.D}`
- `no ip-source-address`

Default

None

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description
<A.B.C.D>	Specifies the circuitless IP (CLIP) interface as the source address for SPBM IP shortcuts.

©Avaya Inc. 2015 All Rights Reserved.

ip spb-multicast enable (for a port)

Enables Layer 3 VSN IP multicast over SPBM.

Syntax

- `default ip spb-multicast enable`
- `ip spb-multicast enable`
- `no ip spb-multicast enable`

Default

`The default is disabled.`

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip spb-multicast enable (for a VLAN)

Enables Layer 3 VSN IP multicast over SPBM.

Syntax

- `default ip spb-multicast enable`
- `ip spb-multicast enable`
- `no ip spb-multicast enable`

Default

`The default is disabled.`

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip supernet

Enable or disable supernetting. If supernetting is globally enabled, the switch can learn routes with a route mask of less then eight bits. Routes with a mask length less than eight bits cannot have ECMP paths, even if the ECMP feature is globally enabled.

Syntax

- `default ip supernet`
- `ip supernet`
- `no ip supernet`

Default

`The default is disabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip ttl

Configure the IP routing protocol stack to specify which routing features the switch can use.

Syntax

- `default ip ttl`
- `ip ttl <1-255>`
- `no ip ttl`

Default

`The default value is 255.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`ttl<1-255>`	Configures the default time-to-live (TTL) value for a routed packet. The TTL is the maximum number of seconds before a packet is discarded. The default value of 255 is used whenever a time is not supplied in the datagram header.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 area

Create and configure an OSPFv3 IPv6 area.

Syntax

- `default ipv6 area {A.B.C.D}`
- `default ipv6 area {A.B.C.D} default-cost`
- `default ipv6 area {A.B.C.D} import`
- `default ipv6 area {A.B.C.D} import-summaries enable`
- `ipv6 area {A.B.C.D}`
- `ipv6 area {A.B.C.D} default-cost <0-16777215>`
- `ipv6 area {A.B.C.D} import external`
- `ipv6 area {A.B.C.D} import noexternal`
- `ipv6 area {A.B.C.D} import nssa`
- `ipv6 area {A.B.C.D} import-summaries enable`
- `ipv6 area {A.B.C.D} translator-role <1-2>`
- `ipv6 area {A.B.C.D} type nssa`
- `ipv6 area {A.B.C.D} type stub`
- `no ipv6 area {A.B.C.D}`
- `no ipv6 area {A.B.C.D} import-summaries enable`

Default

None

Command mode

OSPF Router Configuration

Command parameters

Parameter	Description
`{A.B.C.D}`	Specifies the area address.
`default-cost <0-16777215>`	Specifies the stub metric for the area. The default-cost default is 10.
`import <external|noexternal|nssa>`	Configures the area support for importing advertisements. The default is external.
`import-summaries enable`	Configures the area support for importing summary advertisements into a stub area. Use this entry only for a stub

	area. The default is enabled.
`translator-role {1|2}`	Indicates a Not-So-Stubby-Area (NSSA) border router ability to perform translation of type-7 LSAs into type-5 LSAs. Configure this value to 2 to make it a candidate. You can configure this parameter only when you first create the area. The default translator-role is 1.
`type {nssa|stub}`	Configures the type of area. A Not-So-Stubby-Area (NSSA) prevents flooding of normal route advertisements into the area by replacing them with a default route. A stub area uses only one exit point (router interface) out of the area. You can configure this parameter only when you first create the area. By default, the area is neither a stub area or NSSA (Not-So-Stubby Area).

©Avaya Inc. 2015 All Rights Reserved.

ipv6 area range

Create and configure an area address range on the OSPF router to reduce the number of ABR advertisements into other OSPF areas.

Syntax

- `default ipv6 area range {A.B.C.D} WORD<0-255> inter-area-prefix-link [advertise-metric]`
- `default ipv6 area range {A.B.C.D} WORD<0-255> nssa-extlink [advertise-metric]`
- `ipv6 area range {A.B.C.D} WORD<0-255> advertise-mode advertise`
- `ipv6 area range {A.B.C.D} WORD<0-255> advertise-mode not-advertise`
- `ipv6 area range {A.B.C.D} WORD<0-255> inter-area-prefix-link advertise-metric <0-65535>`
- `ipv6 area range {A.B.C.D} WORD<0-255> inter-area-prefix-link advertise-mode advertise`
- `ipv6 area range {A.B.C.D} WORD<0-255> inter-area-prefix-link advertise-mode not-advertise`
- `ipv6 area range {A.B.C.D} WORD<0-255> nssa-extlink advertise-metric <0-65535>`
- `ipv6 area range {A.B.C.D} WORD<0-255> nssa-extlink advertise-mode advertise`
- `ipv6 area range {A.B.C.D} WORD<0-255> nssa-extlink advertise-mode not-advertise`
- `no ipv6 area range {A.B.C.D} WORD<0-255> inter-area-prefix-link`
- `no ipv6 area range {A.B.C.D} WORD<0-255> nssa-extlink`

Default

None

Command mode

OSPF Router Configuration

Command parameters

Parameter	Description
{A.B.C.D}	Specifies the area address.
advertise-metric <0-65535>	Specifies the advertise metric value and LSA type. The default advertise-metric is 0.
advertise-mode <advertise|not-advertise>	Configures if the area advertises into other OSPF areas. The default avertise-mode is advertise.
inter-area-prefix-link	Configures the area to use this LSA type.
nssa-extlink	Configures the area to use this LSA type.
WORD<0-255>	Specifies the IPv6 address and prefix.

©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

ipv6 area virtual-link

Configure an OSPF virtual interface to the ABR if a remote OSPF ABR uses no connection to the backbone area but needs to be part of the same routing domain in which the switch resides.

Syntax

- `default ipv6 area virtual-link {A.B.C.D} {A.B.C.D}`
- `default ipv6 area virtual-link {A.B.C.D} {A.B.C.D} [dead-interval][retransmit-interval] [transit-delay]`
- `default ipv6 area virtual-link {A.B.C.D} {A.B.C.D} dead-interval`
- `default ipv6 area virtual-link {A.B.C.D} {A.B.C.D} hello-interval`
- `default ipv6 area virtual-link {A.B.C.D} {A.B.C.D} retransmit-interval`
- `default ipv6 area virtual-link {A.B.C.D} {A.B.C.D} transit-delay`
- `ipv6 area virtual-link {A.B.C.D} {A.B.C.D}`
- `ipv6 area virtual-link {A.B.C.D} {A.B.C.D} dead-interval <1-65535>`
- `ipv6 area virtual-link {A.B.C.D} {A.B.C.D} hello-interval <1-65535>`
- `ipv6 area virtual-link {A.B.C.D} {A.B.C.D} retransmit-interval <1-1800>`
- `ipv6 area virtual-link {A.B.C.D} {A.B.C.D} transit-delay <1-1800>`
- `no ipv6 area virtual-link {A.B.C.D} {A.B.C.D}`

Default

None

Command mode

OSPF Router Configuration

Command parameters

Parameter	Description
`{A.B.C.D} {A.B.C.D}`	Specifies the area address and the virtual link address.
`dead-interval <1-65535>`	Specifies the dead interval, as the number of seconds to wait before determining the OSPF router is down. The default dead-interval is 60.
`hello-interval <1-65535>`	Specifies the hello interval, in seconds, for hello packets sent between switches for a virtual interface in an OSPF area. The default hello interval is 10.
`retransmit-interval <1-1800>`	Specifies the retransmit interval, in seconds, for link-state advertisements. The default retransmit-interval is 5.
`transit-delay <1-1800>`	Specifies the transit-delay interval, in seconds, required to transmit a link-state update packet over the virtual interface. The default transit-delay is 1.

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

Home | Command modes | Alphabetical listing

ipv6 as-boundary-router

Enable or disable the boundary-router on the router interface.

Syntax

- `default ipv6 as-boundary-router [enable]`
- `ipv6 as-boundary-router`
- `ipv6 as-boundary-router enable`
- `no ipv6 as-boundary-router [enable]`

Default

`The default is disabled.`

Command mode

OSPF Router Configuration

Command parameters

Parameter	Description
`enable`	Enables the boundary-router.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 dhcp-relay (for a port)

Configure Dynamic Host Configuration Protocol (DHCP) Relay on an interface. The command no ipv6 dhcp-relay disables DHCP on the interface, it does not delete the entry.

Syntax

- `default ipv6 dhcp-relay`
- `default ipv6 dhcp-relay fwd-path WORD<0-255>`
- `default ipv6 dhcp-relay max-hop`
- `default ipv6 dhcp-relay remote-id`
- `ipv6 dhcp-relay`
- `ipv6 dhcp-relay fwd-path WORD<0-255>`
- `ipv6 dhcp-relay fwd-path WORD<0-255> enable`
- `ipv6 dhcp-relay fwd-path WORD<0-255> vrid WORD<1-255>`
- `ipv6 dhcp-relay max-hop <1-32>`
- `ipv6 dhcp-relay remote-id`
- `no ipv6 dhcp-relay`
- `no ipv6 dhcp-relay fwd-path WORD<0-255>`
- `no ipv6 dhcp-relay fwd-path WORD<0-255> enable`
- `no ipv6 dhcp-relay remote-id`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
max-hop <1-32>	Configures the maximum number of hops before a BootP/DHCP packet is discarded. The default is 32.
remoteId	Enables the Remote ID. The default is disabled.
vrid WORD<1-255>	Specifies the ID of the virtual router and is an integer from 1-255.
WORD<0-	Creates a forwarding path to the Dynamic Host Configuration Protocol (DHCP) server with a mode and a state. WORD<0-255> is the IPv6 address of the server. The default IP

255> address of the relay is the address of the interface. If the relay is a Virtual Router configured on this interface, you must set the vrid. By default, the forwarding path is disabled.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 dhcp-relay (for a VLAN)

Configure Dynamic Host Configuration Protocol (DHCP) Relay on an interface. The command no ipv6 dhcp-relay disables DHCP on the interface, it does not delete the entry.

Syntax

- `default ipv6 dhcp-relay`
- `default ipv6 dhcp-relay fwd-path WORD<0-255>`
- `default ipv6 dhcp-relay max-hop`
- `default ipv6 dhcp-relay remote-id`
- `ipv6 dhcp-relay`
- `ipv6 dhcp-relay fwd-path WORD<0-255>`
- `ipv6 dhcp-relay fwd-path WORD<0-255> enable`
- `ipv6 dhcp-relay fwd-path WORD<0-255> vrid WORD<1-255>`
- `ipv6 dhcp-relay max-hop <1-32>`
- `ipv6 dhcp-relay remoteId`
- `no ipv6 dhcp-relay`
- `no ipv6 dhcp-relay fwd-path WORD<0-255>`
- `no ipv6 dhcp-relay fwd-path WORD<0-255> enable`
- `no ipv6 dhcp-relay remoteId`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
max-hop <1-32>	Configures the maximum number of hops before a BootP/DHCP packet is discarded. The default is 32.
remoteId	Enables the Remote ID. The default is disabled.
vrid WORD<1-255>	Specifies the ID of the virtual router and is an integer from 1-255.
WORD<0-	Creates a forwarding path to the Dynamic Host Configuration Protocol (DHCP) server with a mode and a state. WORD<0-255> is the IPv6 address of the server. The default IP

255> address of the relay is the address of the interface. If the relay is a Virtual Router configured on this interface, you must set the vrid. By default, the forwarding path is disabled.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 dhcp-relay fwd-path

Create the forwarding path from the client to the server.

Syntax

- `default ipv6 dhcp-relay fwd-path WORD<0-255> WORD<0-255>`
- `ipv6 dhcp-relay fwd-path WORD<0-255> WORD<0-255>`
- `ipv6 dhcp-relay fwd-path WORD<0-255> WORD<0-255> enable`
- `no ipv6 dhcp-relay fwd-path WORD<0-255> WORD<0-255>`
- `no ipv6 dhcp-relay fwd-path WORD<0-255> WORD<0-255> enable`

Default

`The default is disabled.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`enable`	Enables the forwarding path to the server.
`WORD<0-255>`	Configures the forwarding path from the client to the server. The first WORD<0-255> is the IP address configured on an interface (a locally configured IP address) to forward or relay BootP or DHCP. This address is the relay agent. The relay can be a VRRP address.
`WORD<0-255>`	The second WORD<0-255> is the IP address of the DHCP server in the network. If this IP address corresponds to the locally configured IP network the system generates an error because IPv6 does not include broadcast.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 forwarding (for a port)

Configure IPv6 forwarding. By default, IPv6 forwarding is globally disabled, which means you can only use local IPv6 connections, and traffic does not traverse an IPv6 network.

Syntax

- `default ipv6 forwarding`
- `ipv6 forwarding`
- `no ipv6 forwarding`

Default

By default, forwarding is enabled on an interface. You must enable it globally before the interface configuration takes effect.

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ipv6 forwarding (for a VLAN)

Configure IPv6 forwarding. By default, IPv6 forwarding is globally disabled, which means you can only use local IPv6 connections, and traffic does not traverse an IPv6 network.

Syntax

- `default ipv6 forwarding`
- `ipv6 forwarding`
- `no ipv6 forwarding`

Default

By default, forwarding is enabled on an interface. You must enable it globally before the interface configuration takes effect.

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ipv6 forwarding (globally)

Configure IPv6 forwarding. By default, IPv6 forwarding is globally disabled, which means you can only use local IPv6 connections, and traffic does not traverse an IPv6 network.

Syntax

- `default ipv6 forwarding`
- `ipv6 forwarding`
- `no ipv6 forwarding`

Default

By default, forwarding is globally disabled. You must enable it globally before the interface configuration takes effect.

Command mode

Global Configuration

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.

ipv6 hop-limit

Insert a value into the hop-limit field of the IPv6 header.

Syntax

- `default ipv6 hop-limit <0-255>`
- `ipv6 hop-limit <0-255>`

Default

`The default hop limit is 64.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<0-255>`	Inserts a value into the hop-limit field of IPv6 header in the range of 0 to 255.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 icmp error-interval

Configure the interval (in milliseconds) for sending ICMPv6 error messages.

Syntax

- `default ipv6 icmp error-interval`
- `ipv6 icmp error-interval <0-2147483647>`

Default

`The default error interval is 1000.`

Command mode

Global Configuration

Command parameters

Parameter	Description
<0-2147483647>	Configures the interval (in milliseconds) for sending ICMPv6 error messages. An entry of 0 seconds results in no sent ICMPv6 error messages

©Avaya Inc. 2015 All Rights Reserved.

ipv6 icmp error-quota

Configure the number of Internet Control Message Protocol (ICMP) error messages that can be sent during the ICMP error interval.

Syntax

- `default ipv6 icmp error-quota`
- `ipv6 icmp error-quota <0-2000000>`

Default

`The default error quota is 50.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<0-2000000>`	Configures the number of internet Control Message Protocol (ICMP) error messages that the system can send during the ICMP error interval. A value of zero instructs the system not to send any ICMP error messages.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 icmp redirect-msg

Enable Internet Control Message Protocol (ICMP) redirect messages.

Syntax

- `default ipv6 icmp redirect-msg`
- `ipv6 icmp redirect-msg`
- `no ipv6 icmp redirect-msg`

Default

By default ICMP redirect messages are disabled.

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

ipv6 icmp unreach-msg

Enable Internet Control Message Protocol (ICMP) network unreachable messages.

Syntax

- `default ipv6 icmp unreach-msg`
- `ipv6 icmp unreach-msg`
- `no ipv6 icmp unreach-msg`

Default

`By default ICMP network unreachable messages are disabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface address (for a port)

Configure the IPv6 address for a port.

Syntax

- `ipv6 interface address WORD<0-255>`
- `no ipv6 interface address`
- `no ipv6 interface address WORD<0-255>`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
WORD<0-255>	Assigns an IPv6 address to the port.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface address (for a VLAN)

Configure the IPv6 address for a VLAN.

Syntax

- `ipv6 interface address WORD<0-255>`
- `no ipv6 interface address WORD<0-255>`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
WORD<0-255>	Assigns an IPv6 address to the VLAN.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface address (for the management port)

Configure the IPv6 address for the Ethernet management port.

Syntax

- `ipv6 interface address WORD<0-255>`
- `no ipv6 interface address WORD<0-255>`

Default

None

Command mode

mgmtEthernet Interface Configuration

Command parameters

Parameter	Description
WORD<0-255>	Assigns an IPv6 address to the management port.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface enable (for a port)

Enable IPv6 route advertisement on a port.

Syntax

- `default ipv6 interface enable`
- `ipv6 interface enable`
- `ipv6 interface enable vlan <1-4084>`
- `no ipv6 interface enable`

Default

`The default is disabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`vlan <1-4084>`	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface enable (for a VLAN)

Enable IPv6 route advertisement on a VLAN.

Syntax

- `default ipv6 interface enable`
- `ipv6 interface enable`
- `no ipv6 interface enable`

Default

`The default is disabled.`

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface enable (for the management port)

Enable IPv6 route advertisement on the Ethernet management port.

Syntax

- `default ipv6 interface enable`
- `ipv6 interface enable`
- `no ipv6 interface enable`

Default

`The default is disabled.`

Command mode

mgmtEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface (for a port)

Creates an IPv6 interface.

Syntax

- `default ipv6 interface`
- `ipv6 interface`
- `no ipv6 interface`

Default

None

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface hop-limit (for a port)

Configure the maximum number of hops before packets drop.

Syntax

- `default ipv6 interface hop-limit`
- `ipv6 interface hop-limit <1-255>`

Default

`The default is 64 hops.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
<1-255>	Configures the maximum hops.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface hop-limit (for a VLAN)

Configure the maximum number of hops before packets drop.

Syntax

- `default ipv6 interface hop-limit`
- `ipv6 interface hop-limit <1-255>`

Default

`The default is 64 hops.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
<1-255>	Configures the maximum hops.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface hop-limit (for the management port)

Configure the maximum number of hops before packets drop.

Syntax

- `default ipv6 interface hop-limit`
- `ipv6 interface hop-limit <1-255>`

Default

`The default is 30 hops.`

Command mode

mgmtEthernet Interface Configuration

Command parameters

Parameter	Description
<1-255>	Configures the maximum hops.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface link-local (for a port)

Create a link-local address for the port.

Syntax

- `ipv6 interface link-local WORD<0-19>`
- `ipv6 interface link-local WORD<0-19> address WORD<0-46>`
- `ipv6 interface link-local WORD<0-19> enable`
- `ipv6 interface link-local WORD<0-19> mac-offset <0-1535>`
- `ipv6 interface link-local WORD<0-19> name WORD<0-255>`
- `ipv6 interface link-local WORD<0-19> vlan <1-4084>`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
address WORD<0-46>	Specifies the IPv6 address.
enable	Enables route advertisement.
mac-offset <0-1535>	Use mac-offset to request a particular MAC for an IPv6 VLAN. The system has 1536 MAC addresses. The last four addresses are reserved. You can specify a MAC offset when you configure IPv6 on a VLAN, or the system can assign a MAC address from within the available range.
name WORD<0-255>	Assigns a descriptive name. The network management system also configures this string.
vlan <1-4084>	Specifies the VLAN associated with this entry. This value corresponds to the lower 12 bits of the IEEE 802.1Q VLAN tag.
WORD<0-19>	Specifies the 64-bit interface ID used to calculate the actual link-local address.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface link-local (for a VLAN)

Create a link-local address for the VLAN.

Syntax

- `ipv6 interface link-local WORD<0-19>`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
WORD<0-19>	Specifies the 64-bit interface ID used to calculate the actual link-local address.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface link-local (for the management port)

Create a link-local address for the Ethernet management port.

Syntax

- `ipv6 interface link-local WORD<0-19>`

Default

None

Command mode

mgmtEthernet Interface Configuration

Command parameters

Parameter	Description
WORD<0-19>	Specifies the link-local address for the management port.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface mac-offset

Request a MAC for an IPv6 VLAN.

Syntax

- `ipv6 interface mac-offset <0-1535>`

Default

None

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface mtu (for a port)

Configure the maximum transmission unit for the port.

Syntax

- `default ipv6 interface mtu`
- `ipv6 interface mtu <1280-9500>`

Default

`The default is 1500.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<1280-9500>`	Configures the maximum transmission unit for the interface: 1280-1500, 1850, or 9500.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface mtu (for a VLAN)

Configure the maximum transmission unit for the VLAN.

Syntax

- `default ipv6 interface mtu`
- `ipv6 interface mtu <1280-9500>`

Default

`The default is 1500.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`<1280-9500>`	Configures the maximum transmission unit for the interface: 1280-1500, 1850, or 9500.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface mtu (for the management port)

Configure the maximum transmission unit for the Ethernet management port.

Syntax

- `default ipv6 interface mtu`
- `ipv6 interface mtu <1280-1500>`

Default

`The default is 1500.`

Command mode

mgmtEthernet Interface Configuration

Command parameters

Parameter	Description
`<1280-1500>`	Configures the maximum transmission unit for the interface.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface name (for a port)

Configure an interface description for the port.

Syntax

- `ipv6 interface name WORD<0-255>`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
WORD<0-255>	Assigns a descriptive name to the port.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface name (for a VLAN)

Configure an interface description for the VLAN.

Syntax

- `ipv6 interface name WORD<0-255>`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
WORD<0-255>	Assigns a descriptive name to the VLAN.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface name (for the management port)

Configure an interface description for the Ethernet management port.

Syntax

- `ipv6 interface name WORD<0-255>`

Default

None

Command mode

mgmtEthernet Interface Configuration

Command parameters

Parameter	Description
WORD<0-255>	Assigns a descriptive name to the management port.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface reachable-time (for a port)

Configure the time a neighbor is considered reachable after receiving a reachability confirmation.

Syntax

- `default ipv6 interface reachable-time`
- `ipv6 interface reachable-time <1-3600000>`

Default

`The default is 30000.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
<1-3600000>	Configures the time, in milliseconds, a neighbor is considered reachable after receiving a reachability confirmation.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface reachable-time (for a VLAN)

Configure the time a neighbor is considered reachable after receiving a reachability confirmation.

Syntax

- `default ipv6 interface reachable-time`
- `ipv6 interface reachable-time <1-3600000>`

Default

`The default is 30000.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`<1-3600000>`	Configures the time, in milliseconds, a neighbor is considered reachable after receiving a reachability confirmation.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface reachable-time (for the management port)

Configure the time a neighbor is considered reachable after receiving a reachability confirmation.

Syntax

- `default ipv6 interface reachable-time`
- `ipv6 interface reachable-time <0-3600000>`

Default

`The default is 30000.`

Command mode

mgmtEthernet Interface Configuration

Command parameters

Parameter	Description
`<0-3600000>`	Configures the time, in milliseconds, a neighbor is considered reachable after receiving a reachability confirmation.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface retransmit-timer (for a port)

Configure the time, between retransmissions of Neighbor Solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.

Syntax

- `default ipv6 interface retransmit-timer`
- `ipv6 interface retransmit-timer <1-4294967295>`

Default

`The default is 1000.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
<1-4294967295>	Configures the time, in milliseconds, between retransmissions of Neighbor Solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface retransmit-timer (for a VLAN)

Configure the time, between retransmissions of Neighbor Solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.

Syntax

- `default ipv6 interface retransmit-timer`
- `ipv6 interface retransmit-timer <1-4294967295>`

Default

`The default is 1000.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
<1-4294967295>	Configures the time, in milliseconds, between retransmissions of Neighbor Solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface retransmit-timer (for the management port)

Configure the time, between retransmissions of Neighbor Solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.

Syntax

- `default ipv6 interface retransmit-timer`
- `ipv6 interface retransmit-timer <0-3600000>`

Default

`The default is 1000.`

Command mode

mgmtEthernet Interface Configuration

Command parameters

Parameter	Description
`<0-3600000>`	Configures the time, in milliseconds, between retransmissions of Neighbor Solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 interface vlan (for a port)

Configure the interface as part of an IPv6 VLAN.

Syntax

- `ipv6 interface vlan <1-4084>`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
<1-4084>	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 nd dad-ns (for a port)

Configure the number of neighbor solicitation messages from duplicate address detection.

Syntax

- `default ipv6 nd dad-ns`
- `ipv6 nd dad-ns <0-600>`

Default

The default is 1.

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
<0-600>	Configures the number of neighbor solicitation messages from duplicate address detection. A value of 0 disables duplicate address detection on the specified interface. A value of 1 configures a single transmission without follow-up transmissions.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 nd dad-ns (for a VLAN)

Configure the number of neighbor solicitation messages from duplicate address detection.

Syntax

- `default ipv6 nd dad-ns`
- `ipv6 nd dad-ns <0-600>`
- `ipv6 nd dad-ns <0-600> other-config-flag`

Default

The default is 1.

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
<0-600>	Configures the number of neighbor solicitation messages from duplicate address detection. A value of 0 disables duplicate address detection on the specified interface. A value of 1 configures a single transmission without follow-up transmissions.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 nd dad-ns (for the management port)

Configure the number of neighbor solicitation messages from duplicate address detection.

Syntax

- `default ipv6 nd dad-ns`
- `ipv6 nd dad-ns <0-600>`

Default

The default is 1.

Command mode

mgmtEthernet Interface Configuration

Command parameters

Parameter	Description
<0-600>	Configures the number of neighbor solicitation messages from duplicate address detection. A value of 0 disables duplicate address detection on the specified interface. A value of 1 configures a single transmission without follow-up transmissions.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 nd (for a port)

Configure the neighbor discovery parameters of the interface.

Syntax

- `default ipv6 nd`
- `default ipv6 nd hop-limit`
- `default ipv6 nd mtu`
- `default ipv6 nd reachable-time`
- `default ipv6 nd retransmit-timer`
- `ipv6 nd hop-limit <0-255>`
- `ipv6 nd mtu <0-9500>`
- `ipv6 nd reachable-time <0-3600000>`
- `ipv6 nd retransmit-timer <0-4294967295>`
- `no ipv6 nd`
- `no ipv6 nd hop-limit`
- `no ipv6 nd mtu`
- `no ipv6 nd reachable-time`
- `no ipv6 nd retransmit-timer`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`hop-limit <0-255>`	Sets the neighbor discovery hop-limit value for the interface.
`mtu <0-9500>`	Sets router advertisement MTU size.
`reachable-time <0-3600000>`	Sets router advertisement reachable time.
`retransmit-timer <0-4294967295>`	Sets router advertisement retransmit timer.

©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

ipv6 nd hop-limit (for a port)

Configure the hop limit sent in router advertisements.

Syntax

- `ipv6 nd hop-limit <0-255>`

Default

`The default is 64.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`hop-limit <0-255>`	Specifies the current hop limit field sent in router advertisements from this interface. The value must be the current diameter of the Internet. A value of zero indicates that the advertisement does not specify a hop-limit value.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 nd managed-config-flag (for a port)

Enable M-bit (managed address configuration) on the router.

Syntax

- `default ipv6 nd managed-config-flag`
- `ipv6 nd managed-config-flag`
- `no ipv6 nd managed-config-flag`

Default

`The default is disabled.`

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ipv6 nd managed-config-flag (for a VLAN)

Enable M-bit (managed address configuration) on the router.

Syntax

- `default ipv6 nd managed-config-flag`
- `ipv6 nd managed-config-flag`
- `no ipv6 nd managed-config-flag`

Default

`The default is disabled.`

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ipv6 nd mtu (for a port)

Configure the maximum transmission unit (MTU) for router advertisements.

Syntax

- `ipv6 nd mtu <0-9500>`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`mtu <0-9500>`	Shows the MTU value sent in router advertisements on this interface. A value of zero indicates that the system sends no MTU options. Valid values are: 0, 1280-1500, 1850, or 9500.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 nd other-config-flag (for a port)

Enable the O-bit (other stateful configuration) in the router advertisement. Other stateful configuration autoConfigure received information without addresses.

Syntax

- `default ipv6 nd other-config-flag`
- `ipv6 nd other-config-flag`
- `no ipv6 nd other-config-flag`

Default

`The default is disabled.`

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ipv6 nd other-config-flag (for a VLAN)

Enable the O-bit (other stateful configuration) in the router advertisement. Other stateful configuration autoConfigure received information without addresses.

Syntax

- `default ipv6 nd other-config-flag`
- `ipv6 nd other-config-flag`
- `no ipv6 nd other-config-flag`

Default

`The default is disabled.`

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ipv6 nd prefix (for a port)

Configure neighbor discovery prefixes. IPv6 nodes on the same link use ND to discover link-layer addresses and to obtain and advertise various network parameters and reachability information. ND combines the services provided by ARP and router discovery for IPv4. IPv6 router advertisement includes discovery prefixes.

Syntax

- `default ipv6 nd prefix WORD<0-255>`
- `default ipv6 nd prefix WORD<0-255> no-advertise`
- `default ipv6 nd prefix WORD<0-255> preferred-life`
- `default ipv6 nd prefix WORD<0-255> valid-life`
- `ipv6 nd prefix WORD<0-255> infinite`
- `ipv6 nd prefix WORD<0-255> no-advertise`
- `ipv6 nd prefix WORD<0-255> preferred-life <0-4294967295>`
- `ipv6 nd prefix WORD<0-255> valid-life <0-4294967295>`
- `no ipv6 nd prefix WORD<0-255>`
- `no ipv6 nd prefix WORD<0-255> no-advertise`
- `no ipv6 nd prefix-interface WORD<0-255>`
- `no ipv6 nd prefix-interface WORD<0-255> no-advertise`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`infinite`	Configures the prefix as infinite.
`no-advertise`	Removes the prefix from the neighbor advertisement. The default for no-advertise is disabled.
`preferred-life <0-4294967295>`	Configures the preferred life, in seconds. The valid range is 0-4294967295. The default preferred-life is 604800.
`valid-life <0-4294967295>`	Configures the valid life, in seconds. The valid range is 0-4294967295. The default valid-life is 2592000.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 nd prefix (for a VLAN)

Configure neighbor discovery prefixes. IPv6 nodes on the same link use ND to discover link-layer addresses and to obtain and advertise various network parameters and reachability information. ND combines the services provided by ARP and router discovery for IPv4. IPv6 router advertisement includes discovery prefixes.

Syntax

- `default ipv6 nd prefix WORD<0-255> [no-advertise] [preferred-life] [valid-life]`
- `ipv6 nd prefix WORD<0-255> infinite`
- `ipv6 nd prefix WORD<0-255> no-advertise`
- `ipv6 nd prefix WORD<0-255> preferred-life <0-4294967295>`
- `ipv6 nd prefix WORD<0-255> valid-life <0-4294967295>`
- `no ipv6 nd prefix WORD<0-255> [no-advertise]`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
infinite	Configures the prefix as infinite.
no-advertise	Removes the prefix from the neighbor advertisement. The default for no-advertise is disabled.
preferred-life <0-4294967295>	Configures the preferred life, in seconds. The valid range is 0-4294967295. The default preferred-life is 604800.
valid-life <0-4294967295>	Configures the valid life, in seconds. The valid range is 0-4294967295. The default valid-life is 2592000.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 nd prefix-interface (for a port)

Configure neighbor discovery prefixes IPv6 nodes on the same link use ND to discover link-layer addresses and to obtain and advertise various network parameters and reachability information. ND combines the services provided by Address Resolution Protocol (ARP) and router discovery for IPv4. IPv6 router advertisement includes discovery prefixes.

Syntax

- `default ipv6 nd prefix-interface WORD<0-255>`
- `default ipv6 nd prefix-interface WORD<0-255> no-advertise`
- `ipv6 nd prefix-interface WORD<0-255>`
- `ipv6 nd prefix-interface WORD<0-255> eui <1-3>`
- `ipv6 nd prefix-interface WORD<0-255> no-advertise`
- `ipv6 nd prefix-interface WORD<0-255> no-autoconfig`
- `ipv6 nd prefix-interface WORD<0-255> no-onlink`
- `no ipv6 nd prefix-interface WORD<0-255> [no-advertise]`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`eui <1-3>`	Specifies if extended unique identifier (EUI) is used. The values are:(1) EUI not used (2) EUI with Universal/Local bit (U/L) complement enabled (3) EUI used without U/L.
`no-advertise`	Removes the prefix from the neighbor advertisement. The default is disabled.
`no-autoconfig`	Configures if the prefix is used for autonomous address configuration.
`no-onlink`	Configures if onlink determination uses the prefix. This value is placed in the L-bit field in the prefix information option and is a 1-bit flag.
`WORD <0-255>`	Specifies the IPv6 address prefix.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 nd ra-lifetime (for a port)

Configure the router lifetime included in router advertisement. Other devices use this information to determine if the router can be reached.

Syntax

- `default ipv6 nd ra-lifetime`
- `ipv6 nd ra-lifetime <0-9000>`

Default

`The default is 1800.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<0-9000>`	Configures the router lifetime included in router advertisement. The range is 0 or <4-9000>.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 nd ra-lifetime (for a VLAN)

Configure the router lifetime included in router advertisement. Other devices use this information to determine if the router can be reached.

Syntax

- `default ipv6 nd ra-lifetime`
- `ipv6 nd ra-lifetime <0-9000>`

Default

`The default is 1800.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`<0-9000>`	Configures the router lifetime included in router advertisement. The range is 0 or <4-9000>.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 nd reachable-time (for a port)

Configure the neighbor reachable time.

Syntax

- `ipv6 nd reachable-time <0-3600000>`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`reachable-time <0-3600000>`	Specifies a value (in milliseconds) placed in the router advertisement message sent by the router. The value zero means unspecified (by this system). Configure the amount of time that a remote IPv6 node is considered reachable after a reachability confirmation event.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 nd retransmit-timer (for a port)

Configure the time between neighbor solicitation messages.

Syntax

- `ipv6 nd retransmit-timer <0-4294967295>`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`retransmit-timer <0-4294967295>`	Specifies a value (in milliseconds) placed in the retransmit timer field in the router advertisement message sent from this interface. The value zero means unspecified (by this system). The value configures the amount of time the system waits for the transmission to occur.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 nd rtr-advert-max-interval (for a port)

Configure the maximum time allowed between sending unsolicited multicast router advertisements.

Syntax

- `default ipv6 nd rtr-advert-max-interval`
- `ipv6 nd rtr-advert-max-interval <4-1800>`

Default

`The default is 600.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<4-1800>`	Specifies the maximum interval value.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 nd rtr-advert-max-interval (for a VLAN)

Configure the maximum time allowed between sending unsolicited multicast router advertisements.

Syntax

- `default ipv6 nd rtr-advert-max-interval`
- `ipv6 nd rtr-advert-max-interval <4-1800>`

Default

`The default is 600.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`<4-1800>`	Specifies the maximum interval value.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 nd rtr-advert-min-interval (for a port)

Configure the minimum time allowed between sending unsolicited multicast router advertisements from the interface.

Syntax

- `default ipv6 nd rtr-advert-min-interval`
- `ipv6 nd rtr-advert-min-interval <3-1350>`

Default

`The default is 200.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<3-1350>`	Configures the minimum time, in seconds.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 nd rtr-advert-min-interval (for a VLAN)

Configure the minimum time allowed between sending unsolicited multicast router advertisements from the interface.

Syntax

- `default ipv6 nd rtr-advert-min-interval`
- `ipv6 nd rtr-advert-min-interval <3-1350>`

Default

`The default is 200.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
<3-1350>	Configures the minimum time, in seconds.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 nd send-ra (for a port)

Enable or disables periodic router advertisement messages.

Syntax

- `default ipv6 nd send-ra`
- `ipv6 nd send-ra`
- `no ipv6 nd send-ra`

Default

`The default is enabled.`

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ipv6 nd send-ra (for a VLAN)

Enable or disables periodic router advertisement messages.

Syntax

- `default ipv6 nd send-ra`
- `ipv6 nd send-ra`
- `no ipv6 nd send-ra`

Default

`The default is enabled.`

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

ipv6 nd valid-life (for a port)

Modify an existing neighbor discovery prefix. Configure the valid lifetime in seconds that indicates the length of time this prefix is advertised.

Syntax

- `ipv6 nd prefix WORD<0-255> valid-life <0-4294967295>`

Default

`The default is 2592000.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`valid-life <0-4294967295>`	Configures the valid lifetime in seconds that indicates the length of time this prefix is advertised. The default is 2592000. A valid lifetime is the length of time of the preferred and depreciated state of an auto configuration address.
`WORD<0-255>`	Specifies the IPv6 address and prefix.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 ospf area (for a VLAN)

Configure an OSPFv3 area on an interface.

Syntax

- `ipv6 ospf area {A.B.C.D}`
- `ipv6 ospf area {A.B.C.D} cost <0-65535>`
- `ipv6 ospf area {A.B.C.D} dead-interval <1-65535>`
- `ipv6 ospf area {A.B.C.D} hello-interval <1-65535>`
- `ipv6 ospf area {A.B.C.D} network eth`
- `ipv6 ospf area {A.B.C.D} network nbma`
- `ipv6 ospf area {A.B.C.D} network p2mp`
- `ipv6 ospf area {A.B.C.D} network p2p`
- `ipv6 ospf area {A.B.C.D} network passive`
- `ipv6 ospf area {A.B.C.D} priority <0-255>`
- `ipv6 ospf area {A.B.C.D} retransmit-interval <1-1800>`
- `ipv6 ospf area {A.B.C.D} transit-delay <1-1800>`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`area {A.B.C.D}`	Creates an IPv6 OSPF area.
`cost <0-65535>`	Configures the OSPF metric for the interface. The switch advertises the metric in router link advertisements. The default is 1.
`dead-interval <1-65535>`	Specifies the dead interval, as the number of seconds to wait before determining the OSPF router is down. The default is 40.
`hello-interval <1-65535>`	Specifies the hello interval, in seconds, for hello packets sent between switches for a virtual interface in an OSPF area. The default is 10.
`network <eth|nbma|p2mp|p2p|passive>`	Configures the type of interface as one of the following: eth: broadcast, nbma: NBMA, p2mp: point-to-multipoint, p2p:point-to-point, or passive: passive interface.

priority <0-255>	Configures the OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router. If the priority is 0, the interface cannot become either the designated router or a backup. The priority is used only during election of the designated router and backup designated router. The default is 1.
retransmit-interval <1-1800>	Specifies the retransmit interval, in seconds, for link-state advertisements. The default is 5.
transit-delay <1-1800>	Specifies the transit-delay interval, in seconds, required to transmit a link-state update packet over the virtual interface. The default is 1.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 ospf (for a VLAN)

Configure OSPFv3 on an interface.

Syntax

- `default ipv6 ospf`
- `default ipv6 ospf cost`
- `default ipv6 ospf dead-interval`
- `default ipv6 ospf enable`
- `default ipv6 ospf hello-interval`
- `default ipv6 ospf nbma-nbr WORD<0-43>`
- `default ipv6 ospf poll-interval`
- `default ipv6 ospf priority`
- `default ipv6 ospf retransmit-interval`
- `default ipv6 ospf transit-delay`
- `ipv6 ospf cost <0-65535>`
- `ipv6 ospf dead-interval <1-65535>`
- `ipv6 ospf enable`
- `ipv6 ospf hello-interval <1-65535>`
- `ipv6 ospf nbma-nbr WORD<0-43> <0-255>`
- `ipv6 ospf nbma-nbr WORD<0-43> priority <0-255>`
- `ipv6 ospf poll-interval <0-65535>`
- `ipv6 ospf priority <0-255>`
- `ipv6 ospf retransmit-interval <1-1800>`
- `ipv6 ospf transit-delay <1-1800>`
- `no ipv6 ospf`
- `no ipv6 ospf enable`
- `no ipv6 ospf nbma-nbr WORD<0-43>`

Default

None

Command mode

Command parameters

Parameter	Description
cost <0-65535>	Configures the OSPF metric for the interface. The switch advertises the metric in router link advertisements. The default is 1.
dead-interval <1-65535>	Specifies the dead interval, as the number of seconds to wait before determining the OSPF router is down. The default is 40.
enable	Enables the OSPF on the IPv6 interface.
hello-interval <1-65535>	Specifies the hello interval, in seconds, for hello packets sent between switches for a virtual interface in an OSPF area. The default is 10.
nbma-nbr WORD<0-43>	Configures an NBMA neighbor. WORD<0-43> specifies the IPv6 address. Use priority <0-255> to change an existing priority value for an NBMA neighbor. Use <0-255> to assign the priority value when you create the neighbor.
network <eth | nbma | p2mp | p2p | passive>	Configures the type of interface as one of the following: eth: broadcast, nbma: NBMA, p2mp: point-to-multipoint, p2p:point-to-point, or passive: passive interface.
poll-interval <0-65535>	Configures the polling interval for the OSPF interface in seconds. The default is 120.
priority <0-255>	Configures the OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router. If the priority is 0, the interface cannot become either the designated router or a backup. The priority is used only during election of the designated router and backup designated router. The default is 1.
retransmit-interval <1-1800>	Specifies the retransmit interval, in seconds, for link-state advertisements. The default is 5.
transit-delay <1-1800>	Specifies the transit-delay interval, in seconds, required to transmit a link-state update packet over the virtual interface. The default is 1.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 prefix-list

Use prefix lists to allow or deny specific route updates. A prefix list policy Specify route prefixes to match. When there is a match, the route is used. Configure a prefix list and apply the list to a route policy.

Syntax

- `ipv6 prefix-list WORD<1-64> name WORD<1-64>`
- `ipv6 prefix-list WORD<1-64> WORD<1-256> [ge <0- 128>] [le <0-128>]`
- `no ipv6 prefix-list WORD<1-64> [WORD<1-256>]`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`name WORD<1-64>`	Renames the specified prefix list. The name length is from 1 to 64 characters.
`WORD<1-64> WORD<1-256> ge <0-128> le <0-128>`	Adds a prefix entry to the prefix list. WORD<1-64> is the prefix-list name. WORD<1-256> is the IPv6 address and length. <ge|le><0- 128> is the minimum and maximum length to match. Lower bound and higher bound mask lengths together can define a range of networks.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 redistribute

Enable redistribution to redistribute IPv6 routes into an OSPFv3 routing domain.

Syntax

- `default ipv6 redistribute {bgp|direct|static} [enable]`
- `ipv6 redistribute bgp enable`
- `ipv6 redistribute direct enable`
- `ipv6 redistribute static enable`
- `no ipv6 redistribute {bgp|direct|static} [enable]`

Default

`The default is disabled.`

Command mode

OSPF Router Configuration

Command parameters

Parameter	Description
`{bgp|direct|static}`	Specifies the type of IPv6 route to redistribute to the OSPFv3 routing domain.
`enable`	Enables redistribution.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 route

Configure a static route to destination IPv6 address prefixes.

Syntax

- default ipv6 route WORD<0-46>
- default ipv6 route WORD<0-46> enable next-hop WORD<0-46>
- default ipv6 route WORD<0-46> enable port {slot/port}
- default ipv6 route WORD<0-46> enable tunnel <1-2000>
- default ipv6 route WORD<0-46> enable vlan <1-4084>
- default ipv6 route WORD<0-46> preference
- default ipv6 route WORD<0-46> preference next-hop WORD<0-46>
- default ipv6 route WORD<0-46> preference port {slot/port}
- default ipv6 route WORD<0-46> preference tunnel <1-2000>
- default ipv6 route WORD<0-46> preference vlan <1-4084>
- ipv6 route WORD<0-46> cost <1-65535>
- ipv6 route WORD<0-46> cost <1-65535> next-hop WORD<0-46>
- ipv6 route WORD<0-46> cost <1-65535> port {slot/port}
- ipv6 route WORD<0-46> cost <1-65535> preference <1-255>
- ipv6 route WORD<0-46> cost <1-65535> tunnel <1-2000>
- ipv6 route WORD<0-46> cost <1-65535> vlan <1-4084>
- ipv6 route WORD<0-46> enable
- ipv6 route WORD<0-46> enable next-hop WORD<0-46>
- ipv6 route WORD<0-46> enable port {slot/port}
- ipv6 route WORD<0-46> enable tunnel <1-2000>
- ipv6 route WORD<0-46> enable vlan <1-4084>
- ipv6 route WORD<0-46> preference <1-255>
- ipv6 route WORD<0-46> preference <1-255> next-hop WORD<0-46>
- ipv6 route WORD<0-46> preference <1-255> port {slot/port}
- ipv6 route WORD<0-46> preference <1-255> tunnel <1-2000>
- ipv6 route WORD<0-46> preference <1-255> vlan <1-4084>

- `no ipv6 route WORD<0-46>`
- `no ipv6 route WORD<0-46> enable`
- `no ipv6 route WORD<0-46> enable next-hop WORD<0-46>`
- `no ipv6 route WORD<0-46> enable port {slot/port}`
- `no ipv6 route WORD<0-46> enable tunnel <1-2000>`
- `no ipv6 route WORD<0-46> enable vlan <1-4084>`
- `no ipv6 route WORD<0-46> next-hop WORD<0-46>`
- `no ipv6 route WORD<0-46> port {slot/port}`
- `no ipv6 route WORD<0-46> tunnel <1-2000>`
- `no ipv6 route WORD<0-46> vlan <1-4084>`

Default

`The default state for a new static route is enable.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`cost <1-65535>`	Specifies the cost or distance ratio to reach the destination for this node. The default cost is 1.
`enable`	Enables the static route on the port. The default state for a new static route is enable.
`next-hop WORD<0-46>`	Specifies the IPv6 address of the next hop on this route. You do not need to specify the next hop if the devices directly connect to one another. Configure the next hop if the two nodes do not share the same network prefix but reside on the same link.
`port {slot/port}`	Specifies the port to which this entry applies. You must specify the port if the next hop is a link-local address.
`preference <1-255>`	Specifies the routing preference of the destination IPv6 address. The default preference is 5.
`tunnel <1-2000>`	Specifies the tunnel to which this entry applies.
`vlan <1-4084>`	Specifies the VLAN to which this entry applies. You must specify the VLAN if the next hop is a link-local address.
`WORD<0-46>`	Specifies the IPv6 destination network address.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 router-id

Configure the OSPF router ID.

Syntax

- `default ipv6 router-id`
- `ipv6 router-id {A.B.C.D}`

Default

None

Command mode

OSPF Router Configuration

Command parameters

Parameter	Description
{A.B.C.D}	Specifies the IPv4 address for the router ID.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 route static

Enable static routes globally. If you disable static routes globally, the system removes all enabled static routes from the RTM and does not add new static routes to the RTM.

Syntax

- `default ipv6 route static enable`
- `ipv6 route static enable`
- `no ipv6 route static enable`

Default

`The default is enabled.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`enable`	Enables the static routes globally.
`static`	Modifies IPv6 static route parameters.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 rvs-path-chk (for a port)

Use the unicast reverse path checking feature to reduce the problems that are caused by the introduction of malformed or forged (spoofed) IPv6 source addresses into a network.

Syntax

- `default ipv6 rvs-path-chk`
- `default ipv6 rvs-path-chk mode`
- `ipv6 rvs-path-chk`
- `ipv6 rvs-path-chk mode exist-only`
- `ipv6 rvs-path-chk mode strict`
- `no ipv6 rvs-path-chk`

Default

`Reverse path checking is disabled by default.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`mode <exist-only|strict>`	Specifies the mode for reverse path checking. In exist-only mode, reverse path checking checks whether the source address of the incoming packet exists in the routing table. If the source entry is found, the packet is forwarded as usual; otherwise, the packet is discarded. In strict mode, reverse path checking checks whether the source address for the incoming packet exists in the routing table. If the source entry is found, reverse path checking further checks if the source IP interface address matches the packet incoming interface address. If they match, the packet is forwarded as usual, otherwise, the packet is discarded. The default mode is exist-only.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 rvs-path-chk (for a VLAN)

Use the unicast reverse path checking feature to reduce the problems that are caused by the introduction of malformed or forged (spoofed) IPv6 source addresses into a network.

Syntax

- `default ipv6 rvs-path-chk`
- `default ipv6 rvs-path-chk mode`
- `ipv6 rvs-path-chk`
- `ipv6 rvs-path-chk mode exist-only`
- `ipv6 rvs-path-chk mode strict`
- `no ipv6 rvs-path-chk`

Default

`Reverse path checking is disabled by default.`

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`mode <exist-only|strict>`	Specifies the mode for reverse path checking. In exist-only mode, reverse path checking checks whether the source address of the incoming packet exists in the routing table. If the source entry is found, the packet is forwarded as usual; otherwise, the packet is discarded. In strict mode, reverse path checking checks whether the source address for the incoming packet exists in the routing table. If the source entry is found, reverse path checking further checks if the source IP interface address matches the packet incoming interface address. If they match, the packet is forwarded as usual, otherwise, the packet is discarded. The default mode is exist-only.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 send-trap enable

Configure Virtual Router Redundancy Protocol (VRRP) notification control.

Syntax

- `default ipv6 send-trap enable`
- `ipv6 send-trap enable`
- `no ipv6 send-trap enable`

Default

`Generation of SNMP traps for VRRP events is enabled.`

Command mode

VRRP Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

ipv6 tunnel

Configure a tunnel for IPv6 VLANs or brouter ports to communicate through an IPv4 network.

Syntax

- `default ipv6 tunnel <1-2000>`
- `default ipv6 tunnel <1-2000> hop-limit`
- `ipv6 tunnel <1-2000> hop-limit <0-255>`
- `ipv6 tunnel <1-2000> source {A.B.C.D} address WORD<0-46> destination {A.B.C.D}`
- `no ipv6 tunnel <1-2000>`

Default

`The default hop-limit is 255.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<1-2000>`	Specifies the tunnel ID.
`address WORD<0-46>`	Specifies the IPv6 address and length for the local VLAN or brouter port.
`destination{A.B.C.D}`	Configures the address of the remote endpoint of the tunnel.
`hop-limit <0-255>`	Configures the maximum number of hops in the tunnel.
`source {A.B.C.D}`	Configures the address of the local endpoint of the tunnel, or 0.0.0.0 (for IPv4) or :: (for IPv6) if the device is free to choose its addresses at tunnel establishment.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 tunnel (for OSPF)

Configure OSPF parameters for an IPv6 tunnel.

Syntax

- `default ipv6 tunnel <1-2000>`
- `default ipv6 tunnel <1-2000> dead-interval`
- `default ipv6 tunnel <1-2000> hello-interval`
- `default ipv6 tunnel <1-2000> metric`
- `default ipv6 tunnel <1-2000> poll-interval`
- `default ipv6 tunnel <1-2000> priority`
- `default ipv6 tunnel <1-2000> retransmit-interval`
- `default ipv6 tunnel <1-2000> transmit-delay`
- `ipv6 tunnel <1-2000> area {A.B.C.D}`
- `ipv6 tunnel <1-2000> dead-interval <1-65535>`
- `ipv6 tunnel <1-2000> enable`
- `ipv6 tunnel <1-2000> hello-interval <1-65535>`
- `ipv6 tunnel <1-2000> metric <0-65535>`
- `ipv6 tunnel <1-2000> poll-interval <0-65535>`
- `ipv6 tunnel <1-2000> priority <0-255>`
- `ipv6 tunnel <1-2000> retransmit-interval <1-1800>`
- `ipv6 tunnel <1-2000> transmit-delay <1-1800>`
- `no ipv6 tunnel <1-2000>`
- `no ipv6 tunnel <1-2000> enable`

Default

None

Command mode

OSPF Router Configuration

Command parameters

Parameter	Description
{A.B.C.D}	Specifies the area address.

<1-2000>	Specifies the tunnel ID.
dead-interval <1-65535>	Specifies the dead interval, as the number of seconds to wait before determining the OSPF router is down. The default dead-interval is 40.
hello-interval <1-65535>	Specifies the hello interval, in seconds, for hello packets sent between switches for an interface in an OSPF area. The default hello-interval is 10.
metric <0-65535>	Configures the OSPF metric for the tunnel. The switch advertises the metric in router link advertisements. The default metric is 100.
poll-interval <0-65535>	Configures the polling interval, in seconds, for the OSPF tunnel. The default poll-interval is 120.
priority <0-255>	Configures the OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router. If the priority is 0, the interface cannot become either the designated router or a backup. The default priority is 1.
retransmit-interval <1-1800>	Specifies the retransmit interval, in seconds, for link-state advertisements. The default retransmit-interval is 5.
transmit-delay <1-1800>	Specifies the transmit-delay interval, in seconds, required to transmit a link-state update packet over the virtual interface. The default transmit-delay is 1.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 vrrp address (for a port)

Specify a link-local address to associate with the virtual router. Optionally, you can also assign global unicast IPv6 addresses to associate with the virtual router. Network prefixes for the virtual router are derived from the global IPv6 addresses assigned to the virtual router.

Syntax

- `default ipv6 vrrp address <1-255>`
- `ipv6 vrrp address <1-255> global WORD<0-225>`
- `ipv6 vrrp address <1-255> link-local WORD<0-127>`
- `no ipv6 vrrp address <1-255>`
- `no ipv6 vrrp address <1-255> global WORD<0-225>`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
<1-255>	Specifies the virtual router ID. The virtual router acts as the default router for one or more associated addresses.
link-local WORD<0-127>	Specifies a link-local IPv6 address to associate with the virtual router.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 vrrp address (for a VLAN)

Specify a link-local address to associate with the virtual router. Optionally, you can also assign global unicast IPv6 addresses to associate with the virtual router. Network prefixes for the virtual router are derived from the global IPv6 addresses assigned to the virtual router.

Syntax

- `default ipv6 vrrp address <1-255>`
- `ipv6 vrrp address <1-255> link-local WORD<0-127>`
- `no ipv6 vrrp address <1-255>`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`<1-255>`	Specifies the virtual router ID. The virtual router acts as the default router for one or more associated addresses.
`link-local WORD<0-127>`	Specifies a link-local IPv6 address to associate with the virtual router.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 vrrp (for a port)

Configure Virtual Router Redundancy Protocol (VRRP) to provide fast failover of a default router for IPv6 LAN hosts. VRRP supports a virtual IPv6 address shared between two or more routers that connect the common subnet to the enterprise network. VRRP for IPv6 provides a faster switchover to an alternate default router than is possible using the ND protocol.

Syntax

- `default ipv6 vrrp <1-255>`
- `default ipv6 vrrp <1-255> accept-mode enable`
- `default ipv6 vrrp <1-255> action`
- `default ipv6 vrrp <1-255> adver-int`
- `default ipv6 vrrp <1-255> backup-master enable`
- `default ipv6 vrrp <1-255> critical-ipv6 enable`
- `default ipv6 vrrp <1-255> critical-ipv6-addr`
- `default ipv6 vrrp <1-255> enable`
- `default ipv6 vrrp <1-255> fast-adv enable`
- `default ipv6 vrrp <1-255> fast-adv-int`
- `default ipv6 vrrp <1-255> holddown-timer`
- `default ipv6 vrrp <1-255> priority`
- `ipv6 vrrp <1-255> accept-mode enable`
- `ipv6 vrrp <1-255> action none`
- `ipv6 vrrp <1-255> action preempt`
- `ipv6 vrrp <1-255> adver-int <1..40>`
- `ipv6 vrrp <1-255> backup-master enable`
- `ipv6 vrrp <1-255> critical-ipv6 enable`
- `ipv6 vrrp <1-255> critical-ipv6-addr WORD<0-46>`
- `ipv6 vrrp <1-255> enable`
- `ipv6 vrrp <1-255> fast-adv enable`
- `ipv6 vrrp <1-255> fast-adv-int <200-1000>`
- `ipv6 vrrp <1-255> holddown-timer <0-21600>`
- `ipv6 vrrp <1-255> priority <1-255>`
- `no ipv6 vrrp <1-255>`

- `no ipv6 vrrp <1-255> accept-mode enable`
- `no ipv6 vrrp <1-255> backup-master enable`
- `no ipv6 vrrp <1-255> critical-ipv6 enable`
- `no ipv6 vrrp <1-255> enable`
- `no ipv6 vrrp <1-255> fast-adv enable`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<1-255>`	Specifies a number that uniquely identifies a virtual router on an interface. The virtual router acts as the default router for one or more assigned addresses.
`accept-mode enable`	Controls whether a master router accepts packets addressed to the IPv6 address of the address owner as its own if it is not the IPv6 address owner. The default accept-mode enable is disabled.
`action <none|preempt>`	Lists options to override the holddown timer manually and force preemption. none does not override the timer. preempt preempts the timer. This parameter applies only if the holddown timer is active.
`adver-int <1-40>`	Specifies the time interval, in seconds, between sending advertisement messages. Only the master router sends advertisements. The default is 1.
`backup-master enable`	Uses the backup Virtual Router Redundancy Protocol (VRRP) switch for traffic forwarding. This option reduces the traffic on the IST link. The default backup-master enable is disabled.
`critical-ip enable`	Enables or disables the use of critical IP. When disabled, the Virtual Router Redundancy Protocol (VRRP) ignores the availability of the address configured as critical IP. This address must be a local address.
`critical-ip-addr WORD<0-46>`	Specifies an IP interface on the local router configured so that a change in its state causes a role switch in the virtual router (for example, from master to backup) in case the interface stops responding. The default critical-ip enable is disabled.
`enable`	Enables IPv6 Virtual Router Redundancy Protocol (VRRP). The default is disabled.
`fast-adv enable`	Enables or disables the fast advertisement interval. When disabled, the regular advertisement interval is used. The default fast-adv-int is 200.
`fast-adv-int <200-1000>`	Configures the interval between Virtual Router Redundancy Protocol (VRRP) advertisement messages. You must configure the same value on all participating routers. This unit of measure must be in multiples of 200 milliseconds.
`holddown-timer<0-21600>`	Configures the amount of time, in seconds, to wait before preempting the current Virtual Router Redundancy Protocol (VRRP) master. The default holddown timer is 0.
`priority <1-255>`	Specifies the priority value used by this Virtual Router Redundancy Protocol (VRRP) router. The value 255 is reserved for the router that owns the IP addresses associated with the virtual router. The default priority is 100.

©Avaya Inc. 2015 All Rights Reserved.

ipv6 vrrp (for a VLAN)

Configure Virtual Router Redundancy Protocol (VRRP) to provide fast failover of a default router for IPv6 LAN hosts. VRRP supports a virtual IPv6 address shared between two or more routers that connect the common subnet to the enterprise network. VRRP for IPv6 provides a faster switchover to an alternate default router than is possible using the ND protocol.

Syntax

- `default ipv6 vrrp <1-255> [enable]`
- `default ipv6 vrrp <1-255> accept-mode enable`
- `default ipv6 vrrp <1-255> action`
- `default ipv6 vrrp <1-255> adver-int`
- `default ipv6 vrrp <1-255> backup-master enable`
- `default ipv6 vrrp <1-255> critical-ipv6-addr [critical ipv6 enable]`
- `default ipv6 vrrp <1-255> fast-adv enable [fast-adv-int]`
- `default ipv6 vrrp <1-255> holddown-timer`
- `default ipv6 vrrp <1-255> priority`
- `ipv6 vrrp <1-255> accept-mode enable`
- `ipv6 vrrp <1-255> action none`
- `ipv6 vrrp <1-255> action preempt`
- `ipv6 vrrp <1-255> adver-int <1..40>`
- `ipv6 vrrp <1-255> backup-master enable`
- `ipv6 vrrp <1-255> critical-ipv6 enable`
- `ipv6 vrrp <1-255> critical-ipv6-addr WORD<0-46>`
- `ipv6 vrrp <1-255> enable`
- `ipv6 vrrp <1-255> fast-adv enable`
- `ipv6 vrrp <1-255> fast-adv-int <200-1000>`
- `ipv6 vrrp <1-255> holddown-timer <0-21600>`
- `ipv6 vrrp <1-255> priority <1-255>`
- `no ipv6 vrrp <1-255> [enable]`
- `no ipv6 vrrp <1-255> accept-mode enable`
- `no ipv6 vrrp <1-255> backup-master enable`
- `no ipv6 vrrp <1-255> critical ipv6 enable`

- `no ipv6 vrrp <1-255> fast-adv enable`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`<1-255>`	Specifies a number that uniquely identifies a virtual router on an interface. The virtual router acts as the default router for one or more assigned addresses.
`accept-mode enable`	Controls whether a master router accepts packets addressed to the IPv6 address of the address owner as its own if it is not the IPv6 address owner. The default accept-mode enable is disabled.
`action <none|preempt>`	Lists options to override the holddown timer manually and force preemption. none does not override the timer. preempt preempts the timer. This parameter applies only if the holddown timer is active.
`adver-int <1-40>`	Specifies the time interval, in seconds, between sending advertisement messages. Only the master router sends advertisements. The default is 1.
`backup-master enable`	Uses the backup Virtual Router Redundancy Protocol (VRRP) switch for traffic forwarding. This option reduces the traffic on the IST link. The default backup-master enable is disabled.
`critical-ip enable`	Enables or disables the use of critical IP. When disabled, the Virtual Router Redundancy Protocol (VRRP) ignores the availability of the address configured as critical IP. This address must be a local address. The default critical-ip enable is disabled.
`critical-ip-addr WORD<0-46>`	Specifies an IP interface on the local router configured so that a change in its state causes a role switch in the virtual router (for example, from master to backup) in case the interface stops responding.
`enable`	Enables IPv6 Virtual Router Redundancy Protocol (VRRP). The default is disabled.
`fast-adv enable`	Enables or disables the fast advertisement interval. When disabled, the regular advertisement interval is used. The default is disabled.
`fast-adv-int <200-1000>`	Configures the interval between Virtual Router Redundancy Protocol (VRRP) advertisement messages. You must configure the same value on all participating routers. This unit of measure must be in multiples of 200 milliseconds. The default is 200.
`holddown-timer<0-21600>`	Configures the amount of time, in seconds, to wait before preempting the current Virtual Router Redundancy Protocol (VRRP) master.
`priority <1-255>`	Specifies the priority value used by this Virtual Router Redundancy Protocol (VRRP) router. The value 255 is reserved for the router that owns the IP addresses associated with the virtual router. The default priority is 100.

©Avaya Inc. 2015 All Rights Reserved.

ipvpn

Create an IP Virtual Private Network (VPN) instance on the Virtual Routing and Forwarding (VRF).

Syntax

- `default ipvpn`
- `ipvpn`
- `no ipvpn`

Default

`The default is disabled.`

Command mode

VRF Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

ipvpn enable

Enable IP Virtual Private Network (VPN) on the Virtual Routing and Forwarding (VRF).

Syntax

- `default ipvpn enable`
- `ipvpn enable`
- `no ipvpn enable`

Default

`The default is disabled.`

Command mode

VRF Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

ip vrf

Creates a VRF instance.

Syntax

- `default ip vrf WORD<1-16> max-routes`
- `default ip vrf WORD<1-16> max-routes-trap enable`
- `default ip vrf WORD<1-16> vrf-trap enable`
- `ip vrf WORD<1-16>`
- `ip vrf WORD<1-16> max-routes <0-500000>`
- `ip vrf WORD<1-16> max-routes-trap enable`
- `ip vrf WORD<1-16> name WORD<1-16>`
- `ip vrf WORD<1-16> vrfid <1-511>`
- `ip vrf WORD<1-16> vrf-trap enable`
- `no ip vrf WORD<1-16>`
- `no ip vrf WORD<1-16> max-routes-trap enable`
- `no ip vrf WORD<1-16> vrf-trap enable`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`max-routes <0-500000>`	Specifies the maximum number of routes for the VRF. The default is 10,000. The Global Router is 250,000.
`max-routes-trap enable`	Enables the sending of traps after the maximum number of routes is reached. The default is enabled.
`name WORD<1-16>`	Renames the VRF instance.
`vrfid <1-511>`	Specifies a VRF ID. Virtual Services Platform 9000 supports 512 VRFs.
`vrf-trap enable`	Enables the device to send VRF-related traps. The default is enabled.
`WORD<1-16>`	Specifies the name for the VRF.

©Avaya Inc. 2015 All Rights Reserved.

ip vrrp address (for a port)

Specify an address to associate with the virtual router.

Syntax

- `default ip vrrp address <1-255>`
- `default ip vrrp address <1-255> {A.B.C.D}`
- `ip vrrp address <1-255> {A.B.C.D}`
- `no ip vrrp address <1-255>`
- `no ip vrrp address <1-255> {A.B.C.D}`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
{A.B.C.D}	Specifies an address to associate with the virtual router.
<1-255>	Specifies the virtual router ID. The virtual router acts as the default router for one or more associated addresses.

©Avaya Inc. 2015 All Rights Reserved.

ip vrrp (for a port)

Configure Virtual Router Redundancy Protocol (VRRP) on a port.

Syntax

- default ip vrrp <1-255>
- default ip vrrp <1-255> action
- default ip vrrp <1-255> adver-int
- default ip vrrp <1-255> backup-master enable
- default ip vrrp <1-255> critical-ip enable
- default ip vrrp <1-255> critical-ip-addr
- default ip vrrp <1-255> enable
- default ip vrrp <1-255> fast-adv enable
- default ip vrrp <1-255> fast-adv-int
- default ip vrrp <1-255> holddown-timer
- default ip vrrp <1-255> priority
- ip vrrp <1-255> action none
- ip vrrp <1-255> action preempt
- ip vrrp <1-255> adver-int <1-255>
- ip vrrp <1-255> backup-master enable
- ip vrrp <1-255> critical-ip enable
- ip vrrp <1-255> critical-ip-addr {A.B.C.D}
- ip vrrp <1-255> enable
- ip vrrp <1-255> fast-adv enable
- ip vrrp <1-255> fast-adv-int <200-1000>
- ip vrrp <1-255> holddown-timer <0-21600>
- ip vrrp <1-255> priority <1-255>
- ip vrrp <1-255> enable
- ip vrrp address <1-255> {A.B.C.D}
- no ip vrrp <1-255>
- no ip vrrp <1-255> backup-master enable

- `no ip vrrp <1-255> critical-ip enable`
- `no ip vrrp <1-255> enable`
- `no ip vrrp <1-255> fast-adv enable`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`action {none|preempt}`	Use the action choice option to manually override the hold-down timer and force preemption. none|preempt can be set to preempt the timer or set to none to allow the timer to keep working.
`address <1-255> <A.B.C.D>`	Sets the IP address of the Virtual Router Redundancy Protocol (VRRP) interface that forwards packets to the virtual IP addresses associated with the virtual router. A.B.C.D is the IP address of the master VRRP.
`adver-int <1-255>`	Sets the time interval between sending Virtual Router Redundancy Protocol (VRRP) advertisement messages. The range is between 1 and 255 seconds. This value must be the same on all the participating routers. The default is 1.
`backup-master enable`	Enables the Virtual Router Redundancy Protocol (VRRP) backup master. This option is supported only on Split MultiLink Trunking (SMLT) ports. Do not enable Backup Master if Critical IP is enabled.
`critical-ip enable`	Enables the critical IP address option. Do not enable critical IP if Backup Master is enabled.
`critical-ip-addr <A.B.C.D>`	Sets the critical IP address for VRRP. A.B.C.D is the IP address on the local router, which is configured so that a change in its state causes a role switch in the virtual router (for example, from master to backup in case the interface goes down).
`enable`	Enables Virtual Router Redundancy Protocol (VRRP) on the interface.
`fast-adv enable`	Enables the Fast Advertisement Interval. The default is disabled.
`fast-adv-int <200-1000>`	Sets the Fast Advertisement Interval, in milliseconds, the time interval between sending VRRP advertisement messages. The range must be the same on all participating routers. The default is 200. You must enter values in multiples of 200 milliseconds.
`holddown-timer<0-21600>`	Modifies the behavior of the Virtual Router Redundancy Protocol (VRRP) failover mechanism by allowing the router enough time to detect the OSPF or RIP routes. 0-21600 is the time interval (in seconds) a router is delayed when changing to master state.
`priority <1-255>`	Sets the port Virtual Router Redundancy Protocol (VRRP) priority. 1-255 is the value used by the VRRP router. The default is 100. Assign the value 255 to the router that owns the IP address associated with the virtual router.

©Avaya Inc. 2015 All Rights Reserved.

ip vrrp (for a VLAN)

Configure Virtual Router Redundancy Protocol (VRRP) on a VLAN.

Syntax

- `default ip vrrp <1-255> enable`
- `ip vrrp <1-255> action none`
- `ip vrrp <1-255> action preempt`
- `ip vrrp <1-255> adver-int <1-255>`
- `ip vrrp <1-255> backup-master enable`
- `ip vrrp <1-255> critical-ip enable`
- `ip vrrp <1-255> critical-ip-addr {A.B.C.D}`
- `ip vrrp <1-255> enable`
- `ip vrrp <1-255> fast-adv enable`
- `ip vrrp <1-255> fast-adv-int <200-1000>`
- `ip vrrp <1-255> holddown-timer <0-21600>`
- `ip vrrp <1-255> priority <1-255>`
- `ip vrrp <1-255> enable`
- `ip vrrp address <1-255> {A.B.C.D}`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`action {none|preempt}`	Manually overrides the hold-down timer and force preemption. none|preempt can be set to preempt the timer or set to none to allow the timer to keep working.
`address <1-255> <A.B.C.D>`	Sets the IP address of the Virtual Router Redundancy Protocol (VRRP) interface that forwards packets to the virtual IP addresses associated with the virtual router. A.B.C.D is the IP address of the master VRRP.
`adver-int <1-255>`	Sets the time interval between sending Virtual Router Redundancy Protocol (VRRP) advertisement messages. The range is between 1 and 255 seconds. This value must be the same on all of the participating routers. The default is 1.
	Enables the Virtual Router Redundancy Protocol (VRRP) backup master. This

backup-master enable	option is supported only on Split MultiLink Trunking (SMLT) ports. Do not enable Backup Master if Critical IP is enabled.
critical-ip enable	Enables the critical IP address option. Do not enable Critical IP if Backup Master is enabled.
critical-ip-addr <A.B.C.D>	Sets the critical IP address for Virtual Router Redundancy Protocol (VRRP). A.B.C.D is the IP address on the local router, which is configured so that a change in its state causes a role switch in the virtual router (for example, from master to backup in case the interface goes down).
enable	Enables Virtual Router Redundancy Protocol (VRRP) on the interface.
fast-adv enable	Enables the Fast Advertisement Interval. The default is disabled.
fast-adv-int <200-1000>	Sets the Fast Advertisement Interval, in milliseconds, the time interval between sending Virtual Router Redundancy Protocol (VRRP) advertisement messages. The range must be the same on all participating routers. The default is 200. You must enter values in multiples of 200 milliseconds.
holddown-timer<0-21600>	Modifies the behavior of the Virtual Router Redundancy Protocol (VRRP) failover mechanism by allowing the router enough time to detect the OSPF or RIP routes. 0-21600 is the time interval (in seconds) a router is delayed when changing to master state.
priority <1-255>	Sets the port Virtual Router Redundancy Protocol (VRRP) priority. 1-255 is the value used by the VRRP router. The default is 100. Assign the value 255 to the router that owns the IP address associated with the virtual router.

©Avaya Inc. 2015 All Rights Reserved.

i-sid

Assign an service instance identifier (I-SID) to the VRF.

Syntax

- `default i-sid`
- `i-sid <0-16777215>`
- `no i-sid`

Default

`The default is disabled.`

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
`<0-16777215>`	Specifies the service instance identifier (I-SID).

©Avaya Inc. 2015 All Rights Reserved.

isis accept adv-rtr (for a VRF)

Configure an Intermediate-System-to-Intermediate-System (IS-IS) accept policy instance to apply to all routes for a specific Backbone Edge Bridge (BEB) for a Virtual Routing and Forwarding (VRF) instance.

Syntax

- `isis accept adv-rtr <x.xx.xx>`
- `isis accept adv-rtr <x.xx.xx> enable`
- `isis accept adv-rtr <x.xx.xx> i-sid <0-16777215>`
- `isis accept adv-rtr <x.xx.xx> i-sid <0-16777215> enable`
- `isis accept adv-rtr <x.xx.xx> i-sid <0-16777215> route-map WORD<1-64>`
- `isis accept adv-rtr <x.xx.xx> isid-list WORD<1-32>`
- `isis accept adv-rtr <x.xx.xx> isid-list WORD<1-32> enable`
- `isis accept adv-rtr <x.xx.xx> isid-list WORD<1-32> route-map WORD<1-64>`
- `isis accept adv-rtr <x.xx.xx> route-map WORD<1-64>`
- `no isis accept adv-rtr <x.xx.xx>`
- `no isis accept adv-rtr <x.xx.xx> enable`
- `no isis accept adv-rtr <x.xx.xx> i-sid <0-16777215>`
- `no isis accept adv-rtr <x.xx.xx> i-sid <0-16777215> enable`
- `no isis accept adv-rtr <x.xx.xx> i-sid <0-16777215> route-map`
- `no isis accept adv-rtr <x.xx.xx> isid-list WORD<1-32>`
- `no isis accept adv-rtr <x.xx.xx> isid-list WORD<1-32> enable`
- `no isis accept adv-rtr <x.xx.xx> isid-list WORD<1-32> route-map`
- `no isis accept adv-rtr <x.xx.xx> route-map`

Default

`The default is disabled.`

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
`adv-rtr <x.xx.xx>`	Specifies a specific advertising BEB for the IS-IS accept policy. The x.xx.xx variable specifies an SPBM nickname.

`enable`	Enables the IS-IS accept policy.
`i-sid <0-16777215>`	Configures the service instance identifier (I-SID) to which the IS-IS accept policy applies. The number 0 represents the GRT.
`isid-list WORD <1-32>`	Configures a list of I-SIDs to which the IS-IS accept policy applies.
`route-map WORD<1-64>`	Specifies an IS-IS route policy.

©Avaya Inc. 2015 All Rights Reserved.

isis accept (for a VRF)

Configure an Intermediate-System-to-Intermediate-System (IS-IS) accept policy instance to apply to all routes from all Backbone Edge Bridges (BEBs) for a Virtual Routing and Forwarding (VRF) instance.

Syntax

- `isis accept i-sid <0-16777215>`
- `isis accept i-sid <0-16777215> enable`
- `isis accept i-sid <0-16777215> route-map WORD<1-64>`
- `isis accept isid-list WORD<1-32>`
- `isis accept isid-list WORD<1-32> enable`
- `isis accept isid-list WORD<1-32> route-map WORD<1-64>`
- `isis accept route-map WORD<1-64>`
- `no isis accept i-sid <0-16777215>`
- `no isis accept i-sid <0-16777215> enable`
- `no isis accept i-sid <0-16777215> route-map`
- `no isis accept isid-list WORD<1-32>`
- `no isis accept isid-list WORD<1-32> enable`
- `no isis accept isid-list WORD<1-32> route-map`
- `no isis accept route-map`

Default

`The default is disabled.`

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
`enable`	Enables the IS-IS accept policy.
`i-sid <0-16777215>`	Specifies a service instance identifier (I-SID) number representing a local or remote Layer 3 VSN. The number 0 represents the GRT.
`isid-list WORD <1-32>`	Specifies a list of I-SID numbers representing local or remote Layer 3 VSNs.
`route-map WORD<1-64>`	Specifies an IS-IS route policy.

NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

isis apply accept (for the GRT)

Apply the Intermediate-System-to-Intermediate-System (IS-IS) accept policy changes, which removes and re-adds all routes with updated filters for the Global Routing Table (GRT). If the route policy changes, you must reapply the IS-IS accept policy, unless it was the last sequence in the configuration.

Syntax

- `isis apply accept`

Default

None

Command mode

User EXEC

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

isis apply accept (for the VRF)

Apply the Intermediate-System-to-Intermediate-System (IS-IS) accept policy changes, which removes and re-adds all routes with updated filters for the Virtual Routing and Forwarding (VRF) instance. The isis apply accept [vrf WORD<1-16>] command can disrupt traffic and cause temporary traffic loss. When you apply isis apply accept [vrf<1-16>], the command reapplies the accept policies, which deletes all of the IS-IS routes and adds the IS-IS routes again. Avaya recommends you make all the relevant accept policy changes, and then apply the isis apply accept [vrf WORD<1-16>] command at the end. If the route policy changes, you must reapply the IS-IS accept policy, unless it was the last sequence in the configuration.

Syntax

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

isis apply redistribute

Apply the redistribution of the specified protocol into the Shortest Path Bridging MAC (SPBM) network.

Syntax

- `isis apply redistribute`
- `isis apply redistribute bgp`
- `isis apply redistribute bgp vrf WORD<1-16>`
- `isis apply redistribute direct`
- `isis apply redistribute direct vrf WORD<1-16>`
- `isis apply redistribute ospf`
- `isis apply redistribute ospf vrf WORD<1-16>`
- `isis apply redistribute rip`
- `isis apply redistribute rip vrf WORD<1-16>`
- `isis apply redistribute static`
- `isis apply redistribute static vrf WORD<1-16>`
- `isis apply redistribute vrf WORD<1-16>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies the VRF name.

©Avaya Inc. 2015 All Rights Reserved.

isis hello-auth (on an MLT)

Configure the authentication type used for Intermediate-System-to-Intermediate-System (IS-IS) hello packets on the interface.

Syntax

- `default isis hello-auth`
- `isis hello-auth type { none | simple | hmac-md5 }`
- `isis hello-auth type { none | simple | hmac-md5 } key WORD<1-16>`
- `isis hello-auth type { none | simple | hmac-md5 } key WORD<1-16> key-id <1-255>`
- `no isis hello-auth`

Default

The default is none.

Command mode

MLT Interface Configuration

Command parameters

Parameter	Description
key WORD<1-16>	Specifies the authentication key (password) used by the receiving router to verify the packet.
key-id <1-255>	Specifies the optional key ID.
type { none | simple | hmac-md5 }	Specifies the authentication type used for IS-IS hello packets on the interface. The type can be one of the following: none, simple or hmac-md5. If simple is selected, you can also specify a key value. Simple password authentication uses a text password in the transmitted packet. The receiving router uses an authentication key (password) to verify the packet. If hmac-md5 is selected, you can also specify a key value and key-id. MD5 authentication creates an encoded checksum in the transmitted packet. The receiving router uses an authentication key (password) to verify the MD5 checksum of the packet. There is an optional key ID. The default type is none. Use the no or default options to set the hello-auth type to none.

©Avaya Inc. 2015 All Rights Reserved.

isis hello-auth (on a port)

Specify the authentication type used for Intermediate-System-to-Intermediate-System (IS-IS) hello packets on the interface. The type can be one of the following: none, simple or hmac-md5.

Syntax

- `default isis hello-auth`
- `isis hello-auth type { none | simple | hmac-md5 }`
- `isis hello-auth type { none | simple | hmac-md5 } key WORD<1-16>`
- `isis hello-auth type { none | simple | hmac-md5 } key WORD<1-16> key-id <1-255>`
- `no isis hello-auth`

Default

`The default hello-auth type is none.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`key WORD<1-16>`	Specifies the authentication key (password) used by the receiving router to verify the packet.
`key-id <1-255>`	Specifies the optional key ID.
`type { none | simple | hmac-md5 }`	Specifies the authentication type used for IS-IS hello packets on the interface. The type can be one of the following: none, simple or hmac-md5. If simple is selected, you can also specify a key value. Simple password authentication uses a text password in the transmitted packet. The receiving router uses an authentication key (password) to verify the packet. If hmac-md5 is selected, you can also specify a key value and key-id. MD5 authentication creates an encoded checksum in the transmitted packet. The receiving router uses an authentication key (password) to verify the MD5 checksum of the packet. There is an optional key ID. The default type is none. Use the no or default options to set the hello-auth type to none.

©Avaya Inc. 2015 All Rights Reserved.

isis l1-dr-priority (on an MLT)

Configure the Level 1 Intermediate-System-to-Intermediate-System (IS-IS) designated router priority to the specified value.

Syntax

- `default isis l1-dr-priority`
- `isis l1-dr-priority <0-127>`
- `no isis l1-dr-priority`

Default

`The default Level 1 designated router priority value is 64.`

Command mode

MLT Interface Configuration

Command parameters

Parameter	Description
`<0-127>`	Configures the Level 1 Intermediate-System-to-Intermediate-System (IS-IS) designated router priority to the specified value.

©Avaya Inc. 2015 All Rights Reserved.

isis l1-dr-priority (on a port)

Configure the Level 1 Intermediate-System-to-Intermediate-System (IS-IS) designated router priority to the specified value.

Syntax

- `default isis l1-dr-priority`
- `isis l1-dr-priority <0-127>`
- `no isis l1-dr-priority`

Default

`The default Level 1 designated router priority value is 64.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<0-127>`	Configures the Level 1 Intermediate-System-to-Intermediate-System (IS-IS) designated router priority to the specified value.

©Avaya Inc. 2015 All Rights Reserved.

isis l1-hello-interval (on an MLT)

Configure the hello interval to change how often hello packets are sent out from an interface level.

Syntax

- `default isis l1-hello-interval`
- `isis l1-hello-interval <1-600>`
- `no isis l1-hello-interval`

Default

The default Level 1 hello interval value is 9 seconds.

Command mode

MLT Interface Configuration

Command parameters

Parameter	Description
<1-600>	Configures the Level 1 hello interval.

©Avaya Inc. 2015 All Rights Reserved.

isis l1-hello-interval (on a port)

Configure the hello interval to change how often hello packets are sent out from an interface level.

Syntax

- `default isis l1-hello-interval`
- `isis l1-hello-interval <1-600>`
- `no isis l1-hello-interval`

Default

The default Level 1 hello interval value is 9 seconds.

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
<1-600>	Configures the Level 1 hello interval.

©Avaya Inc. 2015 All Rights Reserved.

isis l1-hello-multiplier (on an MLT)

Configure the hello multiplier to specify how many hellos the Avaya Virtual Services Platform 9000 must miss before it considers the adjacency with a neighboring switch down.

Syntax

- `default isis l1-hello-multiplier`
- `isis l1-hello-multiplier <1-600>`
- `no isis l1-hello-multiplier`

Default

`The default Level 1 hello-multiplier value is 3 seconds.`

Command mode

MLT Interface Configuration

Command parameters

Parameter	Description
`<1-600>`	Configures the Level 1 hello multiplier.

©Avaya Inc. 2015 All Rights Reserved.

isis l1-hello-multiplier (on a port)

Configure the hello multiplier to specify how many hellos the Avaya Virtual Services Platform 9000 must miss before it considers the adjacency with a neighboring switch down.

Syntax

- `default isis l1-hello-multiplier`
- `isis l1-hello-multiplier <1-600>`
- `no isis l1-hello-multiplier`

Default

`The default Level 1 hello-multiplier value is 3 seconds.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<1-600>`	Configures the Level 1 hello multiplier.

©Avaya Inc. 2015 All Rights Reserved.

isis (on an MLT)

Create an Intermediate-System-to-Intermediate-System (IS-IS) circuit and interface on the selected MultiLink Trunking (MLT) instance.

Syntax

- `default isis enable`
- `isis`
- `isis enable`
- `no isis`
- `no isis enable`

Default

None

Command mode

MLT Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables the Intermediate-System-to-Intermediate-System (IS-IS) circuit and interface on the selected MLT.

©Avaya Inc. 2015 All Rights Reserved.

isis (on a port)

Create an Intermediate-System-to-Intermediate-System (IS-IS) circuit and interface on the selected ports.

Syntax

- `default isis enable`
- `isis`
- `isis enable`
- `no isis`
- `no isis enable`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables the Intermediate-System-to-Intermediate-System (IS-IS) circuit and interface on the selected ports.

©Avaya Inc. 2015 All Rights Reserved.

isis redistribute bgp

Identify routes on the local switch to be announced into the Shortest Path Bridging MAC (SPBM) network.

Syntax

- `default isis redistribute bgp enable`
- `default isis redistribute bgp metric`
- `default isis redistribute bgp metric-type`
- `default isis redistribute bgp route-map`
- `default isis redistribute bgp subnets`
- `isis redistribute bgp`
- `isis redistribute bgp enable`
- `isis redistribute bgp metric <0-65535>`
- `isis redistribute bgp metric-type external`
- `isis redistribute bgp metric-type internal`
- `isis redistribute bgp route-map WORD<0-64>`
- `isis redistribute bgp subnets allow`
- `isis redistribute bgp subnets suppress`
- `no isis redistribute bgp`
- `no isis redistribute bgp enable`
- `no isis redistribute bgp metric`
- `no isis redistribute bgp metric-type`
- `no isis redistribute bgp route-map`
- `no isis redistribute bgp subnets`

Default

By default, redistribution is disabled.

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
enable	Enables Border Gateway Protocol (BGP) route redistribution.

metric <0-65535>	Specifies the metric for the redistributed route. Avaya recommends that you use a value that is consistent with the destination protocol. The default is 1.
metric-type external	Specifies the metric type. Specifies a type 1 or a type 2 metric. For metric type 1, the cost of the external routes is equal to the sum of all internal costs and the external cost. For metric type 2, the cost of the external routes is equal to the external cost alone. The default is internal.
metric-type internal	Specifies the metric type. Specifies a type 1 or a type 2 metric. For metric type 1, the cost of the external routes is equal to the sum of all internal costs and the external cost. For metric type 2, the cost of the external routes is equal to the external cost alone. The default is internal.
route-map WORD<0-64>	Configures the route policy to apply to redistributed routes. Specifies a name.
subnets allow	Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.
subnets suppress	Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose suppress to advertise subnets aggregated to their classful subnet. The default is allow.

©Avaya Inc. 2015 All Rights Reserved.

isis redistribute direct

Identify routes on the local switch to be announced into the Shortest Path Bridging MAC (SPBM) network.

Syntax

- `default isis redistribute direct enable`
- `default isis redistribute direct metric`
- `default isis redistribute direct metric-type`
- `default isis redistribute direct route-map`
- `default isis redistribute direct subnets`
- `isis redistribute direct`
- `isis redistribute direct enable`
- `isis redistribute direct metric <0-65535>`
- `isis redistribute direct metric-type external`
- `isis redistribute direct metric-type internal`
- `isis redistribute direct route-map WORD<0-64>`
- `isis redistribute direct subnets allow`
- `isis redistribute direct subnets suppress`
- `no isis redistribute direct`
- `no isis redistribute direct enable`
- `no isis redistribute direct metric`
- `no isis redistribute direct metric-type`
- `no isis redistribute direct route-map`
- `no isis redistribute direct subnets`

Default

By default, redistribution is disabled.

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
enable	Enables route redistribution.

metric <0-65535>	Configures the metric (cost) to apply to redistributed routes. The default is 1.
metric-type external	Configures the type of route to import into the protocol. The default is internal.
metric-type internal	Configures the type of route to import into the protocol. The default is internal.
route-map WORD<0-64>	Configures the route policy to apply to redistributed routes. Specifies a name.
subnets allow	Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.
subnets suppress	Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose suppress to advertise subnets aggregated to their classful subnet. The default is allow.

©Avaya Inc. 2015 All Rights Reserved.

isis redistribute ospf

Identify routes on the local switch to be announced into the Shortest Path Bridging MAC (SPBM) network.

Syntax

- `default isis redistribute ospf enable`
- `default isis redistribute ospf metric`
- `default isis redistribute ospf metric-type`
- `default isis redistribute ospf route-map`
- `default isis redistribute ospf subnets`
- `isis redistribute ospf`
- `isis redistribute ospf enable`
- `isis redistribute ospf metric <0-65535>`
- `isis redistribute ospf metric-type external`
- `isis redistribute ospf metric-type internal`
- `isis redistribute ospf route-map WORD<0-64>`
- `isis redistribute ospf subnets allow`
- `isis redistribute ospf subnets suppress`
- `no isis redistribute ospf`
- `no isis redistribute ospf enable`
- `no isis redistribute ospf metric`
- `no isis redistribute ospf metric-type`
- `no isis redistribute ospf route-map`
- `no isis redistribute ospf subnets`

Default

By default, redistribution is disabled.

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
enable	Enables route redistribution.

metric <0-65535>	Configures the metric (cost) to apply to redistributed routes. The default is 1.
metric-type external	Configures the type of route to import into the protocol. The default is internal.
metric-type internal	Configures the type of route to import into the protocol. The default is internal.
route-map WORD<0-64>	Configures the route policy to apply to redistributed routes. Specifies a name.
subnets allow	Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.
subnets suppress	Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose suppress to advertise subnets aggregated to their classful subnet. The default is allow.

©Avaya Inc. 2015 All Rights Reserved.

Home | Command modes | Alphabetical listing

isis redistribute rip

Identify routes on the local switch to be announced into the Shortest Path Bridging MAC (SPBM) network.

Syntax

- `default isis redistribute rip enable`
- `default isis redistribute rip metric`
- `default isis redistribute rip metric-type`
- `default isis redistribute rip route-map`
- `default isis redistribute rip subnets`
- `isis redistribute rip`
- `isis redistribute rip enable`
- `isis redistribute rip metric <0-65535>`
- `isis redistribute rip metric-type external`
- `isis redistribute rip metric-type internal`
- `isis redistribute rip route-map WORD<0-64>`
- `isis redistribute rip subnets allow`
- `isis redistribute rip subnets suppress`
- `no isis redistribute rip`
- `no isis redistribute rip enable`
- `no isis redistribute rip metric`
- `no isis redistribute rip metric-type`
- `no isis redistribute rip route-map`
- `no isis redistribute rip subnets`

Default

`By default, redistribution is disabled.`

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
`enable`	Enables route redistribution.

metric <0-65535>	Configures the metric (cost) to apply to redistributed routes. The default is 1.
metric-type external	Configures the type of route to import into the protocol. The default is internal.
metric-type internal	Configures the type of route to import into the protocol. The default is internal.
route-map WORD<0-64>	Configures the route policy to apply to redistributed routes. Specifies a name.
subnets allow	Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.
subnets suppress	Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose suppress to advertise subnets aggregated to their classful subnet. The default is allow.

©Avaya Inc. 2015 All Rights Reserved.

isis redistribute static

Identify routes on the local switch to be announced into the Shortest Path Bridging MAC (SPBM) network.

Syntax

- `default isis redistribute static enable`
- `default isis redistribute static metric`
- `default isis redistribute static metric-type`
- `default isis redistribute static route-map`
- `default isis redistribute static subnets`
- `isis redistribute static`
- `isis redistribute static enable`
- `isis redistribute static metric <0-65535>`
- `isis redistribute static metric-type external`
- `isis redistribute static metric-type internal`
- `isis redistribute static route-map WORD<0-64>`
- `isis redistribute static subnets allow`
- `isis redistribute static subnets suppress`
- `no isis redistribute static`
- `no isis redistribute static enable`
- `no isis redistribute static metric`
- `no isis redistribute static metric-type`
- `no isis redistribute static route-map`
- `no isis redistribute static subnets`

Default

By default, redistribution is disabled.

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
enable	Enables route redistribution.

metric <0-65535>	Configures the metric (cost) to apply to redistributed routes. The default is 1.
metric-type external	Configures the type of route to import into the protocol. The default is internal.
metric-type internal	Configures the type of route to import into the protocol. The default is internal.
route-map WORD<0-64>	Configures the route policy to apply to redistributed routes. Specifies a name.
subnets allow	Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.
subnets suppress	Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose suppress to advertise subnets aggregated to their classful subnet. The default is allow.

©Avaya Inc. 2015 All Rights Reserved.

isis spbm (on an MLT)

Configure Shortest Path Bridging MAC (SPBM) on an Intermediate-System-to-Intermediate-System (IS-IS) interface on a MultiLink Trunking (MLT) instance.

Syntax

- `default isis spbm <1-100> interface-type`
- `default isis spbm <1-100> l1-metric`
- `isis spbm <1-100>`
- `isis spbm <1-100> interface-type { broadcast | pt-pt }`
- `isis spbm <1-100> l1-metric <1-16777215>`
- `no isis spbm <1-100>`
- `no isis spbm <1-100> interface-type`
- `no isis spbm <1-100> l1-metric`

Default

None

Command mode

MLT Interface Configuration

Command parameters

Parameter	Description
`<1-100>`	Specifies the Shortest Path Bridging MAC (SPBM) instance ID.
`interface-type { broadcast | pt-pt }`	Configures the Shortest Path Bridging MAC (SPBM) instance interface type.
`l1-metric <1-16777215>`	Configures the cost for the Shortest Path Bridging MAC (SPBM) instance.

©Avaya Inc. 2015 All Rights Reserved.

isis spbm (on a port)

Enable the Shortest Path Bridging MAC (SPBM) instance on the Intermediate-System-to-Intermediate-System (IS-IS) interfaces.

Syntax

- `default isis spbm <1-100> interface-type`
- `default isis spbm <1-100> l1-metric`
- `isis spbm <1-100>`
- `isis spbm <1-100> interface-type { broadcast | pt-pt }`
- `isis spbm <1-100> l1-metric <1-16777215>`
- `no isis spbm <1-100>`
- `no isis spbm <1-100> interface-type`
- `no isis spbm <1-100> l1-metric`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<1-100>`	Specifies the Shortest Path Bridging MAC (SPBM) instance ID.
`interface-type { broadcast | pt-pt }`	Configures the Shortest Path Bridging MAC (SPBM) instance interface type.
`l1-metric <1-16777215>`	Configures the cost for the Shortest Path Bridging MAC (SPBM) instance.

©Avaya Inc. 2015 All Rights Reserved.

ist enable

Enable an interswitch trunk.

Syntax

- `default ist enable`
- `ist enable`
- `no ist enable`

Default

`The default is disabled.`

Command mode

MLT Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables the interswitch trunk (IST).

©Avaya Inc. 2015 All Rights Reserved.

ist peer-ip

Create an interswitch trunking (IST) from an existing MLT.

Syntax

- `default ist peer-ip`
- `ist peer-ip {A.B.C.D} vlan <1-4084>`
- `no ist peer-ip`

Default

`The default is disabled.`

Command mode

MLT Interface Configuration

Command parameters

Parameter	Description
`<1-4084>`	Specifies the VLAN ID.
`<A.B.C.D>`	Specifies the peer IP address-the IP address of the IST VLAN on the other aggregation switch.

©Avaya Inc. 2015 All Rights Reserved.

is-type

Configure the router type globally. This release supports only Level 1 (l1) Intermediate-System-to-Intermediate-System (IS-IS).

Syntax

- `default is-type`
- `is-type l1`
- `is-type l12`
- `no is-type`

Default

`The default router type is Level 1 (l1).`

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description
`l1`	Configures the router type as Level 1 Intermediate-System-to-Intermediate-System (IS-IS).
`l12`	Configures the router type as Level 1 and Level 2 Intermediate-System-to-Intermediate-System (IS-IS). You cannot use this parameter in this release.

©Avaya Inc. 2015 All Rights Reserved.

l2 ping ip-address

Trigger a Layer 2 ping, which acts like a native ping. Enable Connectivity Fault Management (CFM) to debug Layer 2. It can also help you debug ARP problems by providing the ability to troubleshoot next hop ARP records.

Syntax

- `l2 ping ip-address WORD<0-255>`
- `l2 ping ip-address WORD<0-255> burst-count <1-200>`
- `l2 ping ip-address WORD<0-255> data-tlv-size <0-400>`
- `l2 ping ip-address WORD<0-255> time-out <1-10>`
- `l2 ping ip-address WORD<0-255> vrf WORD<1-16>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`burst-count <1-200>`	Specifies the burst count.
`data-tlv-size <0-400>`	Specifies the data Type-Length-Value (TLV) size. The default is 0.
`time-out <1-10>`	Specifies the interval in seconds. The default is 3.
`vrf WORD<1-16>`	Specifies the VRF name.
`WORD<0-255>`	Specifies the IP address.

©Avaya Inc. 2015 All Rights Reserved.

l2 ping vlan

Trigger a Layer 2 ping, which acts like a native ping. Enable Connectivity Fault Management (CFM) to debug Layer 2. It can also help you debug ARP problems by providing the ability to troubleshoot next hop ARP records.

Syntax

- `l2 ping vlan <1-4084> mac <0x00:0x00:0x00:0x00:0x00:0x00>`
- `l2 ping vlan <1-4084> mac <0x00:0x00:0x00:0x00:0x00:0x00> burst-count <1-200>`
- `l2 ping vlan <1-4084> mac <0x00:0x00:0x00:0x00:0x00:0x00> data-tlv-size <0-400>`
- `l2 ping vlan <1-4084> mac <0x00:0x00:0x00:0x00:0x00:0x00> frame-size <64-1500>`
- `l2 ping vlan <1-4084> mac <0x00:0x00:0x00:0x00:0x00:0x00> priority <0-7>`
- `l2 ping vlan <1-4084> mac <0x00:0x00:0x00:0x00:0x00:0x00> source-mode nodal`
- `l2 ping vlan <1-4084> mac <0x00:0x00:0x00:0x00:0x00:0x00> source-mode noVlanMac`
- `l2 ping vlan <1-4084> mac <0x00:0x00:0x00:0x00:0x00:0x00> source-mode smltVirtual`
- `l2 ping vlan <1-4084> mac <0x00:0x00:0x00:0x00:0x00:0x00> testfill-pattern all-zero`
- `l2 ping vlan <1-4084> mac <0x00:0x00:0x00:0x00:0x00:0x00> testfill-pattern all-zero-crc`
- `l2 ping vlan <1-4084> mac <0x00:0x00:0x00:0x00:0x00:0x00> testfill-pattern pseudo-random-bit-sequence`
- `l2 ping vlan <1-4084> mac <0x00:0x00:0x00:0x00:0x00:0x00> testfill-pattern pseudo-random-bit-sequence-crc`
- `l2 ping vlan <1-4084> mac <0x00:0x00:0x00:0x00:0x00:0x00> time-out <1-10>`
- `l2 ping vlan <1-4084> routernodename WORD<0-255>`
- `l2 ping vlan <1-4084> routernodename WORD<0-255> burst-count <1-200>`
- `l2 ping vlan <1-4084> routernodename WORD<0-255> data-tlv-size <0-400>`
- `l2 ping vlan <1-4084> routernodename WORD<0-255> frame-size <64-1500>`
- `l2 ping vlan <1-4084> routernodename WORD<0-255> priority <0-7>`
- `l2 ping vlan <1-4084> routernodename WORD<0-255> source-mode nodal`
- `l2 ping vlan <1-4084> routernodename WORD<0-255> source-mode noVlanMac`
- `l2 ping vlan <1-4084> routernodename WORD<0-255> source-mode smltVirtual`
- `l2 ping vlan <1-4084> routernodename WORD<0-255> testfill-pattern all-zero`
- `l2 ping vlan <1-4084> routernodename WORD<0-255> testfill-pattern all-zero-crc`
- `l2 ping vlan <1-4084> routernodename WORD<0-255> testfill-pattern pseudo-random-bit-sequence`

- `l2 ping vlan <1-4084> routernodename WORD<0-255> testfill-pattern pseudo-random-bit-sequence-crc`
- `l2 ping vlan <1-4084> routernodename WORD<0-255> time-out <1-10>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<1-4084>`	Specifies the VLAN ID.
`burst-count <1-200>`	Specifies the burst count.
`data-tlv-size <0-400>`	Specifies the data Type-Length-Value (TLV) size. The default is 0.
`frame-size <64-1500>`	Specifies the frame size. The default is 0.
`mac <0x00:0x00:0x00:0x00:0x00:0x00>`	Specifies the MAC address.
`priority <0-7>`	Specifies the priority. The default is 7.
`routernodename WORD<0-255>`	Specifies the router node name. VSP 9000 does not support the routernodename option for C-VLANs.
`source-mode nodal`	Specifies the source mode of nodal. Nodal MPs provide both MEP and MIP functionality for SPBM deployments. Nodal MPs are associated with a B-VLAN and are VLAN encapsulated packets. The default is nodal. This mode applies to both B-VLANs and C-VLANs.
`source-mode noVlanMac`	Specifies the source mode of noVlanMac. Use this value only for C-VLANs. The default is nodal.
`source-mode smltVirtual`	Specifies the source mode of smltVirtual. Virtual Services Platform 9000 supports SMLT interaction with SPBM. The platform uses two B-VIDs into the core from each pair of SMLT terminating nodes. Both nodes advertise the Nodal B-MAC into the core on both B-VIDS. In addition each node advertises the SMLT virtual B-MAC on one of the two B-VLANs. The default is nodal.
`testfill-pattern all-zero`	Specifies the testfill pattern. Range is: all-zero: null signal without cyclic redundancy check; all-zero-crc: null signal with cyclic redundancy check with 32-bit polynomial; pseudo-random-bit-sequence: PRBS without cyclic redundancy check; or pseudo-random-bit-sequence-crc: PBRS with cyclic redundancy check with 32-bit polynomial. A cyclic redundancy check is a code that detects errors. The default is all-zero.
`testfill-pattern all-zero-crc`	Specifies the testfill pattern. Range is: all-zero: null signal without cyclic redundancy check; all-zero-crc: null signal with cyclic redundancy check with 32-bit polynomial; pseudo-random-bit-sequence: PRBS without cyclic redundancy check; or pseudo-random-bit-sequence-crc: PBRS with cyclic redundancy check with 32-bit polynomial. A cyclic redundancy check is a code that detects errors. The default is all-zero.
	Specifies the testfill pattern. Range is: all-zero: null signal without cyclic redundancy check; all-zero-crc: null signal

	with cyclic redundancy check with 32-bit polynomial;
testfill-pattern pseudo-random-bit-sequence	pseudo-random-bit-sequence: PRBS without cyclic redundancy check; or pseudo-random-bit-sequence-crc: PBRS with cyclic redundancy check with 32-bit polynomial. A cyclic redundancy check is a code that detects errors. The default is all-zero.
testfill-pattern pseudo-random-bit-sequence-crc	Specifies the testfill pattern. Range is: all-zero: null signal without cyclic redundancy check; all-zero-crc: null signal with cyclic redundancy check with 32-bit polynomial; pseudo-random-bit-sequence: PRBS without cyclic redundancy check; or pseudo-random-bit-sequence-crc: PBRS with cyclic redundancy check with 32-bit polynomial. A cyclic redundancy check is a code that detects errors. The default is all-zero.
time-out <1-10>	Specifies the interval in seconds. The default is 3.

©Avaya Inc. 2015 All Rights Reserved.

l2 tracemroute

Trigger a Layer 2 multicast traceroute. Enable Connectivity Fault Management (CFM) to debug Layer 2.

Syntax

- `l2 tracemroute source {A.B.C.D} group {A.B.C.D}`
- `l2 tracemroute source {A.B.C.D} group {A.B.C.D} priority <0-7>`
- `l2 tracemroute source {A.B.C.D} group {A.B.C.D} ttl-value <1-255>`
- `l2 tracemroute source {A.B.C.D} group {A.B.C.D} vlan <1-4084>`
- `l2 tracemroute source {A.B.C.D} group {A.B.C.D} vrf WORD<1-16>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`group {A.B.C.D}`	Specifies the multicast group address.
`priority <0-7>`	Specifies the priority. The default is 7.
`source {A.B.C.D}`	Specifies the source address.
`ttl-value <1-255>`	Specifies the time-to-live value for the trace.
`vlan <1-4084>`	Specifies the VLAN ID.
`vrf WORD<1-16>`	Specifies the VRF name.

©Avaya Inc. 2015 All Rights Reserved.

l2 traceroute ip-address

Trigger a Layer 2 traceroute, which acts like native traceroute. Enable Connectivity Fault Management (CFM) to debug Layer 2. It can also help you debug ARP problems by providing the ability to troubleshoot next hop ARP records.

Syntax

- `l2 traceroute ip-address WORD<0-255>`
- `l2 traceroute ip-address WORD<0-255> priority <0-7>`
- `l2 traceroute ip-address WORD<0-255> source-mode nodal`
- `l2 traceroute ip-address WORD<0-255> source-mode noVlanMac`
- `l2 traceroute ip-address WORD<0-255> source-mode smltVirtual`
- `l2 traceroute ip-address WORD<0-255> ttl-value <1-255>`
- `l2 traceroute ip-address WORD<0-255> vrf WORD<1-16>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`ip-address WORD<0-255>`	Specifies the IP address.
`priority <0-7>`	Specifies the priority. The default is 7.
`source-mode nodal`	Specifies the source mode of nodal. Nodal MPs provide both MEP and MIP functionality for SPBM deployments. Nodal MPs are associated with a B-VLAN and are VLAN encapsulated packets. The default is nodal.
`source-mode noVlanMac`	Specifies the source mode of noVlanMac. Use this value only for C-VLANs. The default is nodal.
`source-mode smltVirtual`	Specifies the source mode of smltVirtual. Virtual Services Platform 9000 supports SMLT interaction with SPBM. The platform uses two B-VIDs into the core from each pair of SMLT terminating nodes. Both nodes advertise the Nodal B-MAC into the core on both B-VIDS. In addition each node advertises the SMLT virtual B-MAC on one of the two B-VLANs. The default is nodal.
`ttl-value <1-255>`	Specifies the time-to-live (TTL) value. The default is 64.
`vrf WORD<1-16>`	Specifies the VRF name.

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

l2 traceroute vlan

Trigger a Layer 2 traceroute, which acts like native traceroute. Enable Connectivity Fault Management (CFM) to debug Layer 2. It can also help you debug ARP problems by providing the ability to troubleshoot next hop ARP records.

Syntax

- `l2 traceroute vlan <1-4084> mac 0x00:0x00:0x00:0x00:0x00:0x00`
- `l2 traceroute vlan <1-4084> mac 0x00:0x00:0x00:0x00:0x00:0x00`
- `l2 traceroute vlan <1-4084> mac 0x00:0x00:0x00:0x00:0x00:0x00 priority <0-7>`
- `l2 traceroute vlan <1-4084> mac 0x00:0x00:0x00:0x00:0x00:0x00 priority <0-7> vrf WORD<1-16>`
- `l2 traceroute vlan <1-4084> mac 0x00:0x00:0x00:0x00:0x00:0x00 source-mode {nodal|noVlanMac|smltVirtual}`
- `l2 traceroute vlan <1-4084> mac 0x00:0x00:0x00:0x00:0x00:0x00 source-mode {nodal|noVlanMac|smltVirtual} vrf WORD<1-16>`
- `l2 traceroute vlan <1-4084> mac 0x00:0x00:0x00:0x00:0x00:0x00 ttl-value <1-255>`
- `l2 traceroute vlan <1-4084> mac 0x00:0x00:0x00:0x00:0x00:0x00 ttl-value <1-255> vrf WORD<1-16>`
- `l2 traceroute vlan <1-4084> routernodename WORD<0-255>`
- `l2 traceroute vlan <1-4084> routernodename WORD<0-255> priority <0-7>`
- `l2 traceroute vlan <1-4084> routernodename WORD<0-255> priority <0-7> vrf WORD<1-16>`
- `l2 traceroute vlan <1-4084> routernodename WORD<0-255> source-mode {nodal|noVlanMac|smltVirtual}`
- `l2 traceroute vlan <1-4084> routernodename WORD<0-255> source-mode {nodal|noVlanMac|smltVirtual} vrf WORD<1-16>`
- `l2 traceroute vlan <1-4084> routernodename WORD<0-255> ttl-value <1-255>`
- `l2 traceroute vlan <1-4084> routernodename WORD<0-255> ttl-value <1-255> vrf WORD<1-16>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<1-4084>	Specifies the VLAN ID.
mac <0x00:0x00:0x00:0x00:0x00:0x00>	Specifies the MAC address.

`priority <0-7>`	Specifies the priority. The default is 7.
`routernodename WORD<0-255>`	Specifies the router node name. VSP 9000 does not support the routernodename option for C-VLANs.
`source-mode <nodal|noVlanMac|smltVirtual>`	Specifies the source mode as nodal, noVlanMac, or smltVirtual. Use the smltVirtual value with B-VLANs only. Use the noVlanMac value with C-VLANs only. The default is nodal.
`ttl-value <1-255>`	Specifies the time-to-live (TTL) value. The default is 64.
`vrf WORD<1-16>`	Specifies the VRF name.

©Avaya Inc. 2015 All Rights Reserved.

l2 tracetree

Trigger a Layer 2 tracetree. Layer 2 tracetree allows a user to trigger a multicast link trace message (LTM) by specifying the Backbone VLAN (B-VLAN) and service instance identifier (I-SID). The command allows the user to view a multicast tree on the SPBM B-VLAN from the source node to the destination nodes for a particular I-SID.

Syntax

- `l2 tracetree <1-4084> <1-16777215>`
- `l2 tracetree <1-4084> <1-16777215> mac 0x00:0x00:0x00:0x00:0x00:0x00`
- `l2 tracetree <1-4084> <1-16777215> mac 0x00:0x00:0x00:0x00:0x00:0x00 priority <0-7>`
- `l2 tracetree <1-4084> <1-16777215> mac 0x00:0x00:0x00:0x00:0x00:0x00 source-mode nodal`
- `l2 tracetree <1-4084> <1-16777215> mac 0x00:0x00:0x00:0x00:0x00:0x00 source-mode smltVirtual`
- `l2 tracetree <1-4084> <1-16777215> mac 0x00:0x00:0x00:0x00:0x00:0x00 ttl-value <1-255>`
- `l2 tracetree <1-4084> <1-16777215> priority <0-7>`
- `l2 tracetree <1-4084> <1-16777215> routernodename WORD<0-255>`
- `l2 tracetree <1-4084> <1-16777215> routernodename WORD<0-255> priority <0-7>`
- `l2 tracetree <1-4084> <1-16777215> routernodename WORD<0-255> source-mode nodal`
- `l2 tracetree <1-4084> <1-16777215> routernodename WORD<0-255> source-mode smltVirtual`
- `l2 tracetree <1-4084> <1-16777215> routernodename WORD<0-255> ttl-value <1-255>`
- `l2 tracetree <1-4084> <1-16777215> source-mode nodal`
- `l2 tracetree <1-4084> <1-16777215> source-mode smltVirtual`
- `l2 tracetree <1-4084> <1-16777215> ttl-value <1-255>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<1-16777215>	Specifies the service instance identifier (I-SID).
<1-4084>	Specifies the VLAN ID.
mac <0x00:0x00:0x00:0x00:0x00:0x00>	Specifies the MAC address.
priority <0-7>	Specifies the priority value. The default is 7.

routernodename WORD<0-255>	Specifies the router node name.
source-mode nodal	Specifies the source mode of nodal or smltVirtual. The default is nodal.
source-mode smltVirtual	Specifies the source mode of nodal or smltVirtual. The default is nodal.
ttl-value <1-255>	Specifies the time-to-live (TTL) value. The default is 64.

©Avaya Inc. 2015 All Rights Reserved.

lacp aggregation enable

Configures the port as aggregatable. Use the no operator to remove this configuration.

Syntax

- `default lacp aggregation enable`
- `lacp aggregation enable`
- `no lacp aggregation enable`

Default

`The default is disabled.`

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

lacp aggr-wait-time <200-2000>

Configure the aggregation wait time (in milliseconds) for the port.

Syntax

- `default lacp aggr-wait-time`
- `lacp aggr-wait-time <200-2000>`

Default

`The default value is 2000.`

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

lacp enable (for a port)

Enable LACP for the port.

Syntax

- `default lacp`
- `default lacp enable`
- `lacp enable`
- `no lacp`
- `no lacp enable`

Default

`The default is disabled.`

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

lacp fast-periodic-time <200-20000>

Configure the fast-periodic time (in milliseconds) for the port.

Syntax

- `default lacp fast-periodic-time`
- `lacp fast-periodic-time <200-20000>`

Default

`The default is 20000 ms.`

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

lacp (globally)

Configure Link Aggregation Control Protocol (LACP) parameters globally. When the LACP system priority is set globally, it applies to all LACP-enabled aggregators and ports.

Syntax

- `default lacp`
- `default lacp aggr-wait-time`
- `default lacp enable`
- `default lacp fast-periodic-time`
- `default lacp slow-periodic-time`
- `default lacp system-priority`
- `default lacp timeout-scale`
- `lacp aggr-wait-time <200-2000>`
- `lacp enable`
- `lacp fast-periodic-time <200-20000>`
- `lacp slow-periodic-time <10000-30000>`
- `lacp smlt-sys-id 0x00:0x00:0x00:0x00:0x00:0x00`
- `lacp system-priority <0-65535>`
- `lacp timeout-scale <2-10>`
- `no lacp`
- `no lacp enable`

Default

`The default is disabled.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`aggr-wait-time <200-2000>`	Sets the aggregation wait time (in milliseconds) globally. The default value is 2000.
`enable`	Enables the Link Aggregation Control Protocol (LACP) globally.
	Sets the fast-periodic time (in milliseconds) globally. The

`fast-periodic-time <200-20000>`	default is 20000 ms.
`slow-periodic-time <10000-30000>`	Sets the slow periodic time globally. The default value is 1000 ms.
`smlt-sys-id <0x00:0x00:0x00:0x00:0x00:0x00>`	Sets the LACP system ID globally. Enter a MAC address in the following format: 0x00:0x00:0x00:0x00:0x00:0x00.
`system-priority <0-65535>`	Sets the global LACP system priority. The default value is 32768.
`timeout-scale <2-10>`	Sets the timeout scale globally. The default value is 3.

©Avaya Inc. 2015 All Rights Reserved.

lacp key <0-65535>

Configure the aggregation key for the port.

Syntax

- `default lacp key`
- `lacp key <0-65535>`

Default

`The default is 0.`

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

lacp mode

Configure the Link Aggregation Control Protocol (LACP) mode to be active or passive.

Syntax

- `default lacp mode`
- `lacp mode active`
- `lacp mode passive`

Default

`The default is passive.`

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

lacp (on an MLT)

Configure a MultiLink Trunking (MLT) with Link Aggregation Control Protocol (LACP) to use the dynamic link aggregation function.

Syntax

- `default lacp`
- `default lacp enable`
- `default lacp key`
- `default lacp system-priority`
- `lacp enable`
- `lacp key <0-512>`
- `lacp system-priority <0-65535>`
- `no lacp`
- `no lacp enable`

Default

None

Command mode

MLT Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables Link Aggregation Control Protocol (LACP) on the MLT interface. The default is disabled.
`key <0-512>`	Sets the Link Aggregation Control Protocol (LACP) aggregator key for a specific MLT. <0-512> specifies the Link Aggregation Control Protocol (LACP) actor admin key. The default key value is 0
`system-priority <0-65535>`	Sets the Link Aggregation Control Protocol (LACP) system priority for a specific MLT. <0-65535> specifies the system priority. The default system-priority is 32768.

©Avaya Inc. 2015 All Rights Reserved.

lacp partner-key <0-65535>

Configure the partner administrative key.

Syntax

- `default lacp partner-key`
- `lacp partner-key <0-65535>`

Default

`The default is 0.`

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

lacp partner-port <0-65535>

Configure the partner administrative port value.

Syntax

- `default lacp partner-port`
- `lacp partner-port <0-65535>`

Default

None

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

lacp partner-port-priority <0-65535>

Configure the partner administrative port priority value.

Syntax

- `default lacp partner-port-priority`
- `lacp partner-port-priority <0-65535>`

Default

`The default is 0.`

Command mode

GigabitEthernet Interface Configuration

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

lacp partner-state <0-255 | 0x0-0xff>

Configure the partner administrative state bitmask. Specify the partner administrative state bitmap in the range 0x0-0xff. The bit to state mapping is Exp, Def, Dis, Col, Syn, Agg, Time, and Act. For example, to set the two partner-state parameters Act = true Agg = true specify a value of 0x05 (bitmap = 00000101).

Syntax

- `default lacp partner-state`
- `lacp partner-state <0-255 | 0x0-0xff>`

Default

None

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

lacp partner-system-id

Configure the partner administrative system ID.

Syntax

- `default lacp partner-system-id`
- `lacp partner-system-id 0x00:0x00:0x00:0x00:0x00:0x00`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`0x00:0x00:0x00:0x00:0x00:0x00`	Specifies a MAC address in the format 0x00:0x00:0x00:0x00:0x00:0x00.

©Avaya Inc. 2015 All Rights Reserved.

lacp partner-system-priority <0-65535>

Configure the partner administrative system priority value.

Syntax

- `default lacp partner-system-priority`
- `lacp partner-system-priority <0-65535>`

Default

`The default value is 32768.`

Command mode

GigabitEthernet Interface Configuration

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

lacp priority <0-65535>

Configure the port priority.

Syntax

- `default lacp priority`
- `lacp priority <0-65535>`

Default

`The default value is 32768.`

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

lacp slow-periodic-time <10000-30000>

Configure the slow periodic time.

Syntax

- `default lacp slow-periodic-time`
- `lacp slow-periodic-time <10000-30000>`

Default

`The default value is 1000 ms.`

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

lacp system-priority <0-65535>

Configure the LACP system priority.

Syntax

- `default lacp system-priority`
- `lacp system-priority <0-65535>`

Default

`The default value is 32768.`

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

lacp timeout-scale <2-10>

Configure the timeout scale.

Syntax

- `default lacp timeout-scale`
- `lacp timeout-scale <2-10>`

Default

`The default is 3.`

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

lacp timeout-time

Configure the timeout to either long or short.

Syntax

- `default lacp timeout-time`
- `lacp timeout-time long`
- `lacp timeout-time short`

Default

`The default is long.`

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

line-card

Perform trace commands for input/output and switch fabric cards.

Syntax

- line-card trace grep
- line-card trace grep WORD<0-1024>
- line-card trace level
- line-card trace level <67-179> <0-4>
- line-card SF1 trace grep
- line-card SF1 trace grep WORD<0-1024>
- line-card SF1 trace level
- line-card SF1 trace level <67-179> <0-4>
- line-card SF2 trace grep
- line-card SF2 trace grep WORD<0-1024>
- line-card SF2 trace level
- line-card SF2 trace level <67-179> <0-4>
- line-card SF3 trace grep
- line-card SF3 trace grep WORD<0-1024>
- line-card SF3 trace level
- line-card SF3 trace level <67-179> <0-4>
- line-card SF4 trace grep
- line-card SF4 trace grep WORD<0-1024>
- line-card SF4 trace level
- line-card SF4 trace level <67-179> <0-4>
- line-card SF5 trace grep
- line-card SF5 trace grep WORD<0-1024>
- line-card SF5 trace level
- line-card SF5 trace level <67-179> <0-4>
- line-card SF6 trace grep
- line-card SF6 trace grep WORD<0-1024>

- `line-card SF6 trace level`
- `line-card SF6 trace level <67-179> <0-4>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<3-12>	Specifies the slot number for IO card in the range of 3 to 12.
grep <0-1024>	Greps the string in the range of 0 to 1024.
level <67-179>	Sets the trace level.
SF1	Specifies Switch Fabric 1.
SF2	Specifies Switch Fabric 2.
SF3	Specifies Switch Fabric 3.
SF4	Specifies Switch Fabric 4.
SF5	Specifies Switch Fabric 5.
SF6	Specifies Switch Fabric 6.
trace	Sets the trace level.

©Avaya Inc. 2015 All Rights Reserved.

link-flap-detect

Configure link flap detection to control link state changes on a physical port.

Syntax

- `default link-flap-detect auto-port-down`
- `default link-flap-detect auto-port-down frequency`
- `default link-flap-detect auto-port-down frequency interval`
- `default link-flap-detect auto-port-down frequency interval send-trap`
- `default link-flap-detect auto-port-down frequency send-trap`
- `default link-flap-detect auto-port-down interval`
- `default link-flap-detect auto-port-down interval send-trap`
- `default link-flap-detect auto-port-down send-trap`
- `default link-flap-detect frequency`
- `default link-flap-detect frequency interval`
- `default link-flap-detect frequency interval send-trap`
- `default link-flap-detect frequency send-trap`
- `default link-flap-detect interval`
- `default link-flap-detect interval send-trap`
- `default link-flap-detect send-trap`
- `link-flap-detect auto-port-down`
- `link-flap-detect frequency <1-9999>`
- `link-flap-detect frequency <1-9999> interval <2-600>`
- `link-flap-detect interval <2-600>`
- `link-flap-detect send-trap`
- `no link-flap-detect auto-port-down`
- `no link-flap-detect auto-port-down send-trap`
- `no link-flap-detect send-trap`

Default

None

Command mode

Command parameters

Parameter	Description
`auto-port-down`	Activates automatic disabling of the port if the link-flap threshold is exceeded. The default is enabled.
`frequency <1-9999>`	Configures the number of changes that are allowed during the time specified by the interval command. The default is 20.
`interval <2-600>`	Configures the link-flap-detect interval in seconds. The default is 60.
`send-trap`	Activates sending traps. The default is enabled.

©Avaya Inc. 2015 All Rights Reserved.

linktrace

Trigger a linktrace. The linktrace message is often compared to traceroute. A MEP transmits the Linktrace Message packet to a maintenance endpoint with intermediate points responding to indicate the path of the traffic within a domain for the purpose of fault isolation. The packet specifies the target MAC address of a MP, which is the SPBM system ID or the virtual SMLT MAC. MPs on the path to the target address respond with an LTR.

Syntax

- `linktrace WORD<1-22> WORD<1-22> <1-8191> <0x00:0x00:0x00:0x00:0x00:0x00>`
- `linktrace WORD<1-22> WORD<1-22> <1-8191> <0x00:0x00:0x00:0x00:0x00:0x00> detail`
- `linktrace WORD<1-22> WORD<1-22> <1-8191> <0x00:0x00:0x00:0x00:0x00:0x00> priority <0-7>`
- `linktrace WORD<1-22> WORD<1-22> <1-8191> <0x00:0x00:0x00:0x00:0x00:0x00> source-mode nodal`
- `linktrace WORD<1-22> WORD<1-22> <1-8191> <0x00:0x00:0x00:0x00:0x00:0x00> source-mode smltVirtual`
- `linktrace WORD<1-22> WORD<1-22> <1-8191> <0x00:0x00:0x00:0x00:0x00:0x00> ttl-value <1-255>`
- `linktrace WORD<1-22> WORD<1-22> <1-8191> 0x00:0x00:0x00:0x00:0x00:0x00 source-mode noVlanMac`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<0x00:0x00:0x00:0x00:0x00:0x00>`	Specifies the remote MAC address to reach the MEP/MIP.
`<1-8191>`	Specifies the MEP ID.
`detail`	Displays linktrace result details.
`priority <0-7>`	Specifies the priority. The default is 7.
`source-mode {nodal|noVlanMac|smltVirtual}`	Specifies the source mode as nodal, noVlanMac, or smltVirtual. Use the smltVirtual value with B-VLANs only. Use the noVlanMac value with C-VLANs only. The default is nodal.
`ttl-value <1-255>`	Specifies the time-to-live (TTL) value. The default is 64.
`WORD<1-22>`	The first parameter, specifies the MD name.
`WORD<1-22>`	The second parameter, specifies the MA name.

©Avaya Inc. 2015 All Rights Reserved.

load-encryption-module

Load the appropriate Simple Network Management Protocol version 3 (SNMPv3) encryption module before you can use SNMPv3 with Data Encryption Standard (DES) or Advanced Encryption Standard (AES) to access the device.

Syntax

- `load-encryption-module <3DES|DES|AES>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
3DES|DES|AES	Specifies the Simple Network Management Protocol version 3 (SNMPv3) encryption module to load: 3DES| AES| DES.

©Avaya Inc. 2015 All Rights Reserved.

load-license

Load a license file to unlock the licensed features.

Syntax

- `load-license`

Default

None

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

lock

Lock a port to prevent other users from changing port parameters or modifying port action.

Syntax

- `default lock`
- `default lock enable`
- `default lock port {slot/port[-slot/port][,...]}`
- `lock`
- `lock enable`
- `lock port {slot/port[-slot/port][,...]}`
- `no lock`
- `no lock enable`
- `no lock port {slot/port[-slot/port][,...]}`
- `no lock port {slot/port[-slot/port][,...]} enable`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`port{slot/port [-slot/port][,...]}`	Specifies the slot and the port number to be locked.

©Avaya Inc. 2015 All Rights Reserved.

logging level

Determine what messages the system records in the log.

Syntax

- `logging level <0-4>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`level <0-4>`	Shows and configures the logging level. The level is one of the following values: 0 = Information; all messages are recorded. 1 = Warning; only warning and more serious messages are recorded. 2 = Error; only error and more serious messages are recorded. 3 = Manufacturing; this parameter is not available for customer use. 4 = Fatal; only fatal messages are recorded.

©Avaya Inc. 2015 All Rights Reserved.

logging logToExtFlash

Begin or stop logging system messages to the external flash.

Syntax

- `default logging logToExtFlash`
- `logging logToExtFlash`
- `no logging logToExtFlash`

Default

`The default is no logging logToExtFlash`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

logging screen

Configure the system to display log messages on screen.

Syntax

- `logging screen`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
screen	Configures the system to display the log messages on screen.

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

logging transferFile

Configure the remote host address for log transfer. The system transfers the current log file to a remote host when the log file size reaches the configured maximum size.

Syntax

- `logging transferFile <1-10> address <A.B.C.D>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`<1-10>`	Specifies the file ID to transfer.
`address <A.B.C.D>`	Specifies the IP address of the host to which to transfer the log file. The remote host must be reachable or the configuration fails.

©Avaya Inc. 2015 All Rights Reserved.

logging transferFile filename-prefix

Create the filename on the remote host. The system transfers the current log file to a remote host when the log file size reaches the configured maximum size.

Syntax

- `logging transferFile <1-10> filename-prefix WORD<0-200>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`<1-10>`	Specifies the file ID to transfer.
`filename-prefix WORD<0-2005>`	Specifies the name of the file on the remote host. If you do not configure a name, the current log file name is the default. Important: Avaya recommends that you do not configure this option. If you configure this option, the previously transferred log file is overwritten on the remote server.

©Avaya Inc. 2015 All Rights Reserved.

logging write

Write to the log file automatically created by the system.

Syntax

- `logging write WORD<1-1536>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`write WORD<1-1536>`	Writes the designated string to the log file. WORD<1-1536> is the string or command that you append to the log file. If the string contains spaces, you must enclose the string in quotation marks (").

©Avaya Inc. 2015 All Rights Reserved.

login

Login to a different user access level.

Syntax

- `login`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

login-message

Change the login prompt for ACLI.

Syntax

- `default login-message`
- `login-message WORD<1-1513>`
- `no login-message`

Default

`The default is Login.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`WORD<1-1513>`	Changes the ACLI logon prompt. WORD<1-1513> is an American Standard Code for Information Interchange (ASCII) string from 1-1513 characters.

©Avaya Inc. 2015 All Rights Reserved.

logout

Ends the current session.

Syntax

- `logout`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

loopback

Trigger the loopback test. The LBM packet is often compared to ping. A MEP transmits the loopback message to an intermediate or endpoint within a domain for the purpose of fault verification. This can be used to check the ability of the network to forward different sized frames.

Syntax

- `loopback WORD<1-22> WORD<1-22> <1-8191> < 0x00:0x00:0x00:0x00:0x00:0x00> testfill-pattern pseudo-random-bit-sequence`
- `loopback WORD<1-22> WORD<1-22> <1-8191> <0x00:0x00:0x00:0x00:0x00:0x00>`
- `loopback WORD<1-22> WORD<1-22> <1-8191> <0x00:0x00:0x00:0x00:0x00:0x00> burst-count <1-200>`
- `loopback WORD<1-22> WORD<1-22> <1-8191> <0x00:0x00:0x00:0x00:0x00:0x00> data-tlv-size <0-400>`
- `loopback WORD<1-22> WORD<1-22> <1-8191> <0x00:0x00:0x00:0x00:0x00:0x00> frame-size <64-1500>`
- `loopback WORD<1-22> WORD<1-22> <1-8191> <0x00:0x00:0x00:0x00:0x00:0x00> interframe-interval <0-1000>`
- `loopback WORD<1-22> WORD<1-22> <1-8191> <0x00:0x00:0x00:0x00:0x00:0x00> source-mode nodal`
- `loopback WORD<1-22> WORD<1-22> <1-8191> <0x00:0x00:0x00:0x00:0x00:0x00> source-mode noVlanMac`
- `loopback WORD<1-22> WORD<1-22> <1-8191> <0x00:0x00:0x00:0x00:0x00:0x00> source-mode smltVirtual`
- `loopback WORD<1-22> WORD<1-22> <1-8191> <0x00:0x00:0x00:0x00:0x00:0x00> testfill-pattern all-zero`
- `loopback WORD<1-22> WORD<1-22> <1-8191> <0x00:0x00:0x00:0x00:0x00:0x00> testfill-pattern all-zero-crc`
- `loopback WORD<1-22> WORD<1-22> <1-8191> <0x00:0x00:0x00:0x00:0x00:0x00> testfill-pattern pseudo-random-bit-sequence-crc`
- `loopback WORD<1-22> WORD<1-22> <1-8191> <0x00:0x00:0x00:0x00:0x00:0x00> time-out <1-10>`
- `loopback WORD<1-22> WORD<1-22> <1-8191> <0x00:0x00:0x00:0x00:0x00:0x00> priority <0-7>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<0x00:0x00:0x00:0x00:0x00:0x00>	Specifies the remote MAC address to reach the MEP/MIP.

<1-8191>	Specifies the MEP ID.
burst-count <1-200>	Specifies the burst count.
data-tlv-size <0-400>	Specifies the data Type-Length-Value (TLV) size.
frame-size <64-1500>	Specifies the frame size. The default is 0.
interframe-interval <0-1000>	Specifies the interval between LBM frames in msecs. A value of 0 msecs indicates to send the frames as fast as possible. The default is 500.
priority <0-7>	Specifies the priority. The default is 7.
source-mode {nodal|noVlanMac|smltVirtual}	Specifies the source mode as nodal, noVlanMac, or smltVirtual. Use the smltVirtual value with B-VLANs only. Use the noVlanMac value with C-VLANs only. The default is nodal.
test-fill-pattern {all-zero|all-zero-crc|pseudo-random-bit-sequence|pseudo-random-bit-sequence-crc}	Specifies the testfill pattern: all-zero: null signal without cyclic redundancy check; all-zero-crc: null signal with cyclic redundancy check with 32-bit polynomial; pseudo-random-bit-sequence: PRBS without cyclic redundancy check; or pseudo-random-bit-sequence-crc: pseudo-random-bit-sequence with cyclic redundancy check with 32-bit polynomial. A cyclic redundancy check is a code that detects errors. The default is 1:all-zero.
time-out <1-10>	Specifies the time-out interval in seconds. The default is 3.
WORD<1-22>	The first parameter, specifies the MD name.
WORD<1-22>	The second parameter, specifies the MA name.

©Avaya Inc. 2015 All Rights Reserved.

loop-detect

Configure loop detect to determine if the same MAC address appears on different ports. Use the ARP-Detect feature to account for ARP packets on IP configured interfaces.

Syntax

- `default loop-detect`
- `loop-detect`
- `no loop-detect`

Default

`The default is disabled.`

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

loop-detect action

Configure the ARP loop detection when loop-detect is enabled.

Syntax

- `default loop-detect action`
- `loop-detect action mac-discard`
- `loop-detect action port-down`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`action`	Indicates the action that the switch takes: port-down or mac-discard.

©Avaya Inc. 2015 All Rights Reserved.

loop-detect arp-detect

Configure Loop Detection to detect the MAC addresses that are looping from one port to another port.

Syntax

- `default loop-detect arp-detect`
- `loop-detect arp-detect`
- `no loop-detect arp-detect`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`action`	Specifies the loop detect action to be taken.
`arp-detect`	The Address Resolution Protocol (ARP)-Detect feature is used for IP configured interfaces for ARP packets. Enable this feature (in addition to loop detection) on routed interfaces.

©Avaya Inc. 2015 All Rights Reserved.

lossless-port

Enable the lossless mode for the port.

Syntax

- `default lossless-port`
- `default lossless-port enable`
- `default lossless-port pause-type`
- `default lossless-port pfc-bandwidth`
- `lossless-port`
- `lossless-port enable`
- `lossless-port pause-type fc`
- `lossless-port pause-type pfc`
- `lossless-port pfc-bandwidth <2-8>`
- `no lossless-port`
- `no lossless-port enable`

Default

`The default for lossless-port enable is disabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables Lossless Ethernet mode for the port. The default is disabled. Use the no parameter, no lossless-port, to disable Lossless Ethernet mode for the port. On Virtual Services Platform 9000, you can configure 10 GbE ports to be lossless. You can configure all unicast traffic on the port to be lossless, or you can configure all tagged unicast traffic with a specific lossless 802.1p value to be lossless. All tagged unicast traffic on the port with an 802.1p value matching the value of lossless-802.1p is lossless. The switch treats traffic that does not meet this requirement as lossy traffic. The switch can drop the lossy traffic. A maximum of two ports can be operational in a lossless cluster: either two lossless ports, or one lossless port and one lossy port. If a port in a cluster half is lossless enabled, the other three ports in that half will be held operationally down. If you do not enable Lossless Ethernet on any ports in a lossless cluster half, only the lowest numerical port, which is administratively enabled, is operational. The remaining three ports in the cluster half are operationally down. After you disable Lossless Ethernet on one half of a cluster, the system will allow one of the four ports in that half to be

	operationally up in lossy mode. After you disable Lossless Ethernet on the last port in a cluster, all eight ports return to the operational state prior to Lossless Ethernet configuration. The default is disabled.
pause-type {fc|pfc}	Selects the pause frame type. pause (FC) - All unicast traffic on the port is lossless. FC is the default pause type. priority-based flow control (PFC) - All tagged unicast traffic on the port with an 802.1p value matching the value of lossless-802.1p is lossless. The switch treats traffic that does not meet this requirement as lossy traffic. The switch can drop the lossy traffic. The Lossless Ethernet feature applies to both directions on a lossless port. If the port becomes congested, the switch performs flow control based on the pause-type configuration. If traffic enters the device on a PFC-enabled port and exits the device on an FC-enabled port, only packets with the matching lossless-802.1 value are lossless. The following list identifies configuration limitations for Lossless Ethernet: If you configure a port as lossless-PFC, it does not generate nor react to FC frames. If you configure a port as lossless-FC, it does not generate nor react to PFC frames. The default is fc.
pfc-bandwidth <2-8>	Specifies the bandwidth in Gbps when the pause-type is set to pfc. The range is 2 to 8. The default is 5 Gbps.

©Avaya Inc. 2015 All Rights Reserved.

ls

Lists files in a directory.

Syntax

- `ls`
- `ls -r`
- `ls WORD<1-99>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`-r`	Recurse into directories.
`WORD<1-99>`	Specifies the directory path name.

©Avaya Inc. 2015 All Rights Reserved.

mac-flap-time-limit

Configure the interval at which MAC addresses are monitored by loop detection.

Syntax

- `default mac-flap-time-limit`
- `mac-flap-time-limit <10-5000>`

Default

`The default value is 500 milliseconds.`

Command mode

Global Configuration

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

mac-security add

Enables global MAC security to filter out (drop) packets that contains certain MAC addresses as source or destination. Configure a set of MAC addresses.

Syntax

- `mac-security add 0x00:0x00:0x00:0x00:0x00:0x00`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`0x00:0x00:0x00:0x00:0x00:0x00`	Specifies the MAC address.

©Avaya Inc. 2015 All Rights Reserved.

mac-security limit-learning enable

Limits the MAC learning for the port. This feature does not affect the forwarding of the packets. If you enable limit-learning, the FDB entry for each port is limited to the number you specify in max-addrs. If you enable the auto-learn parameter, after the maximum addresses are learned, all the new SA MAC packets are dropped. This feature provides no value if you enable unknown-mac-discard and disable auto-learn because all unknown packets are dropped. Do not enable auto-learning and limit-learning simultaneously.

Syntax

- `default mac-security limit-learning enable`
- `default mac-security limit-learning port {slot/port[-slot/port][,...]} enable`
- `default mac-security port {slot/port[-slot/port][,...]} limit-learning enable`
- `default mac-security port {slot/port[-slot/port][,...]} limit-learning port {slot/port[-slot/port][,...]} enable`
- `mac-security limit-learning enable`
- `mac-security limit-learning enable max-addrs <1-64000>`
- `mac-security port {slot/port[-slot/port][,...]} limit-learning enable`
- `mac-security port {slot/port[-slot/port][,...]} limit-learning enable max-addrs <1-64000>`
- `mac-security port {slot/port[-slot/port][,...]} limit-learning enable min-addrs <0-64000>`
- `mac-security port {slot/port[-slot/port][,...]} limit-learning enable min-addrs <0-64000> max-addrs <1-64000>`
- `mac-security port {slot/port[-slot/port][,...]} limit-learning enable snmp-trap`
- `mac-security port {slot/port[-slot/port][,...]} limit-learning enable violation-down-port`
- `no mac-security limit-learning`
- `no mac-security limit-learning enable`
- `no mac-security port {slot/port[-slot/port][,...]} limit-learning`
- `no mac-security port {slot/port[-slot/port][,...]} limit-learning enable`

Default

`The default is disabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
	Specifies the maximum number of MAC address to learn. After the maximum

max-addrs <1-64000>	value is reached, no further MAC learning occurs. The system does not drop packets; it forwards packets. The default is 1024.
min-addrs <0-64000>	Specifies the minimum number of MAC addresses to learn. MAC learning restarts after the FDB entry count reaches the value you specify in min-addrs. The default is 512.
port {slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
snmp-trap	Enables logging and Simple Network Management Protocol (SNMP) traps for violations. The default is disabled.
violation-down-port	Disables the port on violation. The default is disabled.

©Avaya Inc. 2015 All Rights Reserved.

Home | Command modes | Alphabetical listing

mac-security limit-learning max-addrs

Specifies the maximum number of MAC address to learn.

Syntax

- `default mac-security limit-learning max-addrs`
- `default mac-security limit-learning max-addrs min-addrs`
- `default mac-security limit-learning port {slot/port[-slot/port][,...]} max-addrs`
- `default mac-security limit-learning port {slot/port[-slot/port][,...]} max-addrs min-addrs`
- `default mac-security port {slot/port[-slot/port][,...]} limit-learning max-addrs`
- `default mac-security port {slot/port[-slot/port][,...]} limit-learning max-addrs min-addrs`
- `default mac-security port {slot/port[-slot/port][,...]} limit-learning port {slot/port[-slot/port][,...]} max-addrs`
- `default mac-security port {slot/port[-slot/port][,...]} limit-learning port {slot/port[-slot/port][,...]} max-addrs min-addrs`
- `mac-security limit-learning max-addrs <1-64000>`
- `mac-security port {slot/port[-slot/port][,...]} limit-learning max-addrs <1-64000>`

Default

The default is 1024.

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`max-addrs <1-64000>`	Specifies the maximum number of MAC address to learn. After the maximum value is reached, no further MAC learning occurs. The system does not drop packets; it forwards packets. The default is 1024.
`min-addrs <0-64000>`	Specifies the minimum number of MAC addresses to learn. MAC learning restarts after the FDB entry count reaches the value you specify in min-addrs. The default is 512.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

mac-security limit-learning min-addrs

Specifies the maximum number of MAC address to learn.

Syntax

- `default mac-security limit-learning min-addrs`
- `default mac-security limit-learning min-addrs max-addrs`
- `default mac-security limit-learning port {slot/port[-slot/port][,...]} min-addrs`
- `default mac-security limit-learning port {slot/port[-slot/port][,...]} min-addrs max-addrs`
- `default mac-security port {slot/port[-slot/port][,...]} limit-learning min-addrs`
- `default mac-security port {slot/port[-slot/port][,...]} limit-learning min-addrs max-addrs`
- `default mac-security port {slot/port[-slot/port][,...]} limit-learning port {slot/port[-slot/port][,...]} min-addrs`
- `default mac-security port {slot/port[-slot/port][,...]} limit-learning port {slot/port[-slot/port][,...]} min-addrs max-addrs`
- `mac-security limit-learning enable min-addrs <0-64000>`
- `mac-security limit-learning enable min-addrs <0-64000> max-addrs <1-64000>`
- `mac-security limit-learning min-addrs <0-64000>`
- `mac-security port {slot/port[-slot/port][,...]} limit-learning min-addrs <0-64000>`

Default

`The default is 512.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`max-addrs <1-64000>`	Specifies the maximum number of MAC address to learn. After the maximum value is reached, no further MAC learning occurs. The system does not drop packets; it forwards packets. The default is 1024.
`min-addrs <0-64000>`	Specifies the minimum number of MAC addresses to learn. MAC learning restarts after the FDB entry count reaches the value you specify in min-addrs. The default is 512.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

mac-security limit-learning snmp-trap

Enables logging and Simple Network Management Protocol (SNMP) traps for violations.

Syntax

- `default mac-security limit-learning port {slot/port[-slot/port][,...]} snmp-trap`
- `default mac-security limit-learning snmp-trap`
- `default mac-security port {slot/port[-slot/port][,...]} limit-learning port {slot/port[-slot/port][,...]} snmp-trap`
- `default mac-security port {slot/port[-slot/port][,...]} limit-learning snmp-trap`
- `mac-security limit-learning enable snmp-trap`
- `mac-security limit-learning snmp-trap`
- `mac-security port {slot/port[-slot/port][,...]} limit-learning snmp-trap`
- `no mac-security limit-learning snmp-trap`
- `no mac-security port {slot/port[-slot/port][,...]} limit-learning snmp-trap`

Default

`The default is disabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

mac-security limit-learning violation-down-port

Disables the port on violation.

Syntax

- `default mac-security limit-learning port {slot/port[-slot/port][,...]} violation-down-port`
- `default mac-security limit-learning violation-down-port`
- `default mac-security port {slot/port[-slot/port][,...]} limit-learning port {slot/port[-slot/port][,...]} violation-down-port`
- `default mac-security port {slot/port[-slot/port][,...]} limit-learning violation-down-port`
- `mac-security limit-learning enable violation-down-port`
- `mac-security limit-learning violation-down-port`
- `mac-security port {slot/port[-slot/port][,...]} limit-learning violation-down-port`
- `no mac-security limit-learning violation-down-port`
- `no mac-security port {slot/port[-slot/port][,...]} limit-learning violation-down-port`

Default

`The default is disabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

mac-security mac-da-filter

Add or delete a global MAC filter for MAC security.

Syntax

- `mac-security mac-da-filter [add|delete]`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`add {0x00:0x00:0x00:0x00:0x00:0x00}`	Adds a global filter. {0x00:0x00:0x00:0x00:0x00:0x00} specifies the MAC address to be added.
`delete 0x00:0x00:0x00:0x00:0x00:0x00}`	Deletes a global filter. {0x00:0x00:0x00:0x00:0x00:0x00} specifies the MAC address to be deleted.

©Avaya Inc. 2015 All Rights Reserved.

mac-security unknown-discard

Discard all the unknown MACs to limit the number of forwarding database entries learned on a port to a user-specified value.

Syntax

- `default mac-security port {slot/port[-slot/port][,...]} unknown-discard`
- `default mac-security port {slot/port[-slot/port][,...]} unknown-discard allow-mac 0x00:0x00:0x00:0x00:0x00:0x00`
- `default mac-security port {slot/port[-slot/port][,...]} unknown-discard allow-mac 0x00:0x00:0x00:0x00:0x00:0x00 auto`
- `default mac-security port {slot/port[-slot/port][,...]} unknown-discard auto-learning enable`
- `default mac-security port {slot/port[-slot/port][,...]} unknown-discard auto-learning learning-mode`
- `default mac-security port {slot/port[-slot/port][,...]} unknown-discard auto-learning lock-learning-mac`
- `default mac-security port {slot/port[-slot/port][,...]} unknown-discard auto-learning max-addrs`
- `default mac-security port {slot/port[-slot/port][,...]} unknown-discard enable`
- `default mac-security port {slot/port[-slot/port][,...]} unknown-discard violation-down-port`
- `default mac-security port {slot/port[-slot/port][,...]} unknown-discard violation-logging`
- `default mac-security port {slot/port[-slot/port][,...]} unknown-discard violation-send-authentication-trap`
- `default mac-security unknown-discard`
- `default mac-security unknown-discard allow-mac 0x00:0x00:0x00:0x00:0x00:0x00`
- `default mac-security unknown-discard allow-mac 0x00:0x00:0x00:0x00:0x00:0x00 auto`
- `default mac-security unknown-discard auto-learning enable`
- `default mac-security unknown-discard auto-learning learning-mode`
- `default mac-security unknown-discard auto-learning lock-learning-mac`
- `default mac-security unknown-discard auto-learning max-addrs`
- `default mac-security unknown-discard enable`
- `default mac-security unknown-discard violation-down-port`
- `default mac-security unknown-discard violation-logging`
- `default mac-security unknown-discard violation-send-authentication-trap`
- `mac-security port {slot/port[-slot/port][,...]} unknown-discard allow-mac`

0x00:0x00:0x00:0x00:0x00:0x00

- mac-security port {slot/port[-slot/port][,...]} unknown-discard allow-mac 0x00:0x00:0x00:0x00:0x00:0x00 auto
- mac-security port {slot/port[-slot/port][,...]} unknown-discard auto-learning enable
- mac-security port {slot/port[-slot/port][,...]} unknown-discard auto-learning learning-mode { one-shot | continuous }
- mac-security port {slot/port[-slot/port][,...]} unknown-discard auto-learning lock-learning-mac
- mac-security port {slot/port[-slot/port][,...]} unknown-discard auto-learning max-addrs <0-2048>
- mac-security port {slot/port[-slot/port][,...]} unknown-discard enable
- mac-security port {slot/port[-slot/port][,...]} unknown-discard violation-down-port
- mac-security port {slot/port[-slot/port][,...]} unknown-discard violation-logging
- mac-security port {slot/port[-slot/port][,...]} unknown-discard violation-send-authentication-trap
- mac-security unknown-discard allow-mac 0x00:0x00:0x00:0x00:0x00:0x00
- mac-security unknown-discard allow-mac 0x00:0x00:0x00:0x00:0x00:0x00 auto
- mac-security unknown-discard auto-learning enable
- mac-security unknown-discard auto-learning learning-mode { one-shot | continuous }
- mac-security unknown-discard auto-learning lock-learning-mac
- mac-security unknown-discard auto-learning max-addrs <0-2048>
- mac-security unknown-discard enable
- mac-security unknown-discard violation-down-port
- mac-security unknown-discard violation-logging
- mac-security unknown-discard violation-send-authentication-trap
- no mac-security port {slot/port[-slot/port][,...]} unknown-discard allow-mac 0x00:0x00:0x00:0x00:0x00:0x00
- no mac-security port {slot/port[-slot/port][,...]} unknown-discard allow-mac 0x00:0x00:0x00:0x00:0x00:0x00 auto
- no mac-security port {slot/port[-slot/port][,...]} unknown-discard auto-learning enable
- no mac-security port {slot/port[-slot/port][,...]} unknown-discard auto-learning learning-mode { one-shot | continuous }
- no mac-security port {slot/port[-slot/port][,...]} unknown-discard auto-learning lock-learning-mac
- no mac-security port {slot/port[-slot/port][,...]} unknown-discard enable
- no mac-security port {slot/port[-slot/port][,...]} unknown-discard violation-down-port
- no mac-security port {slot/port[-slot/port][,...]} unknown-discard violation-logging
- no mac-security port {slot/port[-slot/port][,...]} unknown-discard violation-send-authentication-trap
- no mac-security unknown-discard allow-mac 0x00:0x00:0x00:0x00:0x00:0x00
- no mac-security unknown-discard allow-mac 0x00:0x00:0x00:0x00:0x00:0x00 auto

- `no mac-security unknown-discard auto-learning enable`
- `no mac-security unknown-discard auto-learning learning-mode { one-shot | continuous }`
- `no mac-security unknown-discard auto-learning lock-learning-mac`
- `no mac-security unknown-discard enable`
- `no mac-security unknown-discard violation-down-port`
- `no mac-security unknown-discard violation-logging`
- `no mac-security unknown-discard violation-send-authentication-trap`

Default

`The default is disabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`allow-mac 0x00:0x00:0x00:0x00:0x00:0x00 [auto]`	Adds allowed MAC address of the port. 0x00:0x00:0x00:0x00:0x00:0x00 specifies the auto-learned MAC address.
`enable`	Enables unknown MAC discard of the port. The default is disabled.
`learning-mode <one-shot|continuous>`	Specifies the learning mode as one of the following: one-shot: The autolearned addresses do not age out. When the VLAN mac-addressentry is flushed, the autolearned addresses are not flushed. continuous: In continuous mode the aging of the autolearned MAC is subject to the normal aging. When the VLAN macaddress- entry is flushed, the autolearned addresses are also flushed.
`lock-learning-mac`	Saves autolearned addresses when you save the configuration file.
`max-addrs <0-2048>`	Specifies the total number of unknown MAC addresses to learn. The default is 2048.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`violation-down-port`	Configures the violation down port action of the port. The default is disabled.
`violation-logging`	Configures the violation logging action of the port. The default is enabled.
`violation-send-authentication-trap`	Configures the violation send authentication trap action of the port. The default is disabled.

©Avaya Inc. 2015 All Rights Reserved.

manual-area

Configure an Intermediate-System-to-Intermediate-System (IS-IS) manual area, 1-13 bytes in the format <xx.xxx.xxx...xxxx>. You must configure a manual area to use IS-IS. In this release, only one manual area is supported. Use the no format of this command to remove the area.

Syntax

- `manual-area xx.xxxx.xxxx...xxxx - 1...13 bytes`
- `no manual-area xx.xxxx.xxxx...xxxx - 1...13 bytes`

Default

None

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description
`xx.xxxx.xxxx...xxxx - 1...13 bytes`	Configures the manual area in a size up to 13 octets. The current release supports one area. For Intermediate-System-to-Intermediate-System (IS-IS) to operate, you must configure at least one area.

©Avaya Inc. 2015 All Rights Reserved.

manualtrigger ip rip interface

Sends a triggered update.

Syntax

- `manualtrigger ip rip interface vlan <1-4084>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<1-4084>	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

match as-path

If configured, the switch Match the as-path attribute of the Border Gateway Protocol (BGP) routes against the contents of the specified AS-lists. This command is used only for BGP routes and ignored for all other route types.

Syntax

- `default match as-path WORD<0-256>`
- `match as-path WORD<0-256>`
- `no match as-path WORD<0-256>`

Default

None

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
WORD<0-256>	Specifies the list IDs of AS-lists, separated by a comma.

©Avaya Inc. 2015 All Rights Reserved.

match community

If configured, the switch Match the community attribute of the BGP routes against the contents of the specified community lists. This command is used only for BGP routes and ignored for all other route types.

Syntax

- `default match community WORD<0-256>`
- `match community WORD<0-256>`
- `no match community WORD<0-256>`

Default

None

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
WORD<0-256>	Specifies the list IDs of up to four defined community lists, separated by a comma.

©Avaya Inc. 2015 All Rights Reserved.

match community-exact

When disabled, match community-exact results in a match when the community attribute of the BGP routes match any entry of any community-list specified in match community. When enabled, match community-exact results in a match when the community attribute of the BGP routes Match all of the entries of all the community lists specified in match community.

Syntax

- `default match community-exact`
- `default match community-exact enable`
- `match community-exact`
- `match community-exact enable`
- `no match community-exact`
- `no match community-exact enable`

Default

`The default is disable.`

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
`enable`	Enables match community-exact.

©Avaya Inc. 2015 All Rights Reserved.

match extcommunity

Match the extended community.

Syntax

- `default match extcommunity WORD<0-1027>`
- `match extcommunity WORD<0-1027>`
- `no match extcommunity WORD<0-1027>`

Default

None

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
WORD<0-1027>	Specifies the list IDs of AS-lists, separated by a comma.

©Avaya Inc. 2015 All Rights Reserved.

match interface

Match the IP address of the interface by which the RIP route was learned against the contents of the specified prefix list. This command is used only for RIP routes and ignored for all other route types.

Syntax

- `default match interface WORD<1-64>`
- `match interface WORD<1-64>`
- `no match interface WORD<1-64>`

Default

None

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
WORD<1-64>	Specifies the name of up to four defined prefix lists, separated by a comma.

©Avaya Inc. 2015 All Rights Reserved.

match local-preference

Match the preference value from 0-2147483647.

Syntax

- `default match local-preference`
- `match local-preference <0-2147483647>`

Default

The default is 0.

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
<0-2147483647>	Specifies the preference value.

©Avaya Inc. 2015 All Rights Reserved.

match metric

Match the metric of the incoming advertisement or existing route against the specified value. If 0, this field is ignored.

Syntax

- `default match metric`
- `match metric <0-65535>`

Default

`The default is 0.`

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
`<0-65535>`	Specifies the metric to match.

©Avaya Inc. 2015 All Rights Reserved.

match network

Match the destination network against the contents of the specified prefix lists.

Syntax

- `default match network WORD<1-64>`
- `match network WORD<1-64>`
- `no match network WORD<1-64>`

Default

None

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
WORD<1-64>	Specifies the name of up to four defined prefix lists, separated by a comma.

©Avaya Inc. 2015 All Rights Reserved.

match next-hop

Match the next-hop IP address of the route against the contents of the specified prefix list. This command applies only to nonlocal routes.

Syntax

- `default match next-hop WORD<1-64>`
- `match next-hop WORD<1-64>`
- `no match next-hop WORD<1-64>`

Default

None

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
WORD<1-64>	Specifies the name of up to four defined prefix lists, separated by a comma.

©Avaya Inc. 2015 All Rights Reserved.

match protocol

Match the protocol through which the route is learned.

Syntax

- `default match protocol`
- `match protocol WORD<0-60>`
- `no match protocol`
- `no match protocol WORD<0-60>`

Default

`The default is any.`

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
`WORD<0-60>`	Specifies the protocol as any|xxx, where xxx is local, OSPF, External BGP (EBGP), Internal BGP (IBGP), RIP, static, or any combination, in a string length 0 to 60.

©Avaya Inc. 2015 All Rights Reserved.

match route-source

Match the next-hop IP address for RIP routes and advertising router IDs for OSPF routes against the contents of the specified prefix list. This option is ignored for all other route types.

Syntax

- `default match route-source WORD<1-64>`
- `match route-source WORD<1-64>`
- `no match route-source WORD<1-64>`

Default

None

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
WORD<1-64>	Specifies the name of up to four defined prefix lists, separated by a comma.

©Avaya Inc. 2015 All Rights Reserved.

match route-type

Configure a specific route type to match. This command applies only to OSPF routes.

Syntax

- `default match route-type`
- `match route-type { any | local | internal | external | external-1 | external-2 }`

Default

The default is any.

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
`{ any | local | internal | external | external-1 | external-2 }`	Specifies OSPF routes of the specified type only (External-1 or External-2). Any other value is ignored.

©Avaya Inc. 2015 All Rights Reserved.

match tag

Specify a list of tags used during the match criteria process.

Syntax

- `default match tag`
- `match tag WORD<0-256>`
- `no match tag`

Default

None

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
WORD<0-256>	Specifies one or more tag values.

©Avaya Inc. 2015 All Rights Reserved.

match vrf

Configure a specific VRF to match.

Syntax

- `default match vrf WORD<1-16>`
- `match vrf WORD<1-16>`
- `no match vrf WORD<1-16>`

Default

None

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies the VRF name.

©Avaya Inc. 2015 All Rights Reserved.

match vrfids

Configure a specific VRF to match.

Syntax

- `default match vrfids WORD<0-511>`
- `match vrfids WORD<0-511>`
- `no match vrfids WORD<0-511>`

Default

None

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
WORD<0-511>	Specifies the VRF ID.

©Avaya Inc. 2015 All Rights Reserved.

max-logins

Configure the number of supported rlogin sessions.

Syntax

- `default max-logins`
- `max-logins <0-8>`

Default

`The default is 8.`

Command mode

Global Configuration

Command parameters

Parameter	Description
<0-8>	Configures the maximum number of inbound remote ACLI logon sessions.

©Avaya Inc. 2015 All Rights Reserved.

max-lsp-gen-interval

Configure the maximum level, in seconds, between generated Link State Packets (LSPs) by this Intermediate System.

Syntax

- `default max-lsp-gen-interval`
- `max-lsp-gen-interval <30-900>`
- `no max-lsp-gen-interval`

Default

`The default maximum interval value is 900.`

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description
`<30-900>`	Specifies the time interval at which the generated Link State Packet (LSP) is refreshed.

©Avaya Inc. 2015 All Rights Reserved.

md5

Calculate the Message Digest 5 algorithm (MD5) digest to verify the MD5 checksum. The md5 command calculates the MD5 digest for files on the internal or external flash and either Display the output on screen or stores the output in a file that you specify.

Syntax

- `md5 WORD<1-99>`
- `md5 WORD<1-99> -a`
- `md5 WORD<1-99> -c`
- `md5 WORD<1-99> -f WORD<1-99>`
- `md5 WORD<1-99> -r`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
-a	Adds data to the output file instead of overwriting it. You cannot use the -a option with the -c option.
-c	Compares the checksum of the specified file by WORD<1-99> with the MD5 checksum present in the checksum file name. You can specify the checksum file name using the -f option. If the checksum filename is not specified, the file /intflash/checksum.md5 is used for comparison. If the supplied checksum filename and the default file are not available on flash, the following error message appears: Error: Checksum file <filename> not present The -c option also calculates the checksum of files specified by WORD<1-99> compares the checksum with all keys in the checksum file, even if filenames do not match displays the output of comparison
-f WORD<1-99>	Stores the result of MD5 checksum to a file on internal or external flash. If the output file specified with the -f option is one of the reserved filenames on the switch, the command fails with the error message: Error: Invalid operation. If the output file specified with the -f option is one of the files for which MD5 checksum is to be computed, the command fails with the error message: VSP-9012:1# md5 *.cfg -f config.cfg Error: Invalid operation on file <filename>. If the checksum filename specified by the -f option exists on the switch (and is not one of the reserved filenames), the following message appears on the switch: File exists. Do you wish to overwrite? (y/n)
-r	Reverses the output. Use with the -f option to store the output to a file. You cannot use the -r option with the -c option.

©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

metric

Configure the metric type that you can configure on an Intermediate-System-to-Intermediate-System (IS-IS) interface.

Syntax

- `default metric`
- `metric { narrow | wide }`
- `no metric`

Default

`The default IS-IS metric type is wide.`

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description
`narrow`	Configures the metric type as narrow. Only wide is supported in this release.
`wide`	Configures the metric type as wide. Only wide is supported in this release.

©Avaya Inc. 2015 All Rights Reserved.

mirror-by-port

Use port mirroring to aid in diagnostic and security operations.

Syntax

- `default mirror-by-port <1-479> [enable] [ mode] [remote-mirror-vlan-id]`
- `default mirror-by-port mirror-port <1-479> {slot/port[-slot/port][,...]}`
- `default mirror-by-port monitor-ip <1-479> {A.B.C.D} [dscp][ttl]`
- `default mirror-by-port monitor-mlt <1-479> <1-512>`
- `default mirror-by-port monitor-port <1-479> {slot/port[-slot/port][,...]}`
- `default mirror-by-port monitor-vlan <1-479> <1-4084>`
- `mirror-by-port <1-479> [enable] [mode<both|tx|rx>] [remote-mirror-vlan-id<1-4084>]`
- `mirror-by-port <1-479> in-port {slot/port[slot/port][,...]} {monitor-ip {A.B.C.D} [dscp<0-63>][enable][mode<both|tx|rx>][ttl<2-255>] | monitor-mlt <1-512>|monitor-vlan <1-4084>|out-port {slot/port [slot/port][,...]}}`
- `no mirror-by-port <1-479> [enable]`
- `no mirror-by-port mirror-port <1-479> {slot/port[-slot/port][,...]}`
- `no mirror-by-port monitor-ip <1-479> {A.B.C.D}`
- `no mirror-by-port monitor-mlt <1-479> <1-512>`
- `no mirror-by-port monitor-port <1-479> {slot/port[-slot/port][,...]}`
- `no mirror-by-port monitor-vlan <1-479> <1-4084>`

Default

`The default DSCP is 0. The default TTL is 64.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`[in-port {slot/port [slot/port][,...]} {monitorip {A.B.C.D} [dscp <0-63>] [ <2-255>]|monitor-mlt <1-512>|monitor-vlan <1-4084>|out-port {slot/port [slot/port][,...]}}]`	Creates a new mirror-by-port table entry. in-port {slot/port [slot/port][,...]} specifies the mirrored port. monitor-ip {A.B.C.D} [dscp <0-63>] [<2-255> specifies the destination IP address for Layer 3 remote mirroring. You can optionally configure the DSCP and time-to-live values, or accept the defaults. monitor-mlt <1-512> specifies the mirroring MLT ID from 1 to 512. monitor-vlan <1-4084> specifies the mirroring VLAN ID from 1 to 4084. out-port {slot/port [slot/port][,...]} specifies the mirroring port.

<1-479>	Specifies the mirror-by-port entry ID in the range of 1 to 479.
enable	Enables or disables a mirroring instance already created in the mirror-by-port table.
mirror-port <1-479> {slot/port [slot/port][,...]}	Modifies the mirrored port. Before you can modify an existing entry, you must disable the entry: no mirror-by-port <1-479> enable.
mode <both|tx|rx>	Sets the mirroring mode. The default is rx. both mirrors both egress and ingress packets. tx mirrors egress packets. rx mirrors ingress packets.
monitor-ip <1-479> {A.B.C.D} [dscp <0-63>] [<2-255>][ttl<2-255>]	Creates a mirroring instance for Layer 3 remote mirroring. The destination must be an IP address {A.B.C.D}. The default DSCP is 0 and the default is 64. TTL sets the time-to-live value between 2 to 255 seconds.
monitor-mlt <1-479> <1-512>	Modifies the monitoring MLT; <1-479> <1-512> specifies the port mirroring entry id and the MLT ID. Before you can modify an existing entry, you must disable the entry: no mirror-by-port <1-479> enable .
monitor-port <1-479> {slot/port [slot/port][,...]}	Modifies the monitoring ports. Before you can modify an existing entry, you must disable the entry: no mirror-by-port <1-479> enable .
monitor-vlan <1-479> <1-4084>	Modifies the monitoring VLAN. Before you can modify an existing entry, you must disable the entry: no mirror-by-port <1-479> enable .
remote-mirror-vlan-id <1-4084>	Sets the remote mirror VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

mkdir

Creates a new directory.

Syntax

- `mkdir WORD<1-99>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
WORD<1-99>	Specifies the directory path name.

©Avaya Inc. 2015 All Rights Reserved.

mlt

Configure a MultiLink Trunking (MLT) to set up MLTs on the switch.

Syntax

- `mlt <1-512>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`<1-512>`	Specifies the MLT ID in the range of 1-512.
`enable`	Creates and enables a new MLT.
`encapsulation dot1q`	Sets encapsulation. dot1q enables trunking on the MLT.
`member{slot/port[-slot/port][,...]}`	Adds ports to this MLT.
`name <0-20>`	Changes the name for this MLT in the range of 0-20 characters.
`vlan <1-4084>`	Specifies a VLAN ID to add to this MLT.

©Avaya Inc. 2015 All Rights Reserved.

mlt member

Add ports to an MultiLink Trunking (MLT) link aggregation group (LAG) to add an existing VLAN to a link aggregation configuration.

Syntax

- `mlt <1-512> member {slot/port [-slot/port][,...]} vlan <1-4084>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Specifies the port and the slot number.
`<1-512>`	Specifies the MLT ID in the range of 1 to 512.
`vlan <1-4084>`	Specifies the VLAN ID in the range of 1 to 4084.

©Avaya Inc. 2015 All Rights Reserved.

monitor ip mroute stats

Display multicast routing process statistics at regular intervals. You can change the duration or interval for monitoring in Global Configuration mode.

Syntax

- `monitor ip mroute stats WORD<7-160>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
WORD<7-160>	Specifies the group IP address in the format {A.B.C.D[,E.F.G.H][,...]} . The maximum number of group IP addresses is 10. To view statistics, the group IP address is optional. To monitor statistics, the group IP address is required.

©Avaya Inc. 2015 All Rights Reserved.

monitor ip vrrp statistics

Display IP multicast statistics for the Virtual Router Redundancy Protocol (VRRP).

Syntax

- `monitor ip vrrp statistics gigabitethernet`
- `monitor ip vrrp statistics gigabitethernet {slot/port [-slot/port][,...]}`
- `monitor ip vrrp statistics gigabitethernet {slot/port [-slot/port][,...]} verbose`
- `monitor ip vrrp statistics gigabitethernet verbose`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`gigabitethernet {slot/port [-slot/port][,...]}`	Specifies the slot and port.
`verbose`	Specifies the complete list of configuration information.

©Avaya Inc. 2015 All Rights Reserved.

monitor mlt error collision

Monitor MultiLink Trunking (MLT) collision error information.

Syntax

- `monitor mlt error collision`
- `monitor mlt error collision <1-512>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
<1-512>	Specifies the MLT ID.

©Avaya Inc. 2015 All Rights Reserved.

monitor mlt error main

Monitor MultiLink Trunking (MLT) general error information.

Syntax

- `monitor mlt error main`
- `monitor mlt error main <1-512>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
<1-512>	Specifies the MLT ID.

©Avaya Inc. 2015 All Rights Reserved.

monitor mlt stats interface main

Show MultiLink Trunking (MLT) interface statistics.

Syntax

- `monitor mlt stats interface main`
- `monitor mlt stats interface main <1-512>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
<1-512>	Specifies the MLT ID.

©Avaya Inc. 2015 All Rights Reserved.

monitor mlt stats interface utilization

Show MultiLink Trunking (MLT) interface statistics utilization.

Syntax

- `monitor mlt stats interface utilization`
- `monitor mlt stats interface utilization <1-512>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
<1-512>	Specifies the MLT ID.

©Avaya Inc. 2015 All Rights Reserved.

monitor ports error

Monitor port error information.

Syntax

- `monitor ports error {slot/port[-slot/port][,...]} collision`
- `monitor ports error {slot/port[-slot/port][,...]} collision from {slot/port[-slot/port][,...]}`
- `monitor ports error {slot/port[-slot/port][,...]} main`
- `monitor ports error {slot/port[-slot/port][,...]} main from {slot/port[-slot/port][,...]}`
- `monitor ports error {slot/port[-slot/port][,...]} ospf`
- `monitor ports error {slot/port[-slot/port][,...]} ospf from {slot/port[-slot/port][,...]}`
- `monitor ports error {slot/port[-slot/port][,...]} verbose`
- `monitor ports error {slot/port[-slot/port][,...]} verbose from {slot/port[-slot/port][,...]}`
- `monitor ports error collision`
- `monitor ports error collision from {slot/port [-slot/port][,...]}`
- `monitor ports error main`
- `monitor ports error main from {slot/port [-slot/port][,...]}`
- `monitor ports error ospf`
- `monitor ports error ospf from {slot/port [-slot/port][,...]}`
- `monitor ports error verbose`
- `monitor ports error verbose from {slot/port [-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Specifies the slot and port.
`collision`	Monitors port collision error information.
`collision from {slot/port [-`	Monitors port collision error information on a particular slot

slot/port][,...]}	and port or particular slots and ports.
main	Monitors port general error information.
main from{slot/port [-slot/port][,...]}	Monitors general error information on a particular slot and port or particular slots and ports.
ospf	Monitors ports general Open Shortest Path First (OSPF) information.
ospf from{slot/port [-slot/port][,...]}	Monitors ports general OSPF information on a particular slot and port or particular slots and ports.
verbose	Monitors port extended error information.
verbose {slot/port [-slot/port][,...]}	Monitors port extended error information on a particular slot and port or particular slots and ports.

©Avaya Inc. 2015 All Rights Reserved.

monitor ports statistics bridging

Monitor port bridging statistics.

Syntax

- `monitor ports statistics {slot/port[-slot/port][,...]} bridging`
- `monitor ports statistics {slot/port[-slot/port][,...]} bridging from {slot/port[-slot/port][,...]}`
- `monitor ports statistics bridging`
- `monitor ports statistics bridging from {slot/port [-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`bridging`	Monitors port bridging statistics.
`bridging from{slot/port [-slot/port][,...]}`	Monitors port bridging statistics from a particular starting port. Identifies the slot and port in one of the following formats: a single slot and port (3/1),a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

monitor ports statistics dhcp-relay

Monitor port dhcp-relay statistics.

Syntax

- `monitor ports statistics {slot/port[-slot/port][,...]} dhcp-relay`
- `monitor ports statistics {slot/port[-slot/port][,...]} dhcp-relay from {slot/port[-slot/port][,...]}`
- `monitor ports statistics dhcp-relay`
- `monitor ports statistics dhcp-relay from {slot/port [-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`dhcp-relay`	Monitors port DHCP-relay statistics.
`dhcp-relay from{slot/port [-slot/port][,...]}`	Monitors port DHCP-relay statistics from a particular starting port. Identifies the slot and port in one of the following formats: a single slot and port (3/1),a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

monitor ports statistics interface

Monitor port interface statistics.

Syntax

- `monitor ports statistics {slot/port[-slot/port][,...]} interface main`
- `monitor ports statistics {slot/port[-slot/port][,...]} interface main from {slot/port[-slot/port][,...]}`
- `monitor ports statistics {slot/port[-slot/port][,...]} interface utilization`
- `monitor ports statistics {slot/port[-slot/port][,...]} interface utilization from {slot/port[-`
- `monitor ports statistics {slot/port[-slot/port][,...]} interface verbose from {slot/port[-slot/port][,...]}`
- `monitor ports statistics interface main`
- `monitor ports statistics interface main from {slot/port [-slot/port][,...]}`
- `monitor ports statistics interface utilization`
- `monitor ports statistics interface utilization from {slot/port [-slot/port][,...]}`
- `monitor ports statistics interface verbose`
- `monitor ports statistics interface verbose from {slot/port [-slot/port][,...]}`
- `slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Specifies the slot and port. Identifies the slot and port in one of the following formats: a single slot and port (3/1),a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`main`	Monitors port interface statistics.
`main from {slot/port [-slot/port][,...]}`	Monitors port interface statistics from a particular starting port. Identifies the slot and port in one of the following formats: a single slot and port (3/1),a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`utilization`	Monitors port interface utilization statistics.
`utilization from{slot/port`	Monitors port interface utilization statistics from a particular starting port. Identifies the slot and port in one of the following formats: a single slot and

[-slot/port][,...]}	port (3/1),a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
verbose	Monitors port interface statistics.
verbose {slot/port [-slot/port][,...]}	Monitors port interface statistics from a particular starting port. Identifies the slot and port in one of the following formats: a single slot and port (3/1),a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

monitor ports statistics ospf main

Monitor ports statistics for open shortest path first (OSPF) performance.

Syntax

- `monitor ports statistics {slot/port[-slot/port][,...]} ospf main`
- `monitor ports statistics {slot/port[-slot/port][,...]} ospf main from {slot/port[-slot/port][,...]}`
- `monitor ports statistics {slot/port[-slot/port][,...]} ospf verbose`
- `monitor ports statistics {slot/port[-slot/port][,...]} ospf verbose from {slot/port[-slot/port][,...]}`
- `monitor ports statistics ospf main`
- `monitor ports statistics ospf main from {slot/port[-slot/port][,...]}`
- `monitor ports statistics ospf verbose`
- `monitor ports statistics ospf verbose from {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`main`	Monitors ports statistics for OSPF main command.
`main from {slot/port[-slot/port][,...]}`	Monitors ports statistics for OSPF main command from a particular port. Identifies the slot and port in one of the following formats: a single slot and port (3/1),a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`verbose`	Monitors ports statistics for OSPF verbose command.
`verbose from {slot/port[-slot/port][,...]}`	Monitors ports statistics for OSPF verbose command. Identifies the slot and port in one of the following formats: a single slot and port (3/1),a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

monitor ports statistics rmon

Monitor port remote monitoring (RMON) statistics.

Syntax

- `monitor ports statistics {slot/port[-slot/port][,...]} rmon`
- `monitor ports statistics {slot/port[-slot/port][,...]} rmon from {slot/port[-slot/port][,...]}`
- `monitor ports statistics rmon`
- `monitor ports statistics rmon from {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`rmon`	Monitors port remote monitoring statistics.
`rmon {slot/port[-slot/port][,...]}`	Monitors port remote monitoring statistics from a particular port. Identifies the slot and port in one of the following formats: a single slot and port (3/1),a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

monitor ports statistics routing

Monitor port Dynamic Host Configuration Protocol (DHCP) routing statistics.

Syntax

- `monitor ports statistics {slot/port[-slot/port][,...]} routing`
- `monitor ports statistics {slot/port[-slot/port][,...]} routing from {slot/port[-slot/port][,...]}`
- `monitor ports statistics routing`
- `monitor ports statistics routing from {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`routing`	Monitors port DHCP routing statistics.
`routing from {slot/port[-slot/port][,...]}`	Monitors port DHCP routing statistics from a particular port. Identifies the slot and port in one of the following formats: a single slot and port (3/1),a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

more

View the contents of a text file one screen at a time.

Syntax

- `more WORD<1-99>`
- `more WORD<1-99> ascii`
- `more WORD<1-99> binary`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
ascii	Specifies the file format as ASCII.
binary	Specifies the file format as binary.
WORD<1-99>	Specifies a file name in one of the following formats: a.b.c.d:<file>|x:x:x:x:x:x:x:x:<file>|/intflash/<file>|/extflash/<file>|/usb/<file>.

©Avaya Inc. 2015 All Rights Reserved.

multicast smlt-square

Enable square-SMLT globally on each of the four switches to form an SMLT aggregation group.

Syntax

- `multicast smlt-square`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`smlt-square`	Enables multicast SMLT square.

©Avaya Inc. 2015 All Rights Reserved.

multicast software-forwarding

Enables the IP multicast software forwarding feature. If you enable this feature, the system forwards the initial packets of an IP multicast data stream it receives and creates a corresponding hardware record for subsequent packets.

Syntax

- `multicast software-forwarding`

Default

`The default is disabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

mv

Moves a file or directory from one place to another.

Syntax

- `mv WORD<1-255> WORD<1-255>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
WORD<1-255>WORD<1-255>	Specifies the files and location of the files to move in one of the following formats: /intflash/<file>|/extflash/<file>|/usb/<file>. The first WORD<1-255> specifies the original name and location, and the second WORD<1-255> specifies where the filename and where the file moves.

©Avaya Inc. 2015 All Rights Reserved.

mvpn enable

Enables Layer 3 VSN IP multicast over SPBM for a specific VRF.

Syntax

- `default mvpn enable`
- `mvpn enable`
- `no mvpn enable`

Default

The default is disabled.

Command mode

VRF Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

mvpn fwd-cache-timeout <10-86400>

Configures the timeout value on the VRF.

Syntax

- `default mvpn fwd-cache-timeout`
- `mvpn fwd-cache-timeout <10-86400>`
- `no mvpn fwd-cache-timeout`

Default

`The default is 210 seconds.`

Command mode

VRF Router Configuration

Command parameters

Parameter	Description
`<10-86400>`	Specifies the timeout value. The default is 210 seconds.

©Avaya Inc. 2015 All Rights Reserved.

name

Rename a policy and changes the name field for all sequence numbers under the given policy.

Syntax

- `name WORD<1-64>`

Default

None

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
WORD<1-64>	Specifies the new name for the policy.

©Avaya Inc. 2015 All Rights Reserved.

name (for a port)

Specify the name of the port that needs to be changed and have same settings for all the ports.

Syntax

- `default name`
- `default name port {slot/port[-slot/port][,...]}`
- `name port {slot/port[-slot/port][,...]} WORD<0-42>`
- `name WORD<0-42>`
- `no name`
- `no name port {slot/port[-slot/port][,...]}`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`port {slot/port[-slot/port][,...]}`	Specifies the port number that needs to be changed.
`WORD <0-42>`	Specifies the new port name.

©Avaya Inc. 2015 All Rights Reserved.

neighbor-debug-all

Display specified debug information for BGP neighbors.

Syntax

- `default neighbor-debug-all`
- `neighbor-debug-all mask WORD<1-100>`
- `no neighbor-debug-all`

Default

`The default value is none.`

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
`mask <WORD 1-100>`	<WORD 1-100> is a list of mask choices separated by commas with no space between choices.

©Avaya Inc. 2015 All Rights Reserved.

neighbor (for OSPF)

Configure NBMA neighbors so that the interface can participate in Designated Router election. All OSPF neighbors that you manually configure are NBMA neighbors.

Syntax

- `default neighbor {A.B.C.D}`
- `neighbor {A.B.C.D} priority <0-255>`
- `no neighbor {A.B.C.D}`

Default

None

Command mode

OSPF Router Configuration

Command parameters

Parameter	Description
`<A.B.C.D>`	Identifies an OSPF area in IP address format A.B.C.D.
`priority <0-255>`	Changes the priority level of the neighbor.

©Avaya Inc. 2015 All Rights Reserved.

neighbor password

Configure a BGP peer or peer group password for Transmission Control Protocol (TCP) MD5 authentication between two peers.

Syntax

- `default neighbor password <nbr_ipaddr|peer-group-name> WORD<0-1536>`
- `neighbor password <nbr_ipaddr|peer-group-name> WORD<0-1536>`
- `no neighbor password <nbr_ipaddr|peer-group-name> WORD<0-1536>`

Default

None

Command mode

BGP Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

neighbor WORD<0-1536>

Create a peer or peer group.

Syntax

- `default neighbor WORD<0-1536>`
- `neighbor WORD<0-1536>`
- `no neighbor WORD<0-1536>`

Default

None

Command mode

BGP Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

neighbor WORD<0-1536> address-family

Enables BGP address families for IPv6 or IPv4 (BGP) and L3 VPN (MP-BGP) support.

Syntax

- `default neighbor WORD<0-1536> address-family ipv6`
- `default neighbor WORD<0-1536> address-family vpnv4`
- `neighbor WORD<0-1536> address-family ipv6`
- `neighbor WORD<0-1536> address-family vpnv4`
- `no neighbor WORD<0-1536> address-family ipv6`
- `no neighbor WORD<0-1536> address-family vpnv4`

Default

None

Command mode

BGP Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

neighbor WORD<0-1536> advertisement-interval <5-120>

Specifies the time interval (in seconds) that transpires between each transmission of an advertisement from a BGP neighbor.

Syntax

- `default neighbor WORD<0-1536> advertisement-interval`
- `neighbor WORD<0-1536> advertisement-interval <5-120>`

Default

`The default value is 5 seconds.`

Command mode

BGP Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

neighbor WORD<0-1536> default-ipv6-originate

Enables IPv6 BGP neighbor default originate.

Syntax

- `default neighbor WORD<0-1536> default-ipv6-originate`
- `neighbor WORD<0-1536> default-ipv6-originate`
- `no neighbor WORD<0-1536> default-ipv6-originate`

Default

`The default value is disable.`

Command mode

BGP Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

neighbor WORD<0-1536> default-originate

Enables the switch to send a default route advertisement to the specified neighbor. A default route does not have to be in the routing table. Do not use this command if you globally enable default-information originate.

Syntax

- `default neighbor WORD<0-1536> default-originate`
- `neighbor WORD<0-1536> default-originate`
- `no neighbor WORD<0-1536> default-originate`

Default

`The default value is disable.`

Command mode

BGP Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

neighbor WORD<0-1536> ebgp-multihop

Enables a connection to a Border Gateway Protocol (BGP) peer that is more than one hop away from the local router.

Syntax

- `default neighbor WORD<0-1536> ebgp-multihop`
- `neighbor WORD<0-1536> ebgp-multihop`
- `no neighbor WORD<0-1536> ebgp-multihop`

Default

`The default value is disable.`

Command mode

BGP Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

neighbor WORD<0-1536> enable

Enables the Border Gateway Protocol (BGP) neighbor.

Syntax

- `default neighbor WORD<0-1536> enable`
- `neighbor WORD<0-1536> enable`
- `no neighbor WORD<0-1536> enable`

Default

`The default value is disable.`

Command mode

BGP Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

neighbor WORD<0-1536> in-route-map WORD<0-256>

Applies a route policy rule to all incoming routes that are learned from, or sent to, the local BGP router peers, or peer groups. The local BGP router is the BGP router that allows or disallows routes and sets attributes in incoming or outgoing updates.

Syntax

- `default neighbor WORD<0-1536> in-route-map`
- `neighbor WORD<0-1536> in-route-map WORD<0-256>`
- `no neighbor WORD<0-1536> in-route-map`

Default

None

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
WORD<0-256>	Specifies an alphanumeric string length (0 to 256 characters) that indicates the name of the route map or policy.

©Avaya Inc. 2015 All Rights Reserved.

neighbor WORD<0-1536> ipv6-in-route-map WORD<0-256>

Creates IPv6 in route map.

Syntax

- `default neighbor WORD<0-1536> ipv6-in-route-map`
- `neighbor WORD<0-1536> ipv6-in-route-map WORD<0-256>`
- `no neighbor WORD<0-1536> ipv6-in-route-map`

Default

None

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
WORD <0-256>	Specifies the route map name.

©Avaya Inc. 2015 All Rights Reserved.

neighbor WORD<0-1536> ipv6-out-route-map WORD<0-256>

Creates IPv6 out route map.

Syntax

- `default neighbor WORD<0-1536> ipv6-out-route-map`
- `neighbor WORD<0-1536> ipv6-out-route-map WORD<0-256>`
- `no neighbor WORD<0-1536> ipv6-out-route-map`

Default

None

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
WORD <0-256>	Specifies the route map or policy name in an alphanumeric string.

©Avaya Inc. 2015 All Rights Reserved.

neighbor WORD<0-1536> max-prefix <0-2147483647>

Sets a limit on the number of routes that can be accepted from a neighbor.

Syntax

- `default neighbor WORD<0-1536> max-prefix`
- `neighbor WORD<0-1536> max-prefix <0-2147483647>`

Default

`The default value is 12000 routes.`

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
<0-2147483647>	Sets a limit on the number of routes that can be accepted from a neighbor. A value of 0 (zero) indicates that there is no limit to the number of routes that can be accepted.

©Avaya Inc. 2015 All Rights Reserved.

neighbor WORD<0-1536> MD5-authentication enable

Enables TCP MD5 authentication between two peers.

Syntax

- `default neighbor WORD<0-1536> MD5-authentication enable`
- `neighbor WORD<0-1536> MD5-authentication enable`
- `no neighbor WORD<0-1536> MD5-authentication enable`

Default

`The default value is disable.`

Command mode

BGP Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

Home | Command modes | Alphabetical listing

neighbor WORD<0-1536> neighbor-debug-mask WORD<1-100>

Displays specified debug information for a BGP peer.

Syntax

- `default neighbor WORD<0-1536> neighbor-debug-mask`
- `neighbor WORD<0-1536> neighbor-debug-mask WORD<1-100>`
- `no neighbor WORD<0-1536> neighbor-debug-mask`

Default

`The default value is none.`

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
WORD<1-100>	WORD<1-100> is a list of mask choices separated by commas with no space between choices. For example, {<mask>,<mask>,<mask>...}. Mask choices are none - disables all debug messages. all - enables all debug messages. error -enables display of debug error messages. packet - enables display of debug packet messages. event - enables display of debug event messages. trace - enables display of debug trace messages. warning - enables display of debug warning messages. state - enables display of debug state transition messages. init - enables display of debug initialization messages. filter - enables display of debug messages related to filtering. update - enables display of debug messages related to sending and receiving updates.

©Avaya Inc. 2015 All Rights Reserved.

neighbor WORD<0-1536> next-hop-self

When enabled, specifies that the next-hop attribute in an IBGP update is the address of the local router or the router that is generating the IBGP update. You can only configure the next-hop parameter if the neighbor is disabled.

Syntax

- `default neighbor WORD<0-1536> next-hop-self`
- `neighbor WORD<0-1536> next-hop-self`
- `no neighbor WORD<0-1536> next-hop-self`

Default

`The default value is disable.`

Command mode

BGP Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

neighbor WORD<0-1536> out-route-map WORD<0-256>

Applies a route policy rule to all outgoing routes that are learned from, or sent to, the local peers or peer groups, of the BGP router. The local BGP router is the BGP router that allows or disallows routes, and sets attributes in incoming or outgoing updates.

Syntax

- `default neighbor WORD<0-1536> out-route-map`
- `neighbor WORD<0-1536> out-route-map WORD<0-256>`
- `no neighbor WORD<0-1536> out-route-map`

Default

None

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
WORD<0-256>	WORD<0-256> name is an alphanumeric string length (0 to 256 characters) that indicates the name of the route map or policy.

©Avaya Inc. 2015 All Rights Reserved.

neighbor WORD<0-1536> peer-group WORD<0-1536>

Adds a Border Gateway Protocol (BGP) peer to the specified subscriber group. You must create the specified subscriber group before you issue this command.

Syntax

- `neighbor WORD<0-1536> peer-group WORD<0-1536>`
- `no neighbor WORD<0-1536> peer-group`

Default

None

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
WORD<0-1536>	Specifies the subscriber group. You must create the specified subscriber group before you issue this command.

©Avaya Inc. 2015 All Rights Reserved.

neighbor WORD<0-1536> remote-as WORD<0-11>

Configures the remote AS number of a Border Gateway Protocol (BGP) peer or a peer-group. You cannot configure this option when the admin-state is enable.

Syntax

- `default neighbor WORD<0-1536> remote-as`
- `neighbor WORD<0-1536> remote-as WORD<0-11>`
- `no neighbor WORD<0-1536> remote-as`

Default

None

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
WORD<0-11>	Specifies the remote AS number of a peer or a peer-group.

©Avaya Inc. 2015 All Rights Reserved.

neighbor WORD<0-1536> remove-private-as enable

When enabled, strips private AS numbers when an update is sent. This feature is especially useful within a confederation.

Syntax

- `default neighbor WORD<0-1536> remove-private-as enable`
- `neighbor WORD<0-1536> remove-private-as enable`
- `no neighbor WORD<0-1536> remove-private-as enable`

Default

`The default value is enable.`

Command mode

BGP Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

neighbor WORD<0-1536> retry-interval <1-65535>

Configures the time interval (in seconds) for the ConnectRetry Timer.

Syntax

- `default neighbor WORD<0-1536> retry-interval`
- `neighbor WORD<0-1536> retry-interval <1-65535>`

Default

`The default value is 120 seconds.`

Command mode

BGP Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

neighbor WORD<0-1536> route-reflector-client

Configures the specified neighbor or group of neighbors as its route reflector client. All neighbors that are configured become members of the client group and the remaining IBGP peers become members of the nonclient group for the local route reflector.

Syntax

- `neighbor WORD<0-1536> route-reflector-client`
- `no neighbor WORD<0-1536> route-reflector-client`

Default

`The default value is disable.`

Command mode

BGP Router Configuration

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

neighbor WORD<0-1536> route-refresh

Enables IP VPN Route Refresh for the Border Gateway Protocol (BGP) peer. If enabled, a route refresh request received by a BGP speaker causes the speaker to resend all route updates it contains in its database that are eligible for the peer that issues the request.

Syntax

- `default neighbor WORD<0-1536> route-refresh`
- `neighbor WORD<0-1536> route-refresh`
- `no neighbor WORD<0-1536> route-refresh`

Default

`The default value is disable.`

Command mode

BGP Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

neighbor WORD<0-1536> send-community

Enables the switch to send the update message community attribute to the specified peer.

Syntax

- `default neighbor WORD<0-1536> send-community`
- `neighbor WORD<0-1536> send-community`
- `no neighbor WORD<0-1536> send-community`

Default

`The default value is disable.`

Command mode

BGP Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

neighbor WORD<0-1536> soft-reconfiguration-in enable

When enabled, the router relearns routes from the specified neighbor or group of neighbors without resetting the connection when the policy changes in the inbound direction.

Syntax

- `default neighbor WORD<0-1536> soft-reconfiguration-in enable`
- `neighbor WORD<0-1536> soft-reconfiguration-in enable`
- `no neighbor WORD<0-1536> soft-reconfiguration-in enable`

Default

`The default value is disable.`

Command mode

BGP Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

neighbor WORD<0-1536> timers

Configures timers (in seconds) for the Border Gateway Protocol (BGP) speaker for this peer.

Syntax

- `default neighbor WORD<0-1536> timers`
- `neighbor WORD<0-1536> timers <0-21845> <0-65535>`

Default

None

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
<0-65535>	<0-65535> is the hold time. The default is 30.
<0-21845>	<0-21845> is the keepalive time. The default is 10.

©Avaya Inc. 2015 All Rights Reserved.

neighbor WORD<0-1536> update-source

Specifies the source IP address when Border Gateway Protocol (BGP) packets are sent to this peer or peer group. You cannot configure this parameter when the admin-state is enable.

Syntax

- `default neighbor WORD<0-1536> update-source`
- `neighbor WORD<0-1536> update-source WORD<1-256>`
- `no neighbor WORD<0-1536> update-source`

Default

None

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
<A.B.C.D>	<A.B.C.D> is the specified source IP address.

©Avaya Inc. 2015 All Rights Reserved.

neighbor WORD<0-1536> weight

Specifies the weight of a Border Gateway Protocol (BGP) peer or peer groups, or the priority of updates that can be received from that BGP peer.

Syntax

- `default neighbor WORD<0-1536> weight`
- `neighbor WORD<0-1536> weight <0-65535>`
- `no neighbor WORD<0-1536> weight`

Default

`The default value is 0.`

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
<0-65535>	Specifies the weight of a BGP peer or peer groups, or the priority of updates that can be received from that BGP peer. If you have particular neighbors that you want to prefer for most of your traffic, you can assign a higher weight to all routes learned from that neighbor.

©Avaya Inc. 2015 All Rights Reserved.

network (for BGP)

Specify the Interior Gateway Protocol (IGP) network prefixes for Border Gateway Protocol (BGP) to advertise for redistribution.

Syntax

- `default network WORD<1-256>`
- `network WORD<1-256>`
- `network WORD<1-256> metric <0-65535>`
- `no network WORD<1-256>`

Default

None

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
`metric <0-65535>`	metric <0-65535> corresponds to the multiexit discriminator (MED) BGP attribute for the route.
`WORD <1-256>`	Specifies IGP network prefixes for Border Gateway Protocol (BGP) to advertise for redistribution. This command imports routes into BGP. WORD <1-256> is the IPv4 or the IPv6 network address and mask.

©Avaya Inc. 2015 All Rights Reserved.

network (for OSPF)

Enable OSPF on a network.

Syntax

- `default network {A.B.C.D}`
- `network {A.B.C.D}`
- `network {A.B.C.D} area {A.B.C.D}`

Default

None

Command mode

OSPF Router Configuration

Command parameters

Parameter	Description
`{A.B.C.D}`	Specifies the IP address of the network.
`area {A.B.C.D}`	Specifies the OSPF area.

©Avaya Inc. 2015 All Rights Reserved.

network (for RIP)

Enable RIP on a network.

Syntax

- `network {A.B.C.D}`
- `no network {A.B.C.D}`

Default

None

Command mode

RIP Router Configuration

Command parameters

Parameter	Description
{A.B.C.D}	Specifies the IP address of the network.

©Avaya Inc. 2015 All Rights Reserved.

nlb-mode

Configure the NLB support on an IP interface to enable or disable the Network Load Balancer (NLB) support.

Syntax

- `default nlb-mode`
- `nlb-mode igmp-mcast`
- `nlb-mode multicast`
- `nlb-mode unicast`
- `no nlb-mode`

Default

None

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

no-med-path-is-worst

Enable Border Gateway Protocol (BGP) to treat an update without a multiexit discriminator (MED) attribute as the worst path.

Syntax

- `default no-med-path-is-worst`
- `default no-med-path-is-worst enable`
- `no no-med-path-is-worst`
- `no no-med-path-is-worst enable`
- `no-med-path-is-worst enable`

Default

`The default value is enable.`

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
`enable`	Enables Border Gateway Protocol (BGP) to treat an update without a multiexit discriminator (MED) attribute as the worst path.

©Avaya Inc. 2015 All Rights Reserved.

ntp

Enable Network Time Protocol (NTP) globally and create an authentication key.

Syntax

- `default ntp [authentication-key <1-2147483647>]`
- `default ntp [interval]`
- `no ntp [authentication-key <1-2147483647>]`
- `ntp [authentication-key <1-2147483647> WORD<0-8>]`
- `ntp [interval <10-1440>]`

Default

`The default configuration removes the secret key.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`authentication-key<1-2147483647> WORD<0-8>`	Creates an authentication key for Message Digest 5 (MD5) authentication. WORD<0-8> specifies the secret key.
`interval <10-1440>`	Specifies the time interval, in minutes, between successive Network Time Protocol (NTP) updates. The default value is 15. If NTP is already activated, this configuration does not take effect until you disable NTP, and then re-enable it.

©Avaya Inc. 2015 All Rights Reserved.

ntp server

Add an IP address for a Network Time Protocol (NTP) server or modify existing NTP server parameters. You can configure a maximum of 10 time servers.

Syntax

- `default ntp server {A.B.C.D} [auth-enable] [authentication-key]`
- `default ntp server {A.B.C.D} [enable]`
- `no ntp server {A.B.C.D} [auth-enable]`
- `no ntp server {A.B.C.D} [enable]`
- `ntp server {A.B.C.D} [auth-enable] [authentication-key <0-2147483647>]`
- `ntp server {A.B.C.D} [enable]`

Default

`The default configuration does not use MD5 authentication.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`{A.B.C.D}`	Specifies the IP address of the Network Time Protocol (NTP) server to add or modify.
`auth-enable`	Activates MD5 authentication on this Network Time Protocol (NTP) server.
`authentication-key <0-2147483647>`	Specifies the key ID value used to generate the MD5 digest for the Network Time Protocol (NTP) server. The default authentication key is 0, which indicates disabled authentication.
`enable`	Activates the Network Time Protocol (NTP) server.

©Avaya Inc. 2015 All Rights Reserved.

overload

Configure the overload condition. If the overload bit parameter is configured, the Avaya Virtual Services Platform 9000 sets the overload bit in the Link State Packet (LSP). The setting affects Level 1 LSPs. The overload parameter works in conjunction with the overload-on-startup parameter. When the overload-on-startup timer expires, the Shortest Path Bridging MAC (SPBM) node clears the overload bit and re-advertises its LSP. When an LSP with an overload bit is received, the Avaya Virtual Services Platform 9000 ignores the LSP in its SPF calculation. By default, overload is set to false. If overload is set to true, the Avaya Virtual Services Platform 9000 cannot be a transit node, but it can still receive traffic destined to the VSP 9000.

Syntax

- `default overload`
- `no overload`
- `overload`

Default

`The default is false.`

Command mode

IS-IS Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

overload-on-startup

Configure the Intermediate-System-to-Intermediate-System (IS-IS) overload-on-startup value in seconds.

Syntax

- `default overload-on-startup`
- `no overload-on-startup`
- `overload-on-startup <15-3600>`

Default

`The default overload-on-startup value is 20 seconds.`

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description
<15-3600>	Specifies the Intermediate-System-to-Intermediate-System (IS-IS) overload-on-startup value in seconds. The overload-on-startup value is used as a timer to control when to send out Link State Packets (LSPs) with the overload bit cleared after IS-IS startup.

©Avaya Inc. 2015 All Rights Reserved.

password

Configure password options.

Syntax

- `default password [access-level]`
- `default password [aging-time] [default-lockout-time][min-passwd-len] [password-history]`
- `default password [lockout WORD<0-46> [time]]`
- `no password {access-level WORD<2-8>|lockout WORD<0-46>}`
- `password [access-level WORD<2-8>] [aging-time day <1-365>] [default-lockout-time <60-65000>][min-passwd-len <10-20>] [password-history <3-32>]`
- `password lockout WORD<0-46> [time <60-65000>]`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`access level WORD<2-8>`	Permits or blocks this access level. The available access level values are as follows:l1 l2 l3 ro rw rwa. The default access level is allow all.
`aging-time day <1-365>`	Configures the expiration period for passwords in days, from 1-365. The default aging time is 90 days.
`default-lockout-time <60-65000>`	Changes the default lockout time after three invalid attempts. Configures the lockout time, in seconds, and is in the 60-65000 range. The default lockout time is 60 seconds.
`lockout WORD<0-46> time <60-65000>`	Configures the host lockout time. WORD<0-46> is the host IP address in the format a.b.c.d. <60-65000> is the lockout-out time, in seconds, in the 60-65000 range.
`min-passwd-len <10-20>`	Configures the minimum length for passwords in high-secure mode. The default minimum password length is 10 characters.
`password-history <3-32>`	Specifies the number of previous passwords the switch stores. You cannot reuse a password that is stored in the password history. The default password history is 3.

©Avaya Inc. 2015 All Rights Reserved.

password access-level

Enable ACLI access levels to control the configuration actions of various users

Syntax

- `default password [aging-time] [default-lockout-time] [min-passwd-len] [password-history]`
- `default password access-level`
- `no password access-level WORD<2-8>`
- `password access-level WORD<2-8> [aging-time day <1-365>] [default-lockout-time <60-65000>] [min-passwd-len <10-20>] [password-history <3-32>]`

Default

`By default, all access levels are permitted.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`aging-time day <1-365>`	Configures the expiration period for passwords in days, from 1-365.
`default-lockout-time <60-65000>`	Changes the default lockout time after three invalid attempts. Configures the lockout time, in seconds, and is in the 60-65000 range.
`min-passwd-len <10-20>`	Configures the minimum length for passwords in high-secure mode.
`password-history <3-32>`	Specifies the number of previous passwords the switch stores. You cannot reuse a password that is stored in the password history.
`WORD<2-8>`	Permits or blocks this access level. The available access levels are: l1 l2 l3 ro rw rwa.

©Avaya Inc. 2015 All Rights Reserved.

password aging-time

Configure the duration of your password for when it expires.

Syntax

- `password aging-time day <1-365>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`access level WORD<2-8>`	Allows or blocks this access level.
`aging-time day <1-365>`	Specifies the number of days that the password is enabled.
`default-lockout-time <60-65000>`	Changes the default lockout time after three invalid attempts. secs is the lockout time in seconds and is in the range of 60 to 6500. The default is 60 seconds.
`lockout {A.B.C.D| ipv6addr} [time <60-65000>]`	Sets the host lockout time. A.B.C.D is the host IP address. ipv6addr is the IP address for ipv6 address. time is the lockout-out time in seconds for passwords lockout in the range of 60 to 65000. The default is 60 seconds.
`min-passwd-len <10-20>`	Sets the minimum length for passwords in high-secure mode. The range is from a minimum of 10 to 20.
`password-history <3-32>`	Specifies the number of previous passwords to remember. Password-history has a configurable range of 3 to 32. The default is 3.

©Avaya Inc. 2015 All Rights Reserved.

passwordprompt

Change the password prompt for ACLI sessions.

Syntax

- `default passwordprompt`
- `no passwordprompt`
- `passwordprompt WORD<1-1510>`

Default

`The default is Password.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`WORD <1-1510>`	Changes the ACLI password prompt. WORD <1-1510> is an ASCII string from 1-1510 characters.

©Avaya Inc. 2015 All Rights Reserved.

pcap capture-filter

Use capture filters to better define the match criteria used on packets. Avaya highly recommends using Packet Capture tool (PCAP) with IP or MAC filters to reduce the load on the PCAP engine. Note: If a PCAP dump is in progress on the standby, you will encounter the following error if you try to make a PCAP configuration change: Error: PCAP dump in progress. Command not allowed.

Syntax

- `default pcap capture-filter <1-1000> action`
- `default pcap capture-filter <1-1000> dscp`
- `default pcap capture-filter <1-1000> dstip`
- `default pcap capture-filter <1-1000> dstmac`
- `default pcap capture-filter <1-1000> enable`
- `default pcap capture-filter <1-1000> ether-type`
- `default pcap capture-filter <1-1000> packet-count`
- `default pcap capture-filter <1-1000> pbits`
- `default pcap capture-filter <1-1000> protocol-type`
- `default pcap capture-filter <1-1000> refresh-timer`
- `default pcap capture-filter <1-1000> srcip`
- `default pcap capture-filter <1-1000> srcmac`
- `default pcap capture-filter <1-1000> tcp-port`
- `default pcap capture-filter <1-1000> timer`
- `default pcap capture-filter <1-1000> udp-port`
- `default pcap capture-filter <1-1000> user-defined`
- `default pcap capture-filter <1-1000> vid`
- `no pcap capture-filter <1-1000>`
- `no pcap capture-filter <1-1000> dscp <0-63>`
- `no pcap capture-filter <1-1000> dscp <0-63> <0-63>`
- `no pcap capture-filter <1-1000> dscp <0-63> match-zero`
- `no pcap capture-filter <1-1000> dstip {A.B.C.D}`
- `no pcap capture-filter <1-1000> dstip {A.B.C.D} {A.B.C.D}`
- `no pcap capture-filter <1-1000> dstmac 0x00:0x00:0x00:0x00:0x00:0x00`

- no pcap capture-filter <1-1000> dstmac 0x00:0x00:0x00:0x00:0x00:0x00 <1-6>
- no pcap capture-filter <1-1000> enable
- no pcap capture-filter <1-1000> ether-type <0x0-0xffff>
- no pcap capture-filter <1-1000> ether-type <0x0-0xffff> <0x0-0xffff>
- no pcap capture-filter <1-1000> pbits <0-7>
- no pcap capture-filter <1-1000> pbits <0-7> <0-7>
- no pcap capture-filter <1-1000> pbits <0-7> match-zero
- no pcap capture-filter <1-1000> protocol-type <0-255>
- no pcap capture-filter <1-1000> srcip {A.B.C.D}
- no pcap capture-filter <1-1000> srcip {A.B.C.D} {A.B.C.D}
- no pcap capture-filter <1-1000> srcmac 0x00:0x00:0x00:0x00:0x00:0x00
- no pcap capture-filter <1-1000> srcmac 0x00:0x00:0x00:0x00:0x00:0x00 <1-6>
- no pcap capture-filter <1-1000> tcp-port <0-65535>
- no pcap capture-filter <1-1000> tcp-port <0-65535> <0-65535>
- no pcap capture-filter <1-1000> udp-port <0-65535>
- no pcap capture-filter <1-1000> udp-port <0-65535> <0-65535>
- no pcap capture-filter <1-1000> user-defined <0-9600> WORD<0-50>
- no pcap capture-filter <1-1000> vid <1-4084>
- no pcap capture-filter <1-1000> vid <1-4084> <1-4084>
- pcap capture-filter <1-1000>
- pcap capture-filter <1-1000> action capture
- pcap capture-filter <1-1000> action drop
- pcap capture-filter <1-1000> action trigger-off
- pcap capture-filter <1-1000> action trigger-on
- pcap capture-filter <1-1000> dscp <0-63>
- pcap capture-filter <1-1000> dscp <0-63> <0-63>
- pcap capture-filter <1-1000> dscp <0-63> match-zero
- pcap capture-filter <1-1000> dstip {A.B.C.D}
- pcap capture-filter <1-1000> dstip {A.B.C.D} {A.B.C.D}
- pcap capture-filter <1-1000> dstmac 0x00:0x00:0x00:0x00:0x00:0x00
- pcap capture-filter <1-1000> dstmac 0x00:0x00:0x00:0x00:0x00:0x00 <1-6>
- pcap capture-filter <1-1000> enable
- pcap capture-filter <1-1000> ether-type <0x0-0xffff>
- pcap capture-filter <1-1000> ether-type <0x0-0xffff> <0x0-0xffff>
- pcap capture-filter <1-1000> packet-count <0-65535>

- pcap capture-filter <1-1000> pbits <0-7>
- pcap capture-filter <1-1000> pbits <0-7> <0-7>
- pcap capture-filter <1-1000> pbits <0-7> match-zero
- pcap capture-filter <1-1000> protocol-type <0-255>
- pcap capture-filter <1-1000> refresh-timer WORD<1-7>
- pcap capture-filter <1-1000> srcip {A.B.C.D} {A.B.C.D} capture-filter <1-1000> srcip {A.B.C.D}
- pcap capture-filter <1-1000> srcmac 0x00:0x00:0x00:0x00:0x00:0x00
- pcap capture-filter <1-1000> srcmac 0x00:0x00:0x00:0x00:0x00:0x00 <1-6>
- pcap capture-filter <1-1000> tcp-port <0-65535>
- pcap capture-filter <1-1000> tcp-port <0-65535> <0-65535>
- pcap capture-filter <1-1000> timer WORD<1-7>
- pcap capture-filter <1-1000> udp-port <0-65535>
- pcap capture-filter <1-1000> udp-port <0-65535> <0-65535>
- pcap capture-filter <1-1000> user-defined <0-9600> WORD<1-50>
- pcap capture-filter <1-1000> vid <1-4084>
- pcap capture-filter <1-1000> vid <1-4084> <1-4084>
- pcap capture-filter <1-1000>

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
action <capture|drop|trigger-on|trigger-off>	Determines the action taken by the filter. capture indicates that the packet is captured. drop indicates that the packet is dropped. trigger-on indicates to start capturing the packet when a packet matches this filter. PCAP is enabled globally and the trigger filter is disabled. trigger-off indicates to stop capturing the packet when a packet matches this filter. PCAP is disabled globally and the trigger filter is disabled.
dscp <0-63> [<0-63>] [match-zero]	Specifies the DSCP value of the packet. <0-63> is the DSCP from 0 to 63. The default is 0, which means this option is disabled. Use the second <0-63> to specify a range. When match-zero is set, 0 is considered a valid value. When it is not set, 0 is considered a disable value.
dstip <A.B.C.D> [<A.B.C.D>]	Specifies the destination IP address. The default is 0.0.0.0, which means this option is disabled. Use the second <A.B.C.D> to specify a range.
dstmac <0x00:0x00:0x00:0x00:0x00:0x00> [<1-6>]	Specifies the MAC address of the destination. If the mask is set, then only the first few bytes are compared. <1-6> is the destination MAC address mask, and specifies a range.

enable	Enables the filter. The default is disable.
ether-type <0x0-0xffff> [<0x0-0xffff>]	Specifies the Ethernet type of the packet. The default is 0, meaning that this option is disabled. Use the second <0x0-0xffff> to specify a range.
packet-count <0-65535>	When set, The Packet Capture tool (PCAP) stops after capturing the specified number of packets. This is similar to the refresh-timer option; after it is invoked, the filter is disabled. This option is active only when the action parameter is set to trigger-on. The default value is 0, which means this option is disabled.
pbits <0-7> <0-7>[match-zero]	Specifies the priority bit of the packet. The default is 0, which means this option is disabled. Use the second <0-7> to specify a range. When match-zero is set, 0 is considered a valid value. When it is not set, 0 is considered a disable value.
protocol-type <0-255> [<0-255>]	Specifies the packet protocol type. The default is 0, which means this option is disabled. Use the second <0-255> to specify a range.
refresh-timer <WORD 1-7>	When set, this starts or resets a timer. If another packet is not received within the specified time, the Packet Capture tool (PCAP) is disabled globally. This option is active only when the action parameter is set to 'trigger-on'. To delete this option, set it to 0. The default value is 0.
srcip <A.B.C.D> [<A.B.C.D>]	Specifies the source IP address. The default is 0.0.0.0, which means this option is disabled. Use the second <A.B.C.D> to specify a range.
srcmac <0x00:0x00:0x00:0x00:0x00:0x00> [<1-6>]	Specifies the MAC address of the source. If the mask is set, then only the first few bytes are compared. The default is 00:00:00:00:00:00, which means this option is disabled. <1-6> is the mask of the source MAC address. This parameter specifies an address range.
tcp-port <0-65535> [<0-65535>]	Specifies the TCP port of the packet. The default is 0, which means this option is disabled. Use the second <0-65535> to specify a range.
timer <WORD 1-7>	When set, Packet Capture (PCAP) is invoked when the first packet is matched and stopped after the set value of time. After starting the timer, the filter is disabled. This option is active only when the action parameter is set to trigger-on. <WORD 1-7> is a value from 100 to 3600000 milliseconds. The default value is zero. Setting the value to 0 disables the timer.
udp-port <0-65535> [<0-65535>]	Specifies the UDP port of the packet. The default is 0, which means this option is disabled. Use the second <0-65535> to specify a range.
user-defined <0-9600> WORD <1-50>	Sets a user-defined value on which to match the packet. The user can define a pattern in hex or characters to match (<0-9600>). The user can also specify the offset to start the match (WORD <1-50>). The default value of pattern is null ('') which means that this field is discarded. To disable this option, set the pattern to null ('').
vid <1-4084> [<1-4084>]	Specifies the VLAN ID of the packet. The default is 0, which means that this option is disabled. Use the second <1-4084> to specify a range.

©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

pcap enable

Configure the Packet Capture tool (PCAP) globally to define how PCAP operates on the Virtual Services Platform 9000. Note: If a PCAP dump is in progress on the standby, you will encounter the following error if you try to make a PCAP configuration change: Error: PCAP dump in progress. Command not allowed.

Syntax

- `pcap enable`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`auto-save [file-name <WORD 1-40>| extflash| network <A.B.C.D>]`	Enables or disables auto save. When enabled, saves the captured frames into the device specified and continues to capture frames. The default is enable. If this option is disabled, packets are stored in the DRAM buffer only. file-name <WORD 1-40> is the name of the file where captured frames are saved. extflash sets the device to external flash. network sets the device to network. <A.B.C.D> is the IP address used. This is used only if the device is network.
`buffer-size <2-128>`	Specifies the size of the buffer allocated for storing data.
`buffer-wrap`	Enables buffer wrapping. When this parameter is set to true and the buffer becomes full, the capture continues by wrapping the buffer. If this parameter is set to false and the buffer becomes full, the packet capture stops. The default value is true. A log message is generated when the buffer is wrapped.
`enable`	Enables Packet Capture (PCAP) globally. The default is disabled. To disable PCAP, use the no pcap enable command.
`fragment-size <64-9600>`	Specifies the number of bytes from each frame to capture. The default is the first 64 bytes of each frame.
`reset-stat`	This command resets the Packet Capture (PCAP) engine DRAM buffer, as well as all software counters used for PCAP statistics. This command can be executed in the Primary or Secondary CPU.
`wrap-auto-save-file`	Enables wrap around auto-save-file (external flash-wrap around).

©Avaya Inc. 2015 All Rights Reserved.

pcap enable mode

Enable Packet Capture tool (PCAP) globally. Note: If a PCAP dump is in progress on the standby, you will encounter the following error if you try to make a PCAP configuration change: Error: PCAP dump in progress. Command not allowed.

Syntax

- `default pcap enable`
- `default pcap enable mode`
- `no pcap enable`
- `no pcap enable mode both`
- `no pcap enable mode rx`
- `no pcap enable mode tx`
- `pcap enable mode both`
- `pcap enable mode rx`
- `pcap enable mode tx`

Default

None

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

pcap reset-stat

Reset Packet Capture tool (PCAP) statistics and counters. Note: If a PCAP dump is in progress on the standby, you will encounter the following error if you try to make a PCAP configuration change: Error: PCAP dump in progress. Command not allowed.

Syntax

- `pcap reset-stat`

Default

None

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

peer

Access the standby CPU to make changes to the standby CPU without reconnecting to the console port on that module.

Syntax

- `peer {telnet|rlogin}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`(telnet|rlogin)`	Specifies the access method to use to connect to the standby CPU.

©Avaya Inc. 2015 All Rights Reserved.

permit

Specifies the action to take when a permit or deny policy is selected for a specific route. Permit allows the route, deny (no permit) ignores the route.

Syntax

- `default permit`
- `no permit`
- `permit`

Default

`The default is permit.`

Command mode

Route-Map Configuration

©Avaya Inc. 2015 All Rights Reserved.

ping

Ping a device to test the connection between Avaya Virtual Services Platform 9000 and another network device. After you ping a device, the switch sends an Internet Control Message Protocol (ICMP) packet to the target device. If the device receives the packet, it sends a ping reply. After the switch receives the reply, a message appears that indicates traffic can reach the specified IP address. If the switch does not receive a reply, the message indicates the address is not responding.

Syntax

- `ping WORD<0-256>`
- `ping WORD<0-256> count <1-9999>`
- `ping WORD<0-256> -d`
- `ping WORD<0-256> datasize <28-51200>`
- `ping WORD<0-256> -I <1-60>`
- `ping WORD<0-256> interface gigabitEthernet {slot/port}`
- `ping WORD<0-256> interface mgmtEthernet {slot/port}`
- `ping WORD<0-256> interface tunnel <1-2000>`
- `ping WORD<0-256> interface vlan <1-4084>`
- `ping WORD<0-256> -s`
- `ping WORD<0-256> scopeid <1-9999>`
- `ping WORD<0-256> source WORD<1-256>`
- `ping WORD<0-256> -t <1-120>`
- `ping WORD<0-256> vrf WORD<1-16>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`count <1-9999>`	Specifies the number of times to ping (for IPv4) (1-9999).
`-d`	Configures the ping debug mode. This variable detects local software failures (ping related threads creation or write to sending socket) and receiving issues (ICMP packet too short or wrong ICMP packet type).
`datasize <28-51200>`	Specifies the size of ping data sent in byte. For IPv4, the acceptable range is 28-9216. For IPv6, the acceptable range is 28-51200.

`-I <1-60>`	Specifies the interval between transmissions in seconds (1-60).
`interface gigabitEthernet {slot/port} | mgmtEthernet {slot/port} | tunnel <1-2000> | vlan <1-4084>`	Specifies a specific outgoing interface to use by IP address. Additional ping interface filters: gigabitEthernet: {slot/port} gigabit ethernet port mgmtEthernetport: {slot/port} management ethernet port tunnel: tunnel ID as a value from 1 to 2147477248 vlan: VLAN interface as a value from 1 to 4084
`-s`	Configures the continuous ping at the interval rate defined by the [-I] parameter (for IPv4).
`scopeid <1-9999>`	Specifies the scope ID. <1-9999> specifies the circuit ID for IPv6.
`source WORD <1-256>`	Specifies an IP address that will be used as the source IP address in the packet header.
`-t <1-120>`	Specifies the no-answer timeout value in seconds (1-120) for IPv4.
`vrf WORD<1-16>`	Specifies the virtual routing and forwarding (VRF) name from 1-16 characters. Specify the MgmtRouter VRF if you need to run the ping operation through the management interface.
`WORD <0-256>`	Specifies the host name or IPv4 (a.b.c.d) or IPv6 (x:x:x:x:x:x:x:x) address (string length 0-256). Specifies the address to ping.

©Avaya Inc. 2015 All Rights Reserved.

ping-virtual-address

Ping a virtual address to test the connection.

Syntax

- `default ping-virtual-address`
- `default ping-virtual-address enable`
- `default ping-virtual-address enable vrf WORD<1-16>`
- `no ping-virtual-address`
- `no ping-virtual-address enable`
- `no ping-virtual-address enable vrf WORD<1-16>`
- `ping-virtual-address`
- `ping-virtual-address enable`
- `ping-virtual-address enable vrf WORD<1-16>`

Default

None

Command mode

VRRP Router Configuration

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies the virtual routing and forwarding (VRF) name from 1-16 characters.

©Avaya Inc. 2015 All Rights Reserved.

pluggable-optical-module

Configure Digital Diagnostic Monitoring to get information concerning the status of the transmitted and received signals to allow better fault isolation and error detection. The pluggable-optical-module ddm-monitor and pluggable-optical-module ddm-alarm-portdown commands are no longer available; however, VSP 9000 continues to support old configurations that use these commands.

Syntax

- `default pluggable-optical-module ddm-monitor-interval`
- `default pluggable-optical-module ddm-traps-send`
- `no pluggable-optical-module ddm-traps-send`
- `pluggable-optical-module ddm-monitor-interval <10-40>`
- `pluggable-optical-module ddm-traps-send`
- `pluggable-optical-module reset {slot/port}`

Default

`The default is enabled.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`ddm-monitor-interval <10-40>`	Configures the digital diagnostic monitoring (DDM) monitor interval in the range of 10 to 40 in seconds. If any alarm occurs, the user gets the log message before the specific interval configured by the user. The default value is 10 seconds.
`ddm-traps-send`	Enables or disables the sending of trap messages. When enabled, the trap message is sent to the Device manager, any time the alarm occurs. The default is enable.
`reset {slot/port}`	Resets the QSFP+ transceivers.

©Avaya Inc. 2015 All Rights Reserved.

policy-vlan-precedence

Use this command to indicate whether source MAC or IP subnet VLAN classification takes precedence.

Syntax

- `default policy-vlan-precedence`
- `default policy-vlan-precedence port {slot/port[-slot/port][,...]}`
- `policy-vlan-precedence port {slot/port[-slot/port][,...]} source-mac`
- `policy-vlan-precedence port {slot/port[-slot/port][,...]} subnet`
- `policy-vlan-precedence source-mac`
- `policy-vlan-precedence subnet`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`{source-mac|subnet}`	Indicates that the source MAC-based or subnet-based VLAN classification takes precedence.
`port {slot/port [-slot/port][,...]}`	Specifies the slot and the port number.

©Avaya Inc. 2015 All Rights Reserved.

portlock enable

Enable port locking for the security of the ports from any modifications.

Syntax

- `portlock enable`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`enable`	Enables the port locking globally.

©Avaya Inc. 2015 All Rights Reserved.

prompt

Change the root level prompt or the system name for run-time mode.

Syntax

- `prompt WORD <0-255>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`WORD <0-255>`	Specifies the box level or root level prompt in the range of 0 to 255.

©Avaya Inc. 2015 All Rights Reserved.

protocol-vlan

Enable protocol-based VLAN on the port.

Syntax

- `default protocol-vlan`
- `default protocol-vlan enable`
- `default protocol-vlan port {slot/port[-slot/port][,...]}`
- `no protocol-vlan`
- `no protocol-vlan enable`
- `no protocol-vlan port {slot/port[-slot/port][,...]}`
- `protocol-vlan`
- `protocol-vlan enable`
- `protocol-vlan port {slot/port[-slot/port][,...]}`

Default

`The default is enabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables or disables protocol-based VLAN for the port.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

psnp-interval

Configure the Partial Sequence Number Packets (PSNP) interval in seconds. This command is a system level parameter that applies to Level 1 PSNP generation on all interfaces.

Syntax

- `default psnp-interval`
- `no psnp-interval`
- `psnp-interval <1-120>`

Default

`The default PSNP value is 2 seconds.`

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description
`<1-120>`	Configures the interval, in seconds. This is a system level parameter that applies for Level 1 Partial Sequence Number Packet (PSNP) generation on all interfaces. A longer interval reduces overhead, while a shorter interval speeds up convergence.

©Avaya Inc. 2015 All Rights Reserved.

pwc

Prints the current working level.

Syntax

- pwc

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

pwd

Prints the current working directory.

Syntax

- pwd

Default

None

Command mode

Privileged EXEC

©Avaya Inc. 2015 All Rights Reserved.

qos 802.1p-override

Configure a port as untrusted to determine the Layer 2 Quality of Service (QoS) actions the switch performs. An untrusted port (override enabled) overrides 802.1p bit markings.

Syntax

- `default qos 802.1p-override`
- `default qos 802.1p-override enable`
- `no qos 802.1p-override`
- `no qos 802.1p-override enable`
- `qos 802.1p-override`
- `qos 802.1p-override enable`

Default

`The default is disabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	If you configure this variable, it overrides incoming 802.1p bits; if you do not configure this variable, it honors and handles incoming 802.1p bits. The default is disable (Layer 2 trusted).

©Avaya Inc. 2015 All Rights Reserved.

qos egressmap

Modify the egress mappings to change traffic priorities. However, Avaya recommends that you use the default mappings.

Syntax

- `default qos egressmap 1p`
- `qos egressmap 1p <0-7> <0-7> ds <0-7> WORD <1-6>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<0-7>	Specifies the Quality of Service (QoS) level in the range of 0 to 7.
1p <0-7>	Maps the Quality of Service (QoS) level to IEEE 802.1p priority. Each QoS level has a default IEEE 1P value: level 0-1, level 1-0, level 2-2, level 3-3, level 4-4, level 5-5, level 6-6, and level 7-7
ds <0-7>	Maps Quality of Service (QoS) level to Differentiated Services Code Point (DSCP).
WORD<1-6>	Specifies the DiffServ code point in hexadecimal, binary, or decimal.

©Avaya Inc. 2015 All Rights Reserved.

qos if-policer

Configure a port policer to limit incoming traffic. The switch drops or remarks violating traffic.

Syntax

- `default qos if-policer`
- `default qos if-policer port {slot/port[-slot/port][,...]}`
- `no qos if-policer`
- `no qos if-policer port {slot/port[-slot/port][,...]}`
- `qos if-policer peak-rate <64-40000000> svc-rate <64-40000000>`
- `qos if-policer port {slot/port[-slot/port][,...]} peak-rate <64-40000000> svc-rate <64-40000000>`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`peak-rate <64-40000000>`	Specifies the peak rate limit in Kbps. The range is 64-40000000.
`port {slot/port [-slot/port][,...]}`	Specifies the slot and port or slot and portlist.
`svc-rate <64-40000000>`	Specifies the service rate limit in Kbps. The range is 64-40000000.

©Avaya Inc. 2015 All Rights Reserved.

qos if-shaper

Configure port-based shaping to rate-limit all outgoing traffic to a specific rate.

Syntax

- `default qos if-shaper`
- `default qos if-shaper port {slot/port}`
- `no qos if-shaper`
- `no qos if-shaper port {slot/port[-slot/port][,...]}`
- `qos if-shaper port {slot/port} shape-rate <10000-40000000>`
- `qos if-shaper shape-rate <10000-40000000>`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`port {slot/port[-slot/port][,...]}`	Specifies a list of ports.
`port {slot/port}`	Specifies the slot and port, or slot and portlist.
`shape-rate <10000-40000000>`	Configures the shaping rate from 10000-40000000 Kbps.

©Avaya Inc. 2015 All Rights Reserved.

qos ingressmap

Modify the ingress mappings to change traffic priorities. However, Avaya recommends that you use the default mappings.

Syntax

- `default qos ingressmap 1p`
- `qos ingressmap1p <0-7> <0-7> ds <0-63> <0-7>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`1p <0-7> <0-7>`	Maps the IEEE 802.1p bit to Quality of Service (QoS) level. Each QoS level has a default IEEE 1P value: level 0-1, level 1-0, level 2-2, level 3-3, level 4-4, level 5-5, level 6-6, and level 7-7.
`ds <0-63> <0-7>`	Maps the Differentiated Services Code Point (DSCP) to Quality of Service (QoS) level.

©Avaya Inc. 2015 All Rights Reserved.

qos level

Configure the default port QoS level to assign a default QoS level for all traffic (providing the packet does not match an ACL that remarks the packet).

Syntax

- `default qos level`
- `default qos level port {slot/port}`
- `qos level <0-6>`
- `qos level port {slot/port} <0-6>`

Default

`The default value is 1.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<0-6>`	Specifies the default Quality of Service (QoS) level for the port traffic. QoS level 7 is reserved for network control traffic.
`port <slot/port>`	Specifies the slot and port, or slot and port list.

©Avaya Inc. 2015 All Rights Reserved.

qos lossless-802.1p

Configure the lossless 802.1p value. The Lossless Ethernet feature for 10 GbE ports guarantees the switch does not drop certain traffic types. You can configure all unicast traffic on the port to be lossless, or you can configure all tagged unicast traffic with a specific lossless-802.1p value to be lossless. If you change the lossless-802.1p value, the change affects all priority-based flow control (PFC) configured ports. You cannot change this value for individual lossless ports. If traffic enters the device on a PFC-enabled port and exits the device on an FC-enabled port, only packets with the matching lossless-802.1p value are lossless.

Syntax

- `default qos lossless-802.1p`
- `qos lossless-802.1p <0-6>`

Default

`The default is 3.`

Command mode

Global Configuration

Command parameters

Parameter	Description
<0-6>	Specifies the lossless-802.1p value in a range from 0 to 6. The default is 3. The following list identifies configuration limitations for the lossless-802.1p value: Lossless-802.1p can be configured and the change affects all of the lossless-pfc ports in the system. The Lossless-802.1p value must be mapped to internal QoS level 3 and Avaya recommends that you do not use filters to remark the internal QoS. When you enable lossless-PFC on a port, the port does not become lossless-PFC if the lossless-802.1p value is mapped to an internal QoS level other than 3, or if the internal QoS level 3 maps to another 802.1p value. The system displays a warning message if at least one cluster is in Lossless-PFC mode, and you attempt to map a non-lossless 802.1p value to internal QoS level 3, or map the lossless 802.1p value to an internal QoS level other than 3. You cannot change the Lossless 802.1p value to match the configured port QoS value on any of the Lossless-PFC enabled ports in the system. You cannot enable Lossless-PFC on a port if the Lossless-PFC port QoS value is equal to the Lossless 802.1p value. On a Lossless-PFC enabled port, you cannot set the port QoS to a value which is the same as the Lossless 802.1p value. In a Lossless-PFC (802.1Qbb) domain, the lossless behavior is guaranteed as long as the Lossless 802.1p, ingress "1p to QoS" map, and the egress "QoS to 1p" maps are consistent. You must configure the egress "QoS to 1p" map correctly when you change the Lossless 802.1p and Ingress "QoS to 1P" maps".

©Avaya Inc. 2015 All Rights Reserved.

qos policy

Configure a Quality of Service (QoS) policy to configure peak and service policing rates for specific lane members.

Syntax

- `qos policy <1-16000> peak-rate <64-5000000> svc-rate <64-5000000> [name WORD<1-32>]`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`<1-16000>`	Specifies the policer ID number.
`name WORD<1-32>`	Names the policer template.
`peak-rate <64-5000000>`	Configures the policer peak rate in Kbps.
`svc-rate <64-5000000>`	Configures the policer service rate in Kbps.

©Avaya Inc. 2015 All Rights Reserved.

quick-start

Enable the quick-start flag for exponential backoff.

Syntax

- `default quick-start`
- `default quick-start enable`
- `no quick-start`
- `no quick-start enable`
- `quick-start enable`

Default

`The default value is enable.`

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
`enable`	Enables the quick-start flag for exponential backoff.

©Avaya Inc. 2015 All Rights Reserved.

radius

Configure D1019 to authenticate users identity through a central database.

Syntax

- radius

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
access-priority-attribute <192-240>	Specifies the value of the Access Priority attribute in the range of 192 to 240 and the default is 192.
accounting {attribute-value <192-240>|enable|include-cli-commands}	Enables Remote Dial-In User Services (RADIUS) accounting. The default is false.
auth-info-attr-value <0-255>	Specifies the value of the authentication-information attribute in the range of 0 to 255. The default is 91.
clear-stat	Clears the Remote Dial-In User Services (RADIUS) statistics.
cli-commands-attribute <192-240>	Specifies the value of the ACLI commands attribute in the range of 192 to 240 and the default is 195.
command-access-attribute <192-240>	Specifies the value of the command access attribute in the range of 192 to 240 and the default is 194.
maxserver<1-10>	Specific to Remote Dial-In User Services (RADIUS) authentication. Sets the maximum number of servers allowed for the device. The range is between 1 and 10. The default is 10.
mcast-addr-attr-value <0-255>	Specifies the value of the multicast address attribute in the range of 0 to 255. The default is 90.

©Avaya Inc. 2015 All Rights Reserved.

radius cli-cmd-count

Configure a Remote Access Dial-In User Services (RADIUS) accounting interim request to create a log whenever more than forty CLI commands are executed.

Syntax

- `radius cli-cmd-count <1-40>`

Default

`The default value is 40.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<1-40>`	Specifies a value of the ACLI command count in the range of 1 to 40.

©Avaya Inc. 2015 All Rights Reserved.

radius cli-profile

Use Remote Access Dial-In User Services (RADIUS) ACLI profiling to grant or deny ACLI command access to users being authenticated by way of the RADIUS server.

Syntax

- `radius cli-profile`

Default

`The default is disabled/false.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

radius command-access-attribute

Configure Remote Access Dial-In User Services (RADIUS) authentication and RADIUS accounting attributes to determine the size of the packets received.

Syntax

- `radius command-access-attribute <192-240>`

Default

`The default value is 192.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`command-access-attribute <192-240>`	Specifies the Remote Dial-In User Services (RADIUS) authentication attribute value is an integer value of the ACLI command count in the range of 192 to 240.

©Avaya Inc. 2015 All Rights Reserved.

radius enable

Enable or disable Remote Access Dial-In User Services (RADIUS) authentication globally on the device to allow further configuration to take place.

Syntax

- `radius enable`

Default

None

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

radius server host

Add a Remote Access Dial-In User Services (RADIUS) server to allow RADIUS service on the Virtual Services Platform 9000.

Syntax

- `default radius server host WORD<0-46> used-by cli`
- `default radius server host WORD<0-46> used-by cli [acct-enable|acct-port|enable|key|port |priority |retry |source-ip |timeout]`
- `default radius server host WORD<0-46> used-by eapol`
- `default radius server host WORD<0-46> used-by snmp`
- `default radius server host WORD<0-46> used-by web`
- `no radius server host WORD<0-46> used-by cli`
- `no radius server host WORD<0-46> used-by cli [acct-enable|acct-port|enable]`
- `no radius server host WORD<0-46> used-by eapol`
- `no radius server host WORD<0-46> used-by snmp`
- `no radius server host WORD<0-46> used-by web`
- `radius server host WORD<0-46> key WORD<0-32>`
- `radius server host WORD<0-46> key WORD<0-32> [acct-enable|acct-port<1-65536>|enable|port <1-65536>|priority <1-10>|retry <0-6>|source-ip WORD<0-46>|timeout <1-20>]`
- `radius server host WORD<0-46> key WORD<0-32> [used-by cli|used-by eapol|used-by snmp|used-by web]`
- `radius server host WORD<0-46> used-by cli`
- `radius server host WORD<0-46> used-by cli [acct-enable|acct-port <1-65536>|enable|key WORD<0-20>|port <1-65536>|priority <1-10>|retry <0-6>|source-ip WORD<0-46>|timeout <1-20>`
- `radius server host WORD<0-46> used-by eapol`
- `radius server host WORD<0-46> used-by snmp`
- `radius server host WORD<0-46> used-by web`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description

acct-enable	Enables Remote Dial-In User Services (RADIUS) accounting on this server. The default for acct-enable is enabled.
acct-port <1-65536>	Specify a UDP port of the Remote Dial-In User Services (RADIUS) accounting server. The default is 1816.
enable	Enables this server.
host WORD <0-46>	Create a host server. Remote Dial-In User Services (RADIUS) supports IPv4 and IPv6 addresses. WORD <0-46> specifies an address in A.B.C.D or x:x:x:x:x:x:x:x format.
key WORD<-32>	Specify a secret key in the range of 0-20 characters.
port <1-65536>	Specify a UDP port of the Remote Dial-In User Services (RADIUS) server.
priority <1-10>	Specify the priority value for this server. The default is 10.
retry <0-6>	Specify the maximum number of authentication retries. The default is 3.
source-ip WORD <0-46>	Specify a configured IP address as the source address when transmitting RADIUS packets. Remote Dial-In User Services (RADIUS) supports IPv4 and IPv6 addresses. WORD <0-46> specifies an address in A.B.C.D or x:x:x:x:x:x:x:x format.
timeout <1-20>	Specify the number of seconds before the authentication request times out. The default is 3.
used-by {cli|snmp|eapol|web}	Specify how the server functions: cli-configure the server for CLI authentication. snmp-configure the server for Simple Network Management Protocol (SNMP) authentication. eapol-configure the server for Extensible Authentication Protocol (EAPoL) authentication. web-configure the server for web authentication. The default for used-by is cli.

©Avaya Inc. 2015 All Rights Reserved.

radius-snmp

Enable Remote Access Dial-In User Services (RADIUS) accounting to log all of the activity of each remote user in a session on the centralized RADIUS accounting server.

Syntax

- `radius-snmp abort-session-timer <30-65535>`
- `radius-snmp acct-enable`
- `radius-snmp re-auth-timer <30-65535>`
- `radius-snmp user WORD<0-20>`

Default

`The default value is disabled.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`abort-session-timer <30-65535>`	Specifies the timer to be used for sending a stop accounting message for this particular Simple Network Management Protocol (SNMP) session. The timer value ranges from 30 to 65535. This default is 180.
`acct-enable`	Enables Remote Dial-In User Services (RADIUS) accounting globally. RADIUS accounting cannot be enabled unless a valid server is configured. This feature is disabled by default.
`re-auth-timer <30-65535>`	Timer to be sent for re-authentication the Simple Network Management Protocol (SNMP) session. The timer value ranges from 30 to 65535. The default is 180.
`user WORD<0-20>`	Specifies the username for the Simple Network Management Protocol (SNMP) access. WORD<0-20> specifies the username in a range of 0 to 20 characters. The default is snmp_user.

©Avaya Inc. 2015 All Rights Reserved.

radius sourceip-flag

Configure the source IP address if the outgoing interface on the Virtual Services Platform 9000 fails so that configuration changes be made to define the new Remote Access Dial-In User Services (RADIUS) Client on the RADIUS Server.

Syntax

- `radius sourceip-flag`

Default

`The default is disabled/false.`

Command mode

Global Configuration

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

rate-limit

Configure broadcast and multicast bandwidth limiting to limit the amount of ingress broadcast and multicast traffic on a port. The switch drops traffic that violates the bandwidth limit.

Syntax

- `default rate-limit broadcast`
- `default rate-limit multicast`
- `default rate-limit port {slot/port[-slot/port][,...]} broadcast`
- `default rate-limit port {slot/port[-slot/port][,...]} multicast`
- `no rate-limit broadcast`
- `no rate-limit multicast`
- `no rate-limit port {slot/port[-slot/port][,...]} broadcast`
- `no rate-limit port {slot/port[-slot/port][,...]} multicast`
- `rate-limit broadcast <1-65535>`
- `rate-limit multicast <1-65535>`
- `rate-limit port {slot/port[-slot/port][,...]} broadcast <1-65535>`
- `rate-limit port {slot/port[-slot/port][,...]} multicast <1-65535>`

Default

`The default is disabled (no rate limit).`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<1-65535>`	Specifies the bandwidth limit for broadcast and multicast traffic from 1-65535 packets per second.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

redistribute bgp (for IS-IS)

Control the redistribution of routes from the global router into the Shortest Path Bridging MAC (SPBM) Intermediate-System-to-Intermediate-System (IS-IS) domain.

Syntax

- `default redistribute bgp enable`
- `default redistribute bgp metric`
- `default redistribute bgp metric-type`
- `default redistribute bgp route-map`
- `default redistribute bgp subnets`
- `no redistribute bgp`
- `no redistribute bgp enable`
- `no redistribute bgp metric`
- `no redistribute bgp metric-type`
- `no redistribute bgp route-map`
- `no redistribute bgp subnets`
- `redistribute bgp`
- `redistribute bgp enable`
- `redistribute bgp metric <0-65535>`
- `redistribute bgp metric-type external`
- `redistribute bgp metric-type internal`
- `redistribute bgp route-map WORD<0-64>`
- `redistribute bgp subnets allow`
- `redistribute bgp subnets suppress`

Default

By default, route redistribution is disabled.

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description

enable	Enables the redistribution of the specified protocol into the Shortest Path Bridging MAC (SPBM) network.
metric <0-65535>	Configures the metric (cost) to apply to redistributed routes. The default is 1.
metric-type external	Configures the type of route to import into the protocol. The default is internal.
metric-type internal	Configures the type of route to import into the protocol. The default is internal.
route-map WORD<0-64>	Configures the route policy to apply to redistributed routes.
subnets allow	Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.
subnets suppress	Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.

©Avaya Inc. 2015 All Rights Reserved.

redistribute direct (for BGP)

Redistribute routes learned from directly-connected networks into Border Gateway Protocol (BGP).

Syntax

- `default redistribute direct`
- `default redistribute direct enable`
- `default redistribute direct metric`
- `default redistribute direct route-map`
- `default redistribute direct vrf-src WORD<1-16>`
- `no redistribute direct`
- `no redistribute direct enable`
- `no redistribute direct vrf-src WORD<1-16>`
- `redistribute direct`
- `redistribute direct enable`
- `redistribute direct metric <0-65535>`
- `redistribute direct route-map WORD<0-64>`
- `redistribute direct vrf-src WORD<1-16>`

Default

By default, route redistribution is disabled.

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
`enable`	Enables the redistribution.
`metric <0-65535>`	Specifies the value of the metric to be announced in the advertisement. The default is 0.
`route-map WORD<0-64>`	Configures the route policy to apply to redistributed routes.
`vrf-src WORD<1-16>`	Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

©Avaya Inc. 2015 All Rights Reserved.

redistribute direct (for IS-IS)

Control the redistribution of routes from the global router into the Shortest Path Bridging MAC (SPBM) Intermediate-System-to-Intermediate-System (IS-IS) domain.

Syntax

- `default redistribute direct enable`
- `default redistribute direct metric`
- `default redistribute direct metric-type`
- `default redistribute direct route-map`
- `default redistribute direct subnets`
- `no redistribute direct`
- `no redistribute direct enable`
- `no redistribute direct metric`
- `no redistribute direct metric-type`
- `no redistribute direct route-map`
- `no redistribute direct subnets`
- `redistribute direct`
- `redistribute direct enable`
- `redistribute direct metric <0-65535>`
- `redistribute direct metric-type external`
- `redistribute direct metric-type internal`
- `redistribute direct route-map WORD<0-64>`
- `redistribute direct subnets allow`
- `redistribute direct subnets suppress`

Default

By default, route redistribution is disabled.

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description

enable	Enables route redistribution.
metric <0-65535>	Configures the metric (cost) to apply to redistributed routes. The default is 1.
metric-type external	Configures the type of route to import into the protocol. The default is internal.
metric-type internal	Configures the type of route to import into the protocol. The default is internal.
route-map WORD<0-64>	Configures the route policy to apply to redistributed routes.
subnets allow	Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.
subnets suppress	Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.

©Avaya Inc. 2015 All Rights Reserved.

redistribute (for OSPF)

Redistribute learned routes into OSPF.

Syntax

- `default redistribute WORD<0-32>`
- `default redistribute WORD<0-32> enable`
- `default redistribute WORD<0-32> metric`
- `default redistribute WORD<0-32> metric-type`
- `default redistribute WORD<0-32> route-policy`
- `default redistribute WORD<0-32> subnets`
- `default redistribute WORD<0-32> vrf-src WORD<1-16>`
- `no redistribute WORD<0-32>`
- `no redistribute WORD<0-32> enable`
- `no redistribute WORD<0-32> route-policy`
- `no redistribute WORD<0-32> vrf-src WORD<1-16>`
- `redistribute WORD<0-32>`
- `redistribute WORD<0-32> enable`
- `redistribute WORD<0-32> metric <0-65535>`
- `redistribute WORD<0-32> metric-type { type1 | type2 }`
- `redistribute WORD<0-32> route-policy WORD<0-64>`
- `redistribute WORD<0-32> subnets { allow | suppress }`
- `redistribute WORD<0-32> vrf-src WORD<1-16>`

Default

`By default, route redistribution is disabled.`

Command mode

OSPF Router Configuration

Command parameters

Parameter	Description
`enable`	Enables route redistribution of Intermediate-System-to-Intermediate-System (IS-IS) learned IP routes into OSPF.

metric <0-65535>	Configures the metric (cost) to apply to redistributed routes. The default is 1.
metric-type { type1 | type2 }	Configures the type of route to import into the OSPF protocol.
route-policy WORD<0-64>	Configures the route policy to apply to redistributed routes.
subnets { allow | suppress }	Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.
vrf-src WORD<1-16>	Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.
WORD<0-32>	Specifies the protocol type. The possible values are bgp, direct, isis, ospf, rip, or static.

©Avaya Inc. 2015 All Rights Reserved.

redistribute (for RIP)

Redistribute learned routes into RIP.

Syntax

- default redistribute WORD<0-32>
- default redistribute WORD<0-32> enable
- default redistribute WORD<0-32> enable vrf-src WORD<1-16>
- default redistribute WORD<0-32> metric
- default redistribute WORD<0-32> metric vrf-src WORD<1-16>
- default redistribute WORD<0-32> route-map
- default redistribute WORD<0-32> route-map vrf-src WORD<1-16>
- default redistribute WORD<0-32> vrf-src WORD<1-16>
- no redistribute WORD<0-32>
- no redistribute WORD<0-32> enable
- no redistribute WORD<0-32> enable vrf-src WORD<1-16>
- no redistribute WORD<0-32> route-map
- no redistribute WORD<0-32> route-map vrf-src WORD<1-16>
- no redistribute WORD<0-32> vrf-src WORD<1-16>
- redistribute WORD<0-32>
- redistribute WORD<0-32> enable
- redistribute WORD<0-32> enable vrf-src WORD<1-16>
- redistribute WORD<0-32> metric <0-65535>
- redistribute WORD<0-32> metric <0-65535> vrf-src WORD<1-16>
- redistribute WORD<0-32> route-map WORD<0-64>
- redistribute WORD<0-32> route-map WORD<0-64> vrf-src WORD<1-16>
- redistribute WORD<0-32> vrf-src WORD<1-16>

Default

By default, route redistribution is disabled.

Command mode

RIP Router Configuration

Command parameters

Parameter	Description
enable	Enables route redistribution of Intermediate-System-to-Intermediate-System (IS-IS) learned IP routes into RIP.
metric <0-65535>	Configures the metric (cost) to apply to redistributed routes. The default is 1.
route-map WORD<0-64>	Configures the route policy to apply to redistributed routes.
vrf-src WORD<1-16>	Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.
WORD<0-32>	Specifies the protocol type. The possible values are bgp, direct, isis, ospf, rip, or static.

©Avaya Inc. 2015 All Rights Reserved.

redistribute ipv6-direct (for BGP)

Redistribute routes learned from IPv6 directly-connected networks into Border Gateway Protocol (BGP).

Syntax

- `default redistribute ipv6-direct`
- `default redistribute ipv6-direct enable`
- `default redistribute ipv6-direct metric`
- `default redistribute ipv6-direct route-map`
- `no redistribute ipv6-direct`
- `no redistribute ipv6-direct enable`
- `no redistribute ipv6-direct route-map`
- `redistribute ipv6-direct`
- `redistribute ipv6-direct enable`
- `redistribute ipv6-direct metric <0-65535>`
- `redistribute ipv6-direct route-map WORD<0-64>`

Default

By default, route redistribution is disabled.

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
`enable`	Enables the redistribution.
`metric <0-65535>`	Specifies the value of the metric to be announced in the advertisement. The default is 0.
`route-map WORD<0-64>`	Configures the route policy to apply to redistributed routes.

©Avaya Inc. 2015 All Rights Reserved.

redistribute ipv6-static (for BGP)

Redistribute IPv6 static routes into Border Gateway Protocol (BGP).

Syntax

- `default redistribute ipv6-static`
- `default redistribute ipv6-static enable`
- `default redistribute ipv6-static metric`
- `default redistribute ipv6-static route-map`
- `no redistribute ipv6-static`
- `no redistribute ipv6-static enable`
- `no redistribute ipv6-static route-map`
- `redistribute ipv6-static`
- `redistribute ipv6-static enable`
- `redistribute ipv6-static metric <0-65535>`
- `redistribute ipv6-static route-map WORD<0-64>`

Default

By default, route redistribution is disabled.

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
`enable`	Enables the redistribution.
`metric <0-65535>`	Specifies the value of the metric to be announced in the advertisement. The default is 0.
`route-map WORD<0-64>`	Configures the route policy to apply to redistributed routes.

©Avaya Inc. 2015 All Rights Reserved.

redistribute isis (for BGP)

Redistribute learned routes into Border Gateway Protocol (BGP).

Syntax

- `default redistribute isis`
- `default redistribute isis enable`
- `default redistribute isis metric`
- `default redistribute isis route-map`
- `default redistribute isis vrf-src WORD<1-16>`
- `no redistribute isis`
- `no redistribute isis enable`
- `redistribute isis`
- `redistribute isis enable`
- `redistribute isis metric <0-65535>`
- `redistribute isis route-map WORD<0-64>`
- `redistribute isis vrf-src WORD<1-16>`

Default

`By default, route redistribution is disabled.`

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
`enable`	Enables the redistribution of Intermediate-System-to-Intermediate-System (IS-IS) learned IP routes into BGP.
`metric <0-65535>`	Specifies the value of the metric to be announced in the advertisement. The default is 1.
`route-map WORD<0-64>`	Configures the route policy to apply to redistributed routes.
`vrf-src WORD<1-16>`	Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

©Avaya Inc. 2015 All Rights Reserved.

redistribute ospf (for BGP)

Redistribute OSPF-learned routes into Border Gateway Protocol (BGP).

Syntax

- `default redistribute ospf`
- `default redistribute ospf enable`
- `default redistribute ospf metric`
- `default redistribute ospf route-map`
- `default redistribute ospf vrf-src WORD<1-16>`
- `no redistribute ospf`
- `no redistribute ospf enable`
- `no redistribute ospf vrf-src WORD<1-16>`
- `redistribute ospf`
- `redistribute ospf enable`
- `redistribute ospf metric <0-65535>`
- `redistribute ospf route-map WORD<0-64>`
- `redistribute ospf vrf-src WORD<1-16>`

Default

`By default, route redistribution is disabled.`

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
`enable`	Enables the redistribution.
`metric <0-65535>`	Specifies the value of the metric to be announced in the advertisement. The default is 0.
`route-map WORD<0-64>`	Configures the route policy to apply to redistributed routes.
`vrf-src WORD<1-16>`	Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

©Avaya Inc. 2015 All Rights Reserved.

redistribute ospf (for IS-IS)

Control the redistribution of routes from the global router into the Shortest Path Bridging MAC (SPBM) Intermediate-System-to-Intermediate-System (IS-IS) domain.

Syntax

- `default redistribute ospf enable`
- `default redistribute ospf metric`
- `default redistribute ospf metric-type`
- `default redistribute ospf route-map`
- `default redistribute ospf subnets`
- `no redistribute ospf`
- `no redistribute ospf enable`
- `no redistribute ospf metric`
- `no redistribute ospf metric-type`
- `no redistribute ospf route-map`
- `no redistribute ospf subnets`
- `redistribute ospf`
- `redistribute ospf enable`
- `redistribute ospf metric <0-65535>`
- `redistribute ospf metric-type external`
- `redistribute ospf metric-type internal`
- `redistribute ospf route-map WORD<0-64>`
- `redistribute ospf subnets allow`
- `redistribute ospf subnets suppress`

Default

By default, route redistribution is disabled.

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description

enable	Enables route redistribution.
metric <0-65535>	Configures the metric (cost) to apply to redistributed routes. The default is 1.
metric-type external	Configures the type of route to import into the protocol. The default is internal.
metric-type internal	Configures the type of route to import into the protocol. The default is internal.
route-map WORD<0-64>	Configures the route policy to apply to redistributed routes.
subnets allow	Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.
subnets suppress	Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.

©Avaya Inc. 2015 All Rights Reserved.

redistribute ospfv3 (for BGP)

Redistribute OSPFv3-learned routes into Border Gateway Protocol (BGP).

Syntax

- `default redistribute ospfv3`
- `default redistribute ospfv3 enable`
- `default redistribute ospfv3 metric`
- `default redistribute ospfv3 route-map`
- `no redistribute ospfv3`
- `no redistribute ospfv3 enable`
- `no redistribute ospfv3 route-map`
- `redistribute ospfv3`
- `redistribute ospfv3 enable`
- `redistribute ospfv3 metric <0-65535>`
- `redistribute ospfv3 route-map WORD<0-64>`

Default

`By default, route redistribution is disabled.`

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
`enable`	Enables the redistribution.
`metric <0-65535>`	Specifies the value of the metric to be announced in the advertisement. The default is 0.
`route-map WORD<0-64>`	Configures the route policy to apply to redistributed routes.

©Avaya Inc. 2015 All Rights Reserved.

redistribute rip (for BGP)

Redistribute RIP-learned routes into Border Gateway Protocol (BGP).

Syntax

- `default redistribute rip`
- `default redistribute rip enable`
- `default redistribute rip metric`
- `default redistribute rip route-map`
- `default redistribute rip vrf-src WORD<1-16>`
- `no redistribute rip`
- `no redistribute rip enable`
- `no redistribute rip vrf-src WORD<1-16>`
- `redistribute rip`
- `redistribute rip enable`
- `redistribute rip metric <0-65535>`
- `redistribute rip route-map WORD<0-64>`
- `redistribute rip vrf-src WORD<1-16>`

Default

By default, route redistribution is disabled.

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
`enable`	Enables the redistribution.
`metric <0-65535>`	Specifies the value of the metric to be announced in the advertisement. The default is 0.
`route-map WORD<0-64>`	Configures the route policy to apply to redistributed routes.
`vrf-src WORD<1-16>`	Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

©Avaya Inc. 2015 All Rights Reserved.

redistribute rip (for IS-IS)

Control the redistribution of routes from the global router into the Shortest Path Bridging MAC (SPBM) Intermediate-System-to-Intermediate-System (IS-IS) domain.

Syntax

- `default redistribute rip enable`
- `default redistribute rip metric`
- `default redistribute rip metric-type`
- `default redistribute rip route-map`
- `default redistribute rip subnets`
- `no redistribute rip`
- `no redistribute rip enable`
- `no redistribute rip metric`
- `no redistribute rip metric-type`
- `no redistribute rip route-map`
- `no redistribute rip subnets`
- `redistribute rip`
- `redistribute rip enable`
- `redistribute rip metric <0-65535>`
- `redistribute rip metric-type external`
- `redistribute rip metric-type internal`
- `redistribute rip route-map WORD<0-64>`
- `redistribute rip subnets allow`
- `redistribute rip subnets suppress`

Default

By default, route redistribution is disabled.

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description

enable	Enables route redistribution.
metric <0-65535>	Configures the metric (cost) to apply to redistributed routes. The default is 1.
metric-type external	Configures the type of route to import into the protocol. The default is internal.
metric-type internal	Configures the type of route to import into the protocol. The default is internal.
route-map WORD<0-64>	Configures the route policy to apply to redistributed routes.
subnets allow	Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.
subnets suppress	Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.

©Avaya Inc. 2015 All Rights Reserved.

redistribute static (for BGP)

Redistribute static routes into Border Gateway Protocol (BGP).

Syntax

- `default redistribute static`
- `default redistribute static enable`
- `default redistribute static metric`
- `default redistribute static route-map`
- `default redistribute static vrf-src WORD<1-16>`
- `no redistribute static`
- `no redistribute static enable`
- `no redistribute static vrf-src WORD<1-16>`
- `redistribute static`
- `redistribute static enable`
- `redistribute static metric <0-65535>`
- `redistribute static route-map WORD<0-64>`
- `redistribute static vrf-src WORD<1-16>`

Default

`By default, route redistribution is disabled.`

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
`enable`	Enables the redistribution.
`metric <0-65535>`	Specifies the value of the metric to be announced in the advertisement. The default is 0.
`route-map WORD<0-64>`	Configures the route policy to apply to redistributed routes.
`vrf-src WORD<1-16>`	Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

©Avaya Inc. 2015 All Rights Reserved.

redistribute static (for IS-IS)

Control the redistribution of routes from the global router into the Shortest Path Bridging MAC (SPBM) Intermediate-System-to-Intermediate-System (IS-IS) domain.

Syntax

- `default redistribute static enable`
- `default redistribute static metric`
- `default redistribute static metric-type`
- `default redistribute static route-map`
- `default redistribute static subnets`
- `no redistribute static`
- `no redistribute static enable`
- `no redistribute static metric`
- `no redistribute static metric-type`
- `no redistribute static route-map`
- `no redistribute static subnets`
- `redistribute static`
- `redistribute static enable`
- `redistribute static metric <0-65535>`
- `redistribute static metric-type external`
- `redistribute static metric-type internal`
- `redistribute static route-map WORD<0-64>`
- `redistribute static subnets allow`
- `redistribute static subnets suppress`

Default

By default, route redistribution is disabled.

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description

enable	Enables route redistribution.
metric <0-65535>	Configures the metric (cost) to apply to redistributed routes. The default is 1.
metric-type external	Configures the type of route to import into the protocol. The default is internal.
metric-type internal	Configures the type of route to import into the protocol. The default is internal.
route-map WORD<0-64>	Configures the route policy to apply to redistributed routes.
subnets allow	Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.
subnets suppress	Indicates whether the subnets are advertised individually or aggregated to their classful subnet. Choose allow to advertise the subnets individually with the learned or configured mask of the subnet. The default is allow.

©Avaya Inc. 2015 All Rights Reserved.

remote-mirroring

Use remote mirroring to monitor many ports from different switches using one network probe device.

Syntax

- default remote-mirroring
- default remote-mirroring dstMac
- default remote-mirroring enable
- default remote-mirroring ether-type
- default remote-mirroring mode
- default remote-mirroring port {slot/port[-slot/port][,...]}
- default remote-mirroring srcMac
- no remote-mirroring
- no remote-mirroring enable
- no remote-mirroring port {slot/port[-slot/port][,...]}
- no remote-mirroring vlan-id <1-4084>
- remote-mirroring
- remote-mirroring dstMac 0x00:0x00:0x00:0x00:0x00:0x00
- remote-mirroring enable
- remote-mirroring ether-type <0x00-0xffff>
- remote-mirroring mode source
- remote-mirroring mode termination
- remote-mirroring port {slot/port[-slot/port][,...]}
- remote-mirroring srcMac 0x00:0x00:0x00:0x00:0x00:0x00
- remote-mirroring vlan-id <1-4084>

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
dstMac <0x00:0x00:0x00:0x00:0x00:0x00>	Sets the destination MAC address for use in the remote mirroring encapsulation header. The mirrored packet is sent to this MAC address. The DstMac is used only for RMS ports. For RMT ports, one of the unused MAC addresses from the switch port MAC address range is used. This MAC address is saved in the configuration file.
enable	Enables remote mirroring on the port. When remote mirroring is enabled, the following events occur: A static entry for the DstMac is added to the Forwarding Database (FDB). All packets that come with this remote mirroring DstMac are sent to the RMT port. The switch periodically (once in 10 seconds) transmits broadcast Layer 2 packets in the associated VLAN so that all nodes in the network can learn the DstMac.
ether-type <0x00-0xffff>	Specifies the ethertype of the remote mirrored packet. The default value is 0x8103.
mode <source|termination>	Specifies whether the port is an RMT (mode is termination) or an RMS (mode is source).
srcMac <0x00:0x00:0x00:0x00:0x00:0x00>	Sets the source MAC address for use in the remote mirroring encapsulation header. The mirrored packet is sent from the RMS port, and the source MAC parameter in the header is derived from this address. The source MAC address of the encapsulated frame contains the first 45 bits of this MAC address. The three least significant bits are derived from the port number of the RMS port. The MAC address of the port is used as the default value.
vlan-id <1-4084>	Specifies to which VLAN the remote mirroring destination MAC address belongs. This must be a port-based VLAN. Used only for Remote Mirroring Termination (RMT) ports. When the RMT port is removed from the last VLAN in the list, RMT is disabled on the port.

©Avaya Inc. 2015 All Rights Reserved.

remove

Remove files or directories to free space.

Syntax

- `remove WORD<1-255>`
- `remove WORD<1-255> -y`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
WORD<1-255>	WORD<1-255> specifies the file to remove.
WORD<1-255>	Specifies the file name to remove in one of the following formats:/intflash/ <file>, /extflash/ <file>, /usb/<file>, /mnt/intflash/ <file> , or /mnt/extflash/ <file>. /mnt/intflash is the internal flash of the second CP module (the one to which you are not connected) /mnt/extflash is the external flash of the second CP module (the one to which you are not connected) WORD<1-255> is a string of 1-255 characters.
-y	Skips the confirm question.

©Avaya Inc. 2015 All Rights Reserved.

rename

Use this command to rename a file.

Syntax

- `rename WORD<1-255> WORD<1-255>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
WORD<1-255>	Specifies the file to rename.
WORD<1-255>	The second instance, specifies the file name to rename in one of the following formats:/intflash/ <file>, /extflash/ <file> , /usb/<file>, /mnt/intflash/ <file>, or /mnt/extflash/ <file>. /mnt/intflash is the internal flash of the second CP module (the one to which you are not connected) /mnt/extflash is the external flash of the second CP module (the one to which you are not connected) WORD<1-255> is a string of 1-255 characters.

©Avaya Inc. 2015 All Rights Reserved.

reset

Reset the platform to reload system parameters from the most recently saved configuration file.

Syntax

- `reset`
- `reset -coredump`
- `reset -coredump -y`
- `reset -y`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`-coredump`	Creates a coredump for the main process before the switch resets. Caution: Only use the -coredump parameter if an issue causes you to reset the switch, and you need to contact customer service for analysis of the problem.
`-y`	Suppresses the confirmation message before the switch resets. If you omit this parameter, you must confirm the action before the switch resets.

©Avaya Inc. 2015 All Rights Reserved.

restore

Use this command to restore the internal flash or the external flash from the USB device. You must disable logging to the compact flash you want to restore before you can use the restore.

Syntax

- `restore <intflash|extflash>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
extflash	Specifies the external flash to be restored.
intflash	Specifies the internal flash to be restored.

©Avaya Inc. 2015 All Rights Reserved.

retransmit-lsp-interval

Configure the minimum time between retransmission of a Link State Packet (LSP). This defines how fast the switch resends the same LSP. This is a system level parameter that applies for Level 1 retransmission of LSPs.

Syntax

- `default retransmit-lsp-interval`
- `no retransmit-lsp-interval`
- `retransmit-lsp-interval <1-300>`

Default

`The default is 5 seconds.`

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description
`<1-300>`	Specifies the minimum time between retransmission of a Link State Packet (LSP). This defines how fast the switch resends the same LSP. This is a system level parameter that applies for Level1 retransmission of LSPs.

©Avaya Inc. 2015 All Rights Reserved.

rfc1583-compatibility enable

Controls the preference rules used when the router chooses among multiple autonomous system external (ASE) LSAs which advertise the same destination. If enabled, the preference rule is the same as that specified by RFC1583. If disabled, the preference rule is as described in RFC2328, which can prevent routing loops when ASE LSAs for the same destination originate from different areas.

Syntax

- `default rfc1583-compatibility`
- `default rfc1583-compatibility enable`
- `no rfc1583-compatibility`
- `no rfc1583-compatibility enable`
- `rfc1583-compatibility enable`

Default

`The default is disabled.`

Command mode

OSPF Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

rlogin

Use this command to login remotely to a remote host.

Syntax

- `rlogin {A.B.C.D}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
{A.B.C.D}	Specifies the IP address.

©Avaya Inc. 2015 All Rights Reserved.

rmon

Configure RMON functions on the switch.

Syntax

- `default rmon`
- `default rmon memsize`
- `default rmon trap-option`
- `default rmon util-method`
- `no rmon`
- `rmon`
- `rmon memsize <250000-4000000>`
- `rmon trap-option { toOwner | toAll }`
- `rmon util-method { half | full }`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`memsize <250000-4000000>`	Configures the amount of RAM in bytes to allocate for Remote Network Monitoring (RMON). The range is 250000-4000000.
`trap-option <toOwner|toAll>`	Controls whether the Remote Network Monitoring (RMON) traps are sent to the owner or to all trap recipients. toOwner|toAll is set to either the owner or to all trap recipients.
`util-method <half|full>`	Controls whether port utilization is calculated in half or full duplex.

©Avaya Inc. 2015 All Rights Reserved.

rmon alarm

Creates an alarm interface.

Syntax

- `default rmon alarm <1-65535>`
- `default rmon alarm <1-65535> owner`
- `no rmon alarm <1-65535>`
- `rmon alarm <1-65535> WORD<1-1536> <1-3600> { absolute | delta }`
- `rmon alarm <1-65535> WORD<1-1536> <1-3600> { absolute | delta } falling-threshold <-2147483647-2147483647> event <1-65535>`
- `rmon alarm <1-65535> WORD<1-1536> <1-3600> { absolute | delta } falling-threshold <-2147483647-2147483647> event <1-65535> owner WORD<1-127>`
- `rmon alarm <1-65535> WORD<1-1536> <1-3600> { absolute | delta } falling-threshold <-2147483647-2147483647> event <1-65535> rising-threshold <-2147483647-2147483647> event <1-65535>`
- `rmon alarm <1-65535> WORD<1-1536> <1-3600> { absolute | delta } falling-threshold <-2147483647-2147483647> event <1-65535> rising-threshold <-2147483647-2147483647> event <1-65535> owner WORD<1-127>`
- `rmon alarm <1-65535> WORD<1-1536> <1-3600> { absolute | delta } owner WORD<1-127>`
- `rmon alarm <1-65535> WORD<1-1536> <1-3600> { absolute | delta } rising-threshold <-2147483647-2147483647> event <1-65535>`
- `rmon alarm <1-65535> WORD<1-1536> <1-3600> { absolute | delta } rising-threshold <-2147483647-2147483647> event <1-65535> falling-threshold <-2147483647-2147483647> event <1-65535>`
- `rmon alarm <1-65535> WORD<1-1536> <1-3600> { absolute | delta } rising-threshold <-2147483647-2147483647> event <1-65535> falling-threshold <-2147483647-2147483647> event <1-65535> owner WORD<1-127>`
- `rmon alarm <1-65535> WORD<1-1536> <1-3600> { absolute | delta } rising-threshold <-2147483647-2147483647> event <1-65535> owner WORD<1-127>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`{absolute | delta}`	Specifies the sample type.
`<1-3600>`	Specifies the sampling interval.

<1-65535>	Specifies the interface index number from 1-65535.
event <1-65535>	Specifies the event number.
falling-threshold <-2147483647-2147483647>	Specifies the falling threshold value for the sampled statistic.
owner WORD<1-127>	Specifies the name of the owner. The default value is CLI if the entry is configured using ACLI. The default is SNMP if the entry is configured using EDM or SNMP.
rising-threshold <-2147483647-2147483647>	Specifies the rising threshold value for the samples statistic.
WORD<1-536>	Specifies the variable name or OID, case sensitive.

©Avaya Inc. 2015 All Rights Reserved.

rmon event

Creates an event.

Syntax

- `default rmon event <1-65535>`
- `default rmon event <1-65535> community`
- `default rmon event <1-65535> description`
- `default rmon event <1-65535> owner`
- `no rmon event <1-65535>`
- `no rmon event <1-65535> log`
- `rmon event <1-65535>`
- `rmon event <1-65535> community WORD<1-127>`
- `rmon event <1-65535> description WORD<0-127>`
- `rmon event <1-65535> log`
- `rmon event <1-65535> owner WORD<1-127>`
- `rmon event <1-65535> trap`
- `rmon event <1-65535> trap_dest`
- `rmon event <1-65535> trap_dest {A.B.C.D}`
- `rmon event <1-65535> trap_src`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`<1-65535>`	Specifies the event index number.
`community WORD<1-127>`	Specifies the event community.
`description WORD<0-127>`	Specifies the event description.
`log`	Displays information about configured traps.
`owner`	Specifies the name of the event owner. The default value is CLI if the entry is

WORD<1-127>	configured using ACLI. The default is SNMP if the entry is configured using EDM or SNMP.
trap_dest {A.B.C.D}	Specifies trap destination IP addresses.
trap_src	Specifies trap source IP addresses.

©Avaya Inc. 2015 All Rights Reserved.

rmon history

Creates a history control interface.

Syntax

- `default rmon history <1-65535>`
- `default rmon history <1-65535> buckets`
- `default rmon history <1-65535> interval`
- `default rmon history <1-65535> owner`
- `no rmon history <1-65535>`
- `rmon history <1-65535> {slot/port[-slot/port][,...]}`
- `rmon history <1-65535> {slot/port[-slot/port][,...]} buckets <1-65535>`
- `rmon history <1-65535> {slot/port[-slot/port][,...]} interval <1-3600>`
- `rmon history <1-65535> {slot/port[-slot/port][,...]} owner WORD<1-127>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-65535>`	Specifies the index number of the history control interface.
`buckets <1-65535>`	Specifies the number of buckets requested. The default is 50.
`interval <1-3600>`	Specifies the the time interval in seconds over which the data is sampled for each bucket. The default is 1800.
`owner WORD<1-127>`	Specifies the name of the entry owner. The default value is CLI if the entry is configured using ACLI. The default is SNMP if the entry is configured using EDM or SNMP.

©Avaya Inc. 2015 All Rights Reserved.

rmon stats

Creates an ether-stats control interface.

Syntax

- `default rmon stats <1-65535>`
- `default rmon stats <1-65535> owner`
- `no rmon stats <1-65535>`
- `rmon stats <1-65535> {slot/port[-slot/port][,...]}`
- `rmon stats <1-65535> {slot/port[-slot/port][,...]} owner WORD<1-127>`
- `rmon stats <1-65535> owner WORD<1-127>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-65535>`	Specifies the index number of the ether stats control interface.
`owner WORD<1-127>`	Specifies the name of the entry owner. The default value is CLI if the entry is configured using ACLI. The default is SNMP if the entry is configured using EDM or SNMP.

©Avaya Inc. 2015 All Rights Reserved.

route-map

Configure and enable a route policy so that the switch can control routes that certain packets can take.

Syntax

- `default route-map WORD<1-64> <1-65535>`
- `no route-map WORD<1-64> <1-65535>`
- `route-map WORD<1-64> <1-65535>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-65535>	Specifies the sequence number for the route policy.
WORD<1-64>	Specifies the policy name.

©Avaya Inc. 2015 All Rights Reserved.

router bgp

Access the router configuration mode to configure the Border Gateway Protocol (BGP) commands.

Syntax

- `router bgp`
- `router bgp [WORD<0-11>] [enable]`

Default

None

Command mode

Global Configuration

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

router bgp as-4-byte enable

Globally enable 4-byte autonomous system numbers.

Syntax

- `default router bgp as-4-byte enable`
- `no router bgp as-4-byte enable`
- `router bgp as-4-byte enable`

Default

`The default is disabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

router bgp as-dot enable

Globally enable the AS dot representation for 4-byte AS numbers.

Syntax

- `default router bgp as-dot enable`
- `no router bgp as-dot enable`
- `router bgp as-dot enable`

Default

`The default is disabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

router bgp enable

Specify the AS number and enable BGP.

Syntax

- `router bgp [WORD <0-11>] [enable]`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`enable`	Enables the BGP on the router.
`WORD<0-11>`	Specifies the AS number. You cannot enable BGP until you change the local AS to a value other than 0.

©Avaya Inc. 2015 All Rights Reserved.

router bgp enable globally

Specify the AS number and enable BGP.

Syntax

- `router bgp [WORD <0-11>][enable]`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`enable`	Enables the BGP on the router.
`WORD<0-11>`	Specifies the AS number. You cannot enable BGP until you change the local AS to a value other than 0.

©Avaya Inc. 2015 All Rights Reserved.

route-reflector enable

Enable the reflection of routes from IBGP neighbors.

Syntax

- `default route-reflector`
- `default route-reflector enable`
- `no route-reflector`
- `no route-reflector enable`
- `route-reflector`
- `route-reflector enable`

Default

`The default value is enable.`

Command mode

BGP Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

route-refresh

Enable or disable IP VPN Route Refresh. If enabled, a route refresh request received by a BGP speaker causes the speaker to resend all route updates it contains in its database that are eligible for the peer that issues the request.

Syntax

- `default route-refresh`
- `no route-refresh`
- `route-refresh`

Default

`The default value is disable`

Command mode

BGP Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

router-id (for BGP)

Specify the BGP router ID in IP address format.

Syntax

- `default router-id`
- `no router-id`
- `router-id {A.B.C.D}`

Default

None

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
<A.B.C.D>	Identifies the router IP address.

©Avaya Inc. 2015 All Rights Reserved.

router-id (for OSPF)

Configure OSPF parameters on the switch to control how OSPF behaves on the system. The Virtual Services Platform 9000 uses global parameters to communicate with other OSPF routers. Globally configure OSPF before you configure OSPF for an interface, port, or VLAN.

Syntax

- `default router-id`
- `no router-id`
- `router-id {A.B.C.D}`

Default

None

Command mode

OSPF Router Configuration

Command parameters

Parameter	Description
`router-id <A.B.C.D>`	Configures the OSPF router ID IP address, where A.B.C.D is the IP address.

©Avaya Inc. 2015 All Rights Reserved.

router isis

Enter Intermediate-System-to-Intermediate-System (IS-IS) Router Configuration mode.

Syntax

- `default router isis`
- `no router isis`
- `router isis`

Default

None

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

router isis enable

Enable Intermediate-System-to-Intermediate-System (IS-IS) globally. If you use the default or no format of this command, you disable IS-IS globally.

Syntax

- `default router isis enable`
- `no router isis enable`
- `router isis enable`

Default

`The default is disabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

router ospf

Enable OSPF for the switch. If you do not use an optional parameter with the command, you enter the OSPF Router Configuration mode.

Syntax

- `default router ospf [enable|ipv6-enable]`
- `no router ospf [enable|ipv6-enable]`
- `router ospf [enable|ipv6-enable]`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`enable`	Enables OSPF routing on the Virtual Services Platform 9000.
`ipv6-enable`	Enables OSPFv3 for IPv6 routing.

©Avaya Inc. 2015 All Rights Reserved.

router rip enable

Enable RIP globally.

Syntax

- `router rip enable`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`enable`	Globally enables RIP on the VRF or switch.

©Avaya Inc. 2015 All Rights Reserved.

routing

Enable or disable routing capabilities on specified switch ports. The specified port can be part of a routed VLAN, while routing is disabled only on that port.

Syntax

- `default routing`
- `default routing enable`
- `default routing port {slot/port[-slot/port][,...]}`
- `default routing port {slot/port[-slot/port][,...]} enable`
- `no routing`
- `no routing enable`
- `no routing port {slot/port[-slot/port][,...]}`
- `no routing port {slot/port[-slot/port][,...]} enable`
- `routing`
- `routing enable`
- `routing port {slot/port[-slot/port][,...]} enable`

Default

`The default setting for routing is enabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Sets the IP routing to enable.
`port {slot/port[-slot/port][,...]}`	Specifies the port and the slot number to be changed.

©Avaya Inc. 2015 All Rights Reserved.

rsh

Use this command to execute a shell command on a remote machine.

Syntax

- rsh {A.B.C.D} -l WORD<0-1536> WORD<1-1536>
- rsh {A.B.C.D} -l WORD<0-1536> WORD<1-1536> WORD<0-1536> WORD<0-1536>
- rsh {A.B.C.D} -l WORD<0-1536> WORD<1-1536> WORD<0-1536> WORD<0-1536>
- rsh {A.B.C.D} -l WORD<0-1536> WORD<1-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536>
- rsh {A.B.C.D} -l WORD<0-1536> WORD<1-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536>
- rsh {A.B.C.D} -l WORD<0-1536> WORD<1-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536>
- rsh {A.B.C.D} -l WORD<0-1536> WORD<1-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536>

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
{A.B.C.D}	Specifies the IP address in the {A.B.C.D} format.
-l	Specifies the user login name.
WORD<0-1536>	Specifies the command to execute on the remote host: Param1 for rsh command. String length {0-1536} Param2 for rsh command. String length {0-1536} Param3 for rsh command. String length {0-1536} Param4 for rsh command. String length {0-1536} Param5 for rsh command. String length {0-1536} Param6 for rsh command. String length {0-1536} Param7 for rsh command. String length {0-1536}

©Avaya Inc. 2015 All Rights Reserved.

save clilog

Save the CLI logs to a file. This command only applies to log files generated by past releases prior to Release 3.2. This command is obsolete starting with Release 3.2.

Syntax

- `save clilog`
- `save clilog file WORD<1-99>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`file WORD<1-99>`	Specifies the file name in one of the following formats: a.b.c.d: <file>, /intflash/ <file>, /extflash/ <file>, /mnt/intflash/ <file>, /mnt/extflash/ <file>, or /usb/<file> . /mnt/intflash is equivalent to the /intflash of the standby CP (if present). /mnt/extflash is equivalent to the /extflash of the standby CP (if present). WORD<1-99> is a string of 1-99 characters.

©Avaya Inc. 2015 All Rights Reserved.

save config

Save the configuration to a file to retain the configuration settings.

Syntax

- `save config`
- `save config backup WORD<1-99>`
- `save config file WORD<1-99>`
- `save config standby WORD<1-99>`
- `save config verbose`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
backup WORD<1-99>	Saves the specified file name and identifies the file as a backup file. a.b.c.d: <file>, /intflash/ <file>, /extflash/ <file>, /mnt/intflash/ <file>, /mnt/extflash/ <file>, or /usb/<file> . /mnt/intflash is equivalent to the /intflash of the standby CP (if present). /mnt/extflash is equivalent to the /extflash of the standby CP (if present). The VSP 9000 supports /mnt/intflash and /mnt/extflash. WORD<1-99> is a string of 1-99 characters.
file WORD<1-99>	Specifies the file name in one of the following formats: a.b.c.d: <file>, /intflash/ <file>, /extflash/ <file>, /mnt/intflash/ <file>, /mnt/extflash/ <file>, or /usb/<file> . /mnt/intflash is the internal flash of the second CP module (the one to which you are not connected) /mnt/extflash is the external flash of the second CP module (the one to which you are not connected) WORD<1-99> is a string of 1-99 characters.
standby WORD<1-99>	Saves the specified file name to the standby CPU in the following format:/intflash/ <file>, /extflash/ <file> , or /usb/<file> . WORD<1-99> is a string of 1-99 characters.
verbose	Saves the default and current configuration. If you omit this parameter, the command saves only parameters you change.

©Avaya Inc. 2015 All Rights Reserved.

save log

Save the log files, assuming the files use the default file names.

Syntax

- `save log`
- `save log file WORD<1-99>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`file WORD<1-99>`	Specifies the file name in one of the following formats: a.b.c.d: <file>, /intflash/ <file>, /extflash/ <file>, /mnt/intflash/ <file>, /mnt/extflash/ <file>, or /usb/<file> . /mnt/intflash is the internal flash of the second CP module (the one to which you are not connected) /mnt/extflash is the external flash of the second CP module (the one to which you are not connected) WORD<1-99> is a string of 1-99 characters.

©Avaya Inc. 2015 All Rights Reserved.

save snmplog

Save the Simple Network Management Protocol (SNMP) trap log files to a file. This command only applies to log files generated by past releases prior to Release 3.2. This command is obsolete starting with Release 3.2.

Syntax

- `save snmplog`
- `save snmplog file WORD<1-99>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`file WORD<1-99>`	Specifies the file name in one of the following formats: a.b.c.d: <file>, /intflash/ <file>, /extflash/ <file>, /mnt/intflash/ <file>, /mnt/extflash/ <file>, or /usb/<file> . /mnt/intflash is the internal flash of the second CP module (the one to which you are not connected) /mnt/extflash is the external flash of the second CP module (the one to which you are not connected) WORD<1-99> is a string of 1-99 characters.

©Avaya Inc. 2015 All Rights Reserved.

save trace

Save the trace file to the card for retrieval.

Syntax

- `save trace`
- `save trace file WORD<1-99>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`file WORD<1-99>`	Specifies the file name in one of the following formats: a.b.c.d: <file>, /intflash/ <file>, /extflash/ <file>, /mnt/intflash/ <file>, /mnt/extflash/ <file>, or /usb/<file> . /mnt/intflash is the internal flash of the second CP module (the one to which you are not connected) . /mnt/extflash is the external flash of the second CP module (the one to which you are not connected) .

©Avaya Inc. 2015 All Rights Reserved.

send-trap

Configure Virtual Router Redundancy Protocol (VRRP) notification control.

Syntax

- `default send-trap`
- `default send-trap enable`
- `default send-trap enable vrf WORD<1-16>`
- `no send-trap`
- `no send-trap enable`
- `no send-trap enable vrf WORD<1-16>`
- `send-trap`
- `send-trap enable`
- `send-trap enable vrf WORD<1-16>`

Default

`Generation of SNMP traps for VRRP events is enabled.`

Command mode

VRRP Router Configuration

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies the VRF name.

©Avaya Inc. 2015 All Rights Reserved.

set as-path

Add the AS number of the AS-list to the BGP routes that match this policy.

Syntax

- `default set as-path WORD<0-256>`
- `no set as-path WORD<0-256>`
- `set as-path WORD<0-256>`

Default

None

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
WORD<0-256>	Specifies the list ID of up to four defined AS-lists separated by a comma.

©Avaya Inc. 2015 All Rights Reserved.

set as-path-mode

Configure the AS path mode.

Syntax

- `default set as-path-mode`
- `set as-path-mode prepend`
- `set as-path-mode tag`

Default

`The default is prepend.`

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
`prepend`	Prepends the Autonomous System (AS) number of the AS-list specified in set-as-path to the old as-path attribute of the BGP routes that match this policy.
`tag`	Configures the Autonomous System (AS) path mode to tag.

©Avaya Inc. 2015 All Rights Reserved.

set automatic-tag

Configure the tag automatically. This command is used for BGP routes only.

Syntax

- `default set automatic-tag`
- `default set automatic-tag enable`
- `no set automatic-tag`
- `no set automatic-tag enable`
- `set automatic-tag`
- `set automatic-tag enable`

Default

`The default is disable.`

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
`enable`	Enables this configuration.

©Avaya Inc. 2015 All Rights Reserved.

set community

Add the community number of the community list to the BGP routes that match this policy.

Syntax

- `default set community WORD<0-256>`
- `no set community WORD<0-256>`
- `set community WORD<0-256>`

Default

None

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
WORD<0-256>	Specifies the list ID of up to four defined community lists separated by a comma.

©Avaya Inc. 2015 All Rights Reserved.

set community-mode

Configure the community mode.

Syntax

- `default set community-mode`
- `set community-mode additive`
- `set community-mode none`
- `set community-mode unchanged`

Default

`The default is unchanged.`

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
`additive`	Prepends the community number of the community list specified in set-community to the old community path attribute of the BGP routes that match this policy.
`none`	Removes the community path attribute of the BGP routes that match this policy to the specified value.
`unchanged`	Configures the community mode to unchanged.

©Avaya Inc. 2015 All Rights Reserved.

set injectlist

Replace the destination network of the route that Match this policy with the contents of the specified prefix list.

Syntax

- `default set injectlist`
- `no set injectlist`
- `set injectlist WORD<1-64>`

Default

None

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
WORD<1-64>	Specifies one prefix list by name.

©Avaya Inc. 2015 All Rights Reserved.

set ip-preference

Specify the route preference value to assign to the routes that match this policy. This command applies to accept policies only.

Syntax

- `default set ip-preference`
- `set ip-preference <0-255>`

Default

None

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
<0-255>	Assigns the preference to the routes. If you configure the default, the global preference value is used.

©Avaya Inc. 2015 All Rights Reserved.

set local-preference

Specify a value used during the route decision process in the BGP protocol. This command applies to BGP only.

Syntax

- `default set local-preference`
- `set local-preference <0-65535>`

Default

`The default is 0.`

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
`<0-65535>`	Specifies the local preference value.

©Avaya Inc. 2015 All Rights Reserved.

set mask

Configure the mask of the route that matches this policy. This command applies only to RIP accept policies.

Syntax

- `default set mask`
- `no set mask`
- `set mask {A.B.C.D}`

Default

`The default is 0.0.0.0.`

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
{A.B.C.D}	Specifies a valid contiguous IP mask.

©Avaya Inc. 2015 All Rights Reserved.

set metric

Configure the metric value for the route while announcing a redistribution. If you configure the default, the original cost of the route is advertised into OSPF; for RIP, the original cost of the route or defaultimport- metric is used.

Syntax

- `default set metric`
- `set metric <0-65535>`

Default

`The default is 0.`

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
`<0-65535>`	Specifies a metric value.

©Avaya Inc. 2015 All Rights Reserved.

set metric-type

Configure the metric type for the routes to announce into the OSPF domain that Match this policy. This command applies only for OSPF announce policies.

Syntax

- `default set metric-type`
- `set metric-type { type1 | type2 }`

Default

`The default is type 2.`

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
`{ type1 | type2 }`	Specifies the metric type to announce.

©Avaya Inc. 2015 All Rights Reserved.

set metric-type-internal

Configure the MED value for routes advertised to EBGP neighbors to the specified IGP metric value.

Syntax

- `default set metric-type-internal`
- `set metric-type-internal <0-1>`

Default

`The default is 0.`

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
`<0-1>`	Specifies the Interior Gateway Protocol (IGP) metric value.

©Avaya Inc. 2015 All Rights Reserved.

set next-hop

Specify the IPv4 or IPv6 address of the next-hop router.

Syntax

- `default set next-hop`
- `no set next-hop`
- `set next-hop WORD<1-256>`

Default

None

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
WORD<1-256>	Specifies the IP address.

©Avaya Inc. 2015 All Rights Reserved.

set nssa-pbit

Configure the not so stubby area (NSSA) translation P bit. This command applies to OSPF announce policies only.

Syntax

- `default set nssa-pbit`
- `default set nssa-pbit enable`
- `no set nssa-pbit`
- `no set nssa-pbit enable`
- `set nssa-pbit`
- `set nssa-pbit enable`

Default

`The default is enable.`

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
`enable`	Enables P bit translation.

©Avaya Inc. 2015 All Rights Reserved.

set origin

Change the origin path attribute of the BGP routes that match this policy to the specified value.

Syntax

- `default set origin`
- `set origin { igp | egp | incomplete }`

Default

`The default is unchanged.`

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
`{ igp | egp | incomplete }`	Specifies the origin path attribute.

©Avaya Inc. 2015 All Rights Reserved.

set origin-egp-as

Configure the origin EGP autonomous system (AS). This command applies to BGP only.

Syntax

- `default set origin-egp-as`
- `set origin-egp-as <0-65535>`

Default

`The default is 0.`

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
`<0-65535>`	Indicates the remote Autonomous System (AS) number.

©Avaya Inc. 2015 All Rights Reserved.

set tag

Configure the tag of the destination routing protocol. If not specified, the switch forwards the tag value in the source routing protocol.

Syntax

- `default set tag`
- `set tag <0-65535>`

Default

`The default is 0.`

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
`<0-65535>`	Specifies the tag value. A value of 0 indicates that this parameter is not set.

©Avaya Inc. 2015 All Rights Reserved.

set weight

Configure the weight for the routing table. This command applies to BGP only. This value overrides the weight configured through NetworkTableEntry, FilterListWeight, or NeighborWeight.

Syntax

- `default set weight`
- `set weight <0-65535>`

Default

`The default is 0.`

Command mode

Route-Map Configuration

Command parameters

Parameter	Description
`<0-65535>`	Specifies the weight value. A value of 0 indicates that this parameter is not set.

©Avaya Inc. 2015 All Rights Reserved.

show access-policy

Show access policy configurations.

Syntax

- `show access-policy`
- `show access-policy by-mac`
- `show access-policy snmp-group`
- `show access-policy WORD<0-15>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`by-mac`	Shows access-policy information for MAC addresses.
`snmp-group`	Shows access-policy information by SNMP group.
`WORD<0-15>`	Specifies an access policy name.

©Avaya Inc. 2015 All Rights Reserved.

show alarm database

Display the alarm database statistics.

Syntax

- `show alarm database`
- `show alarm database alarm-id WORD<0-32>`
- `show alarm database alarm-status WORD<0-32>`
- `show alarm database alarm-type WORD<0-32>`
- `show alarm database event-code <0x0-0x00FFFFFF | 0x0-0x0>`
- `show alarm database module WORD<0-100>`
- `show alarm database severity WORD<0-25>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`alarm-id WORD<0-32>`	Displays alarm details for a specific alarm ID.
`alarm-status WORD<0-32>`	Displays alarm details based on alarm status: set or clear.
`alarm-type WORD<0-32>`	Displays alarm details based on alarm type: persistent or dynamic.
`event-code <0x0-0x00FFFFFF | 0x0-0x0>`	Displays alarm details for a specific event code.
`module WORD<0-100>`	Displays alarm details for one or more modules.
`severity WORD<0-25>`	Displays alarm details based on severity level: info, error, warning, or fatal.

©Avaya Inc. 2015 All Rights Reserved.

show application slamon agent

Shows the SLA Mon™ configuration.

Syntax

- `show application slamon agent`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show application vsptalk

Display global VSP Talk information.

Syntax

- `show application vsptalk`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show application vsptalk client

Display VSP Talk client information.

Syntax

- `show application vsptalk client`
- `show application vsptalk client <gtalk|avaya>`

Default

None

Command mode

User EXEC

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

show application vsptalk server

Display VSP Talk server information.

Syntax

- `show application vsptalk server`
- `show application vsptalk server <gtalk|avaya>`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show autotopology

View topology message status to view the interconnections between Layer 2 devices in a network.

Syntax

- `show autotopology nmm-table`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show banner

Display the banner information.

Syntax

- `show banner`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show basic config

Display the basic switch configuration.

Syntax

- `show basic config`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show bgp ipv6 aggregates

Display BGP IPv6 aggregates information.

Syntax

- `show bgp ipv6 aggregates`
- `show bgp ipv6 aggregates WORD<1-256>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
WORD <1-256>	Specifies IPv6 prefix and length in the range of 1 to 256
WORD <1-256>	Specifies the IPv6 prefix and length.

©Avaya Inc. 2015 All Rights Reserved.

show bgp ipv6 imported-routes

Display BGP ipv6 imported-routes information.

Syntax

- `show bgp ipv6 imported-routes`
- `show bgp ipv6 imported-routes WORD<1-256>`
- `show bgp ipv6 imported-routes WORD<1-256> longer-prefixes`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`longer-prefixes`	Shows long prefixes. the longer-prefixes indicate the mask length from any specified prefix to 32 (for example show from prefix A.B.C.D/len to A.B.C.D/32.)
`WORD <1-256>`	Specifies the IPv6 prefix and length.

©Avaya Inc. 2015 All Rights Reserved.

show bgp ipv6 networks

Display information about BGP network configurations.

Syntax

- `show bgp ipv6 networks`
- `show bgp ipv6 networks WORD<1-256>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
WORD <1-256>	Specifies IPv6 prefix and length in the range of 1 to 256

©Avaya Inc. 2015 All Rights Reserved.

show bgp ipv6 redistributed-routes

Display BGP ipv6 redistributed-routes information.

Syntax

- `show bgp ipv6 redistributed-routes`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show bgp ipv6 route

Display information about BGP IPv6 routes.

Syntax

- `show bgp ipv6 route`
- `show bgp ipv6 route community {disable|enable}`
- `show bgp ipv6 route ipv6 WORD<1-256>`
- `show bgp ipv6 route WORD <1-256>`
- `show bgp ipv6 route WORD<1-256> longer-prefixes`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`community {disable|enable}`	Enables or disables the display of community attributes.
`ipv6 WORD<1-256>`	Specifies an IPv6 address.
`longer-prefixes`	Shows long prefixes. the longer-prefixes indicate the mask length from any specified prefix to 32 (for example show from prefix A.B.C.D/len to A.B.C.D/32.)
`WORD <1-256>`	Specifies IPv6 address and length in the range of 1 to 256

©Avaya Inc. 2015 All Rights Reserved.

show boot config

Display the configuration to view current or changed settings for the boot parameters.

Syntax

- `show boot config choice`
- `show boot config flags`
- `show boot config general`
- `show boot config host`
- `show boot config master`
- `show boot config running-config`
- `show boot config running-config verbose`
- `show boot config sio`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`choice`	Shows the current boot configuration choices.
`flags`	Shows the current flag settings.
`general`	Shows system information.
`host`	Shows the current host configuration.
`master`	Identifies the current CP module slot configured as master and shows the current master configuration.
`running-config [verbose]`	Displays the current boot configuration. verbose includes all possible information. If you omit verbose, the system displays only the values that you changed from their default value.
`sio`	Specifies the current configuration of the CP module serial port.

©Avaya Inc. 2015 All Rights Reserved.

show brouter

Show brouter port information.

Syntax

- `show brouter`
- `show brouter <1-4084>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<1-4084>	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show cfm cmac

Displays the global CFM CMAC configuration for the C-VLAN.

Syntax

- `show cfm cmac`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show cfm maintenance-association

Display the Connectivity Fault Management (CFM) Maintenance-Association configuration. An MA represents a logical grouping of monitored entities within its Maintenance Domain.

Syntax

- `show cfm maintenance-association`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show cfm maintenance-domain

Display the Connectivity Fault Management (CFM) Maintenance-Domain configuration. A Maintenance-Domain is the part of a network that is controlled by a single administrator. A single MD may contain several Maintenance-Associations (MA).

Syntax

- `show cfm maintenance-domain`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show cfm maintenance-endpoint

Display the Connectivity Fault Management Maintenance Endpoint configuration. A Maintenance Endpoint (MEP) represents a managed CFM entity, associated with a specific Domain Service Access Point of a service instance, which can generate and receive CFM Protocol Data Units (PDUs) and track any responses. MEP functionality can be divided into the following functions: Fault Detection, Fault Verification, Fault Isolation and Fault Notification.

Syntax

- `show cfm maintenance-endpoint`

Default

None

Command mode

User EXEC

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

show cfm spbm

Displays the global CFM SPBM configuration for SPBM VLANs.

Syntax

- `show cfm spbm`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show cli info

Display information about the ACLI configuration.

Syntax

- `show cli info`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show clilog

Verify the configuration and view the log file. This command only applies to log files generated by releases prior to Release 3.2. The command is replaced by show logging file module clilog.

Syntax

- `show clilog`
- `show clilog file`
- `show clilog file grep WORD<1-256>`
- `show clilog file tail`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`file`	Shows the log file.
`grep WORD <1-256>`	Shows the last results first.
`tail`	Performs a string search in the log file. WORD <1-256> is the string, of up to 256 characters in length, to match.

©Avaya Inc. 2015 All Rights Reserved.

show cli password

Display the access, logon name, and password combinations.

Syntax

- `show cli password`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show clock

Show clock configurations.

Syntax

- `show clock`
- `show clock detail`
- `show clock time-zone`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`detail`	Displays detailed date information.
`time-zone`	Displays the local time-zone configuration.

©Avaya Inc. 2015 All Rights Reserved.

show core-files

Display the core files generated by the exception dump command.

Syntax

- `show core-files`
- `show core-files {slot [-slot][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot [-slot][,...]}`	Specifies the slot number to display the core files. Valid slots are 1 to 12, SF1 to SF6, and all.

©Avaya Inc. 2015 All Rights Reserved.

show debug-file

View all types of debug files for all slots or for specific slots.

Syntax

- `show debug-file`
- `show debug-file {slot[-slot][,...]}`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot[-slot][,...]}`	Shows debug files for one or more slots. You can specify a specific slot number , a range of slots, or use the value of all to view information for all slots.

©Avaya Inc. 2015 All Rights Reserved.

show debug ip pim

Shows Protocol Independent Multicast (PIM) debug configuration.

Syntax

- `show debug ip pim`
- `show debug ip pim vrf WORD<1-16>`
- `show debug ip pim vrfids WORD<0-512>`
- `show ip pim`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Displays the route for a particular VRF.
`vrfids WORD<0-512>`	Displays the route for a particular VRF ID.

©Avaya Inc. 2015 All Rights Reserved.

show eapol auth-diags interface

Display the Extensible Authentication Protocol (EAPoL) Authenticator diagnostics to manage network performance.

Syntax

- `show eapol auth-diags interface`
- `show eapol auth-diags interface gigabitethernet`
- `show eapol auth-diags interface gigabitethernet {slot/port [-slot/port][,...]}`
- `show eapol auth-diags interface vlan <1-4084>`
- `show eapol auth-diags interface vlan <1-4084>{slot/port [-slot/port][,...]}`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`gigabitethernet {slot/port [-slot/port][,...]}`	Specifies the type of interface displayed.
`vlan <1-4084>`	Specifies the VLAN for which to show the statistics.

©Avaya Inc. 2015 All Rights Reserved.

show eapol auth-stats interface

Display the Authenticator statistics to manage network performance.

Syntax

- `show eapol auth-stats interface`
- `show eapol auth-stats interface gigabitEthernet`
- `show eapol auth-stats interface gigabitEthernet {slot/port [-slot/port][,...]}`
- `show eapol auth-stats interface vlan <1-4084>`
- `show eapol auth-stats interface vlan <1-4084> slot/port[-slot/port][,...]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`gigabitethernet {slot/port [-slot/port][,...]}`	Specifies the type of interface displayed.
`vlan <1-4084>`	Specifies the VLAN for which to show the statistics.

©Avaya Inc. 2015 All Rights Reserved.

show eapol multihost-session-stats interface

Display the manage mode parameters for the specified interface type.

Syntax

- `show eapol multihost-session-stats interface`
- `show eapol multihost-session-stats interface gigabitEthernet [{slot/port[-slot/port][,...]}]`
- `show eapol multihost-session-stats interface vlan <1-4084>`
- `show eapol multihost-session-stats interface vlan <1-4084> [{slot/port[-slot/port][,...]}]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`gigabitethernet {slot/port [-slot/port][,...]}`	Specifies the type of interface displayed.
`vlan <1-4084>`	Specifies the VLAN for which to show the statistics.

©Avaya Inc. 2015 All Rights Reserved.

show eapol port

Display Extensible Authentication Protocol (EAPoL) information for the specified port or interface type.

Syntax

- `show eapol port {slot/port}`
- `show eapol port interface gigabitEthernet`
- `show eapol port interface gigabitEthernet {slot/port [-slot/port][,...]}`
- `show eapol port interface vlan <1-4084>`
- `show eapol port interface vlan <1-4084> [{slot/port [-slot/port][,...]}]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port}`	Identifies the slot and port.
`gigabitethernet {slot/port [-slot/port][,...]}`	Specifies the type of interface displayed.
`vlan <1-4084>`	Specifies the VLAN for which to show the statistics.

©Avaya Inc. 2015 All Rights Reserved.

show eapol session interface

View EAPoL session statistics to manage network performance.

Syntax

- `show eapol session interface [gigabitethernet {slot/port[-slot/port][,...]}] [vlan <1-4084>]`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`gigabitethernet {slot/port [-slot/port][,...]}`	Specifies the type of interface displayed.
`vlan <1-4084>`	Specifies the VLAN for which to show the statistics.

©Avaya Inc. 2015 All Rights Reserved.

show eapol session-stats interface

Display the port Extensible Authentication Protocol (EAPoL) authenticator session statistics for the specified interface type.

Syntax

- `show eapol session-stats interface`
- `show eapol session-stats interface gigabitethernet`
- `show eapol session-stats interface gigabitethernet {slot/port [-slot/port][,...]}`
- `show eapol session-stats interface vlan <1-4084>`
- `show eapol session-stats interface[vlan <1-4084>[{slot/port [-slot/port][,...]}]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`gigabitethernet {slot/port [-slot/port][,...]}`	Specifies the type of interface displayed.
`vlan <1-4084>`	Specifies the VLAN for which to show the statistics.

©Avaya Inc. 2015 All Rights Reserved.

show eapol status interface

Display the port Extensible Authentication Protocol (EAPoL) operation statistics for the specified interface type.

Syntax

- `show eapol status interface`
- `show eapol status interface gigabitEthernet`
- `show eapol status interface gigabitEthernet {slot/port[-slot/port][,...]}`
- `show eapol status interface vlan <1-4084>`
- `show eapol status interface vlan <1-4084> {slot/port[-slot/port][,...]}`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`gigabitethernet {slot/port [-slot/port][,...]}`	Specifies the type of interface displayed.
`vlan <1-4084>`	Specifies the VLAN for which to show the statistics.

©Avaya Inc. 2015 All Rights Reserved.

show eapol system

Display the current Extensible Authentication Protocol (EAPoL) setting on the switch.

Syntax

- `show eapol system`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show fabric

Display complete fabric information on the switch.

Syntax

- `show fabric [cp <1-2>|io <3-12>|sf <SF1|SF2|SF3|SF4|SF5|SF6>statistics cos <0-7>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`cp <1-2>`	Displays fabric information for the CP card. <1-2> specifies the CP slot number.
`io <3-12>`	Displays fabric information for the IO card. <3-12> specifies the IO slot number.
`sf <SF1|SF2|SF3|SF4|SF5|SF6>`	Displays fabric information for the SF card.
`statistics cos <0-7>`	Displays the fabric statistics. <0-7> specifies the cos ID.

©Avaya Inc. 2015 All Rights Reserved.

show fdb-filter

Show forwarding database filter information.

Syntax

- `show fdb-filter`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show filter acl

Display filter access control list (ACL) configuration information.

Syntax

- `show filter acl`
- `show filter acl <1-2048>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
<1-2048>	Specifies an access control list (ACL) ID from 1 to 2048.

©Avaya Inc. 2015 All Rights Reserved.

show filter acl ace

Display the filter access control list (ACL) access control entry (ACE) configuration information.

Syntax

- `show filter acl ace`
- `show filter acl ace <1-2048>`
- `show filter acl ace <1-2048> <1-2000>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
<1-2000>	Specifies an access control entry (ACE) ID from 1 to 2000.
<1-2048>	Specifies an access control list (ACL) ID from 1 to 2048.

©Avaya Inc. 2015 All Rights Reserved.

show filter acl action

Display the filter access control list (ACL) advanced information.

Syntax

- `show filter acl action`
- `show filter acl action <1-2048>`
- `show filter acl action <1-2048> <1-2000>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
<1-2000>	Specifies an access control entry (ACE) ID from 1 to 2000.
<1-2048>	Specifies an access control list (ACL) ID from 1 to 2048.

©Avaya Inc. 2015 All Rights Reserved.

show filter acl arp

Display the filter access control list (ACL) ARP operation configuration information.

Syntax

- `show filter acl arp`
- `show filter acl arp <1-2048>`
- `show filter acl arp <1-2048> <1-2000>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
<1-2000>	Specifies an access control entry (ACE) ID from 1 to 2000.
<1-2048>	Specifies an access control list (ACL) ID from 1 to 2048.

©Avaya Inc. 2015 All Rights Reserved.

show filter acl config

Review your configuration to ensure that it is correct.

Syntax

- `show filter acl config`
- `show filter acl config <1-2048>`
- `show filter acl config <1-2048> <1-2000>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
<1-2000>	Specifies an access control entry (ACE) ID from 1-2000.
<1-2048>	Specifies an access control list (ACL) ID from 1-2048.

©Avaya Inc. 2015 All Rights Reserved.

show filter acl ethernet

Display the filter access control list (ACL) Ethernet configuration information.

Syntax

- `show filter acl ethernet`
- `show filter acl ethernet <1-2048>`
- `show filter acl ethernet <1-2048> <1-2000>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
<1-2000>	Specifies an access control entry (ACE) ID from 1 to 2000.
<1-2048>	Specifies an access control list (ACL) ID from 1 to 2048.

©Avaya Inc. 2015 All Rights Reserved.

show filter acl ip

Display the filter access control list (ACL) IP configuration information.

Syntax

- `show filter acl ip`
- `show filter acl ip <1-2048>`
- `show filter acl ip <1-2048> <1-2000>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
<1-2000>	Specifies an access control entry (ACE) ID from 1 to 2000.
<1-2048>	Specifies an access control list (ACL) ID from 1 to 2048.

©Avaya Inc. 2015 All Rights Reserved.

show filter acl log

Display the filter access control list (ACL) debug configuration information.

Syntax

- `show filter acl log {slot/port}`
- `show filter acl log {slot/port} <1-2048>`
- `show filter acl log {slot/port} <1-2048> <1-2000>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-2000>`	Specifies an access control entry (ACE) ID from 1-2000.
`<1-2048>`	Specifies an access control list (ACL) ID from 1-2048.

©Avaya Inc. 2015 All Rights Reserved.

show filter acl protocol

Display the filter access control list (ACL) protocol configuration information.

Syntax

- `show filter acl protocol`
- `show filter acl protocol <1-2048>`
- `show filter acl protocol <1-2048> <1-2000>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
<1-2000>	Specifies an access control entry (ACE) ID from 1-2000.
<1-2048>	Specifies an access control list (ACL) ID from 1-2048.

©Avaya Inc. 2015 All Rights Reserved.

show filter acl statistics

View port statistics to ensure that the access control entry (ACE) operates correctly.

Syntax

- `show filter acl statistics`
- `show filter acl statistics <1-2048>`
- `show filter acl statistics <1-2048> <1-2000>`
- `show filter acl statistics <1-2048> qos`
- `show filter acl statistics <1-2048> security`
- `show filter acl statistics all`
- `show filter acl statistics default`
- `show filter acl statistics default <1-2048>`
- `show filter acl statistics global`
- `show filter acl statistics global <1-2048>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`<1-2048>`	Specifies access control list (ACL) ID.
`<1-2048> <1-2000>`	Specifies the access control list (ACL) and the ACE ID.
`<1-2048> qos`	Shows statistics for Quality of Service (QoS) access control entries.
`<1-2048> security`	Shows statistics for security access control entries.
`all`	Shows all statistics for all access control entries.
`default`	Shows traffic statistics for access control entry.
`global`	Shows global statistics for access control entry.

©Avaya Inc. 2015 All Rights Reserved.

show ftp-access

Show the maximum FTP sessions.

Syntax

- `show ftp-access`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show fulltech

Run all show commands and, optionally, capture the output to a file.

Syntax

- `show fulltech [file WORD<1-99>]`
- `show fulltech khi [file WORD<1-99>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`file WORD<1-99>`	Specifies the file name in the range of 1 to 99 for which you need the logs to be displayed. WORD<1-99> specifies the filename in the form /intflash/<file>| /extflash/<file>| /usb/<file>.

©Avaya Inc. 2015 All Rights Reserved.

show ha-state

Show the state of High Availability (HA) on the system.

Syntax

- `show ha-state`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show history

Shows a list of previously used commands. You can use this command in any mode, beginning with Privileged EXEC. The output shows the last 32 commands used in the active session.

Syntax

- `show history`

Default

None

Command mode

Privileged EXEC

©Avaya Inc. 2015 All Rights Reserved.

show hosts

Query the DNS host for information about host addresses. You can enter either a hostname or an IP address. If you enter the hostname, this command shows the IP address corresponding to the hostname and if you enter an IP address, this command shows the hostname for the IP address.

Syntax

- `show hosts WORD<0-256>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
WORD<0-256>	Specifies one of the following the name of the host DNS server as a string of 0-256 characters. the IP address of the host DNS server in a.b.c.d format. the IPv6 address of the host DNS server in hexadecimal format (string length 0-46).

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet

Show configuration information for GigabitEthernet ports.

Syntax

- `show interfaces gigabitEthernet`
- `show interfaces gigabitEthernet {slot/port[-slot/port][,...]}`
- `show interfaces gigabitEthernet {slot/port[-slot/port][,...]} <1-4084>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet config

Show the configuration for specific ports and VLANs to manage network performance.

Syntax

- `show interfaces gigabitEthernet config`
- `show interfaces gigabitEthernet config <1-4084>`
- `show interfaces gigabitEthernet config {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-4084>`	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet cp-limit

Show CP-Limit configuration information for the port .

Syntax

- `show interfaces gigabitEthernet cp-limit`
- `show interfaces gigabitEthernet cp-limit <1-4084>`
- `show interfaces gigabitEthernet cp-limit {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet error

Show general error information for the port.

Syntax

- `show interfaces gigabitEthernet error`
- `show interfaces gigabitEthernet error {slot/port[-slot/port][,...]}`
- `show interfaces gigabitEthernet error collision`
- `show interfaces gigabitEthernet error collision {slot/port[-slot/port][,...]}`
- `show interfaces gigabitEthernet error ospf`
- `show interfaces gigabitEthernet error ospf {slot/port[-slot/port][,...]}`
- `show interfaces gigabitEthernet error verbose`
- `show interfaces gigabitEthernet error verbose {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Specifies the slot and the port number or a range of ports.
`collision`	Show port collision error information.
`ospf`	Show port ospf error information.
`verbose`	Show port error information. Display priority-based flow control pause transmit and receive counter.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet fdb-entry

Show the forwarding database (FDB) entries for the port.

Syntax

- `show interfaces gigabitEthernet fdb-entry`
- `show interfaces gigabitEthernet fdb-entry <1-4084>`
- `show interfaces gigabitEthernet fdb-entry {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-4084>`	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet high-secure

Show the high-secure configuration for the port.

Syntax

- `show interfaces gigabitEthernet high-secure`
- `show interfaces gigabitEthernet high-secure <1-4084>`
- `show interfaces gigabitEthernet high-secure {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-4084>`	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet interface

Show general port information.

Syntax

- `show interfaces gigabitEthernet interface`
- `show interfaces gigabitEthernet interface <1-4084>`
- `show interfaces gigabitEthernet interface {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-4084>`	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet l1-config

Show Layer 1 configuration information for the port.

Syntax

- `show interfaces gigabitEthernet l1-config`
- `show interfaces gigabitEthernet l1-config <1-4084>`
- `show interfaces gigabitEthernet l1-config {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-4084>`	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet limit-fdb-learning

Show the configuration for the limit forwarding database (FDB) learning feature.

Syntax

- `show interfaces gigabitEthernet limit-fdb-learning`
- `show interfaces gigabitEthernet limit-fdb-learning <1-4084>`
- `show interfaces gigabitEthernet limit-fdb-learning {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-4084>`	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet loop-detected

Display loop detection information for the port.

Syntax

- `show interfaces gigabitEthernet loop-detected`
- `show interfaces gigabitEthernet loop-detected <1-4084>`
- `show interfaces gigabitEthernet loop-detected {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-4084>`	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet lossless-config

Display information on a port configured for Lossless Ethernet.

Syntax

- `show interfaces gigabitEthernet lossless-config`
- `show interfaces gigabitEthernet lossless-config {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`lossless-config {slot/port [-slot/port][,...]}`	Display information on a port configured for Lossless Ethernet. The parameter {slot/port[-slot/port][,...]} identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet mac-security

Show information about the unknown MAC discard feature for the port.

Syntax

- `show interfaces gigabitEthernet mac-security`
- `show interfaces gigabitEthernet mac-security <1-4084>`
- `show interfaces gigabitEthernet mac-security {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-4084>`	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet name

Show port names and general configuration information.

Syntax

- `show interfaces gigabitEthernet name`
- `show interfaces gigabitEthernet name <1-4084>`
- `show interfaces gigabitEthernet name {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-4084>`	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet ospf

Shows OSPF port information.

Syntax

- `show interfaces gigabitEthernet ospf`
- `show interfaces gigabitEthernet ospf <1-4084>`
- `show interfaces gigabitEthernet ospf {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-4084>`	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet rate-limit

Show rate-limit configuration information for the port.

Syntax

- `show interfaces gigabitEthernet rate-limit`
- `show interfaces gigabitEthernet rate-limit <1-4084>`
- `show interfaces gigabitEthernet rate-limit {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-4084>`	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet shape

Show the configuration for egress rate-limiting on the port.

Syntax

- `show interfaces gigabitEthernet shape`
- `show interfaces gigabitEthernet shape {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet slpp

Display the simple loop prevention protocol (SLPP) configuration information for the port.

Syntax

- `show interfaces gigabitEthernet slpp`
- `show interfaces gigabitEthernet slpp {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet state

Shows the state of the port.

Syntax

- `show interfaces gigabitEthernet state`
- `show interfaces gigabitEthernet state <1-4084>`
- `show interfaces gigabitEthernet state {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-4084>`	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet statistics

Display individual statistics for specific ports to manage network performance.

Syntax

- `show interfaces gigabitEthernet statistics`
- `show interfaces gigabitEthernet statistics {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Displays all statistics by port.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet statistics bridging

Display individual bridging statistics for specific ports to manage network performance.

Syntax

- `show interfaces gigabitEthernet statistics bridging`
- `show interfaces gigabitEthernet statistics bridging {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Displays all statistics by port.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet statistics dhcp-relay

Show Dynamic Host Configuration Protocol (DHCP) Relay information to view DHCP parameter information for one port, for all ports, or for a VLAN.

Syntax

- `show interfaces gigabitEthernet statistics dhcp-relay`
- `show interfaces gigabitEthernet statistics dhcp-relay {slot/port[-slot/port][,...]}`
- `show interfaces gigabitEthernet statistics dhcp-relay vrf WORD<1-16>`
- `show interfaces gigabitEthernet statistics dhcp-relay vrfids WORD<0-512>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Specifies the slot and the port number.
`vrf WORD<1-16>`	The name of the VRF. The range is 0 to 16.
`vrfids WORD<0-512>`	The ID of the VRF and is an integer. The range is 0-512.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet statistics lacp

Display individual Link Aggregation Control Protocol (LACP) statistics for specific ports to manage network performance.

Syntax

- `show interfaces gigabitEthernet statistics lacp`
- `show interfaces gigabitEthernet statistics lacp {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Displays all statistics by port.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet statistics policer

Display individual policer statistics for specific ports to manage network performance.

Syntax

- `show interfaces gigabitEthernet statistics policer`
- `show interfaces gigabitEthernet statistics policer {slot/port [-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Displays all statistics by port.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet statistics rmon

Display individual Remote Network Monitoring (RMON) statistics for specific ports to manage network performance.

Syntax

- `show interfaces gigabitEthernet statistics rmon`
- `show interfaces gigabitEthernet statistics rmon {slot/port[-slot/port][,...]}`
- `show interfaces gigabitEthernet statistics rmon history`
- `show interfaces gigabitEthernet statistics rmon history {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Displays all statistics by port.
`history`	Displays Remote Network Monitoring (RMON) history statistics.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet statistics verbose

Display individual verbose statistics for specific ports to manage network performance.

Syntax

- `show interfaces gigabitEthernet statistics verbose`
- `show interfaces gigabitEthernet statistics verbose {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Displays all statistics by port.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet vlan

Show VLAN information for the port.

Syntax

- `show interfaces gigabitEthernet vlan`
- `show interfaces gigabitEthernet vlan <1-4084>`
- `show interfaces gigabitEthernet vlan {slot/port[-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-4084>`	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces gigabitethernet vrfs

Show VRF-association information for the port..

Syntax

- `show interfaces gigabitEthernet vrfs`
- `show interfaces gigabitEthernet vrfs {slot/port[-slot/port][,...]}`
- `show interfaces gigabitEthernet vrfs vrf WORD<1-16>`
- `show interfaces gigabitEthernet vrfs vrfids WORD<0-512>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`vrf WORD<1-16>`	Specifies a VRF instance by name.
`vrfids WORD<0-512>`	Specifies a range of VRFs by ID number.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces loopback

Display the circuitless IP interface configuration information.

Syntax

- `show interfaces loopback`
- `show interfaces loopback vrf WORD<1-16>`
- `show interfaces loopback vrfids WORD<0-512>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Displays the loopback information for the associated VRF name. WORD<1-16> specifies the VRF name in the range of 1 to 16 characters.
`vrfids WORD<0-512>`	Displays the loopback configuration for the specified VRF IDs. WORD<0-512> specifies the VRF IDs in the range of 0 to 512.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces mgmtethernet

Show configuration information for MgmtEthernet ports.

Syntax

- `show interfaces mgmtethernet [{slot/port [-slot/port][,...]}]`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

show interfaces mgmtethernet config-L1

Show Layer 1 configuration information for the port.

Syntax

- `show interfaces mgmtethernet config-l1 [{slot/port [-slot/port][,...]}]`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

show interfaces mgmtethernet error

Show general error information for the port.

Syntax

- `show interfaces mgmtethernet error [{slot/port [-slot/port][,...]}]`
- `show interfaces mgmtethernet error collision [{slot/port [-slot/port][,...]}]`
- `show interfaces mgmtethernet error ospf [{slot/port [-slot/port][,...]}]`
- `show interfaces mgmtethernet error verbose [{slot/port [-slot/port][,...]}]`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Specifies the slot and the port number or a range of management ports.
`collision`	Shows management port collision error information.
`ospf`	Shows management port ospf error information.
`verbose`	Shows management port error information. Displays priority-based flow control pause transmit and receive counter.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces mgmtethernet statistics

Display individual statistics for specific management ports to manage network performance.

Syntax

- `show interfaces mgmtethernet statistics`
- `show interfaces mgmtethernet statistics {slot/port [-slot/port][,...]}`
- `show interfaces mgmtethernet statistics verbose [{slot/port [-slot/port][,...]}]`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Displays all statistics by management port.
`verbose {slot/port [-slot/port][,...]}`	Displays verbose statistics for specific management ports to manage network performance.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces vlan

Show basic and advanced VLAN information.

Syntax

- `show interfaces vlan [<1-4084>]`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
<1-4084>	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces vlan arp

Display Address Resolution Protocol (ARP) information for the VLAN.

Syntax

- `show interfaces vlan arp [<1-4084>]`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
<1-4084>	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces vlan autolearn-mac

Show bridging autolearn MAC address information for VLANs.

Syntax

- `show interfaces vlan autolearn-mac`

Default

None

Command mode

Privileged EXEC

©Avaya Inc. 2015 All Rights Reserved.

show interfaces vlan dhcp-relay

Show Dynamic Host Configuration Protocol (DHCP) information for the VLAN.

Syntax

- `show interfaces vlan dhcp-relay [<1-4084>]`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
<1-4084>	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces vlan igmp

Show Internet Group Management Protocol (IGMP) information for the VLAN.

Syntax

- `show interfaces vlan igmp [<1-4084>]`
- `show interfaces vlan igmp vrf WORD<1-32>`
- `show interfaces vlan igmp vrfids WORD<0-255>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`<1-4084>`	Specifies the VLAN ID.
`vrf WORD<1-32>`	Specifies the VRF name.
`vrfids WORD<0-255>`	Specifies the VRF ID.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces vlan igmp-mrdisc

Show Internet Group Management Protocol (IGMP) multicast route discovery information for the VLAN.

Syntax

- `show interfaces vlan igmp-mrdisc [<1-4084>]`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
<1-4084>	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces vlan ip

Show the IP configuration for the VLAN.

Syntax

- `show interfaces vlan ip [<1-4084>] [vrf WORD<1-16>] [vrfids WORD<0-512>]`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`<1-4084>`	Specifies the VLAN ID.
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids WORD<0-512>`	Specifies a range of VRF IDs.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces vlan manual-edit-mac

Display the manually-edited bridging MAC address information for VLANs.

Syntax

- `show interfaces vlan manual-edit-mac`

Default

None

Command mode

Privileged EXEC

©Avaya Inc. 2015 All Rights Reserved.

show interfaces vlan nlb-mode

Show the Network Load Balancer (NLB) configuration for the VLAN.

Syntax

- `show interfaces vlan nlb-mode [<1-4084>]`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
<1-4084>	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show interfaces vlan vlan-bysrcmac

Show source MAC-based VLAN information.

Syntax

- `show interfaces vlan vlan-bysrcmac`

Default

None

Command mode

Privileged EXEC

©Avaya Inc. 2015 All Rights Reserved.

show interfaces vlan vrfs

Show VRF-association information for the VLAN.

Syntax

- `show interfaces vlan vrfs [<1-4084>] [vrf WORD<1-16>] [vrfids WORD<0-512>] [{slot/port [-slot/port][,...]}]`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-4084>`	Specifies the VLAN ID.
`vrf WORD<1-16>`	Specifies a VRF instance by name.
`vrfids WORD<0-512>`	Specifies a range of VRFs by ID number.

©Avaya Inc. 2015 All Rights Reserved.

show interface vlan nlb-mode

Use the following command to view Network Load Balancing-mode (NLB-mode) information.

Syntax

- `show interface vlan nlb-mode <1-4084>`

Default

None

Command mode

VLAN Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

show ip arp

Show ARP information to view the configuration information in the ARP table.

Syntax

- `show ip arp`
- `show ip arp {A.B.C.D}`
- `show ip arp gigabitEthernet {slot/port}`
- `show ip arp gigabitEthernet {slot/port} vrf WORD<1-16>`
- `show ip arp gigabitEthernet {slot/port} vrfids WORD<0-512>`
- `show ip arp -s {A.B.C.D} {A.B.C.D}`
- `show ip arp spbm-tunnel-as-mac`
- `show ip arp vlan <1-4084>`
- `show ip arp vrf WORD<1-16>`
- `show ip arp vrfids WORD<0-512>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
{A.B.C.D}	Specifies the network IP address for the table.
<A.B.C.D>	Specifies the specific network IP address for the table.
gigabitEthernet	Displays the entries for a particular brouter port.
-s <A.B.C.D> <A.B.C.D>	Specifies the specific subnet for the table.
spbm-tunnel-as-mac	Displays the remote host name in the TUNNEL column for the SPBM ARP entry.
vlan	Displays ARP entries for a particular VLAN ID. Use these parameters to display ARP table information specifically for: vrf WORD<1-16> - the VLAN VRF name vrfids WORD<0-512> - the VLAN VRF ID.
vrf WORD<1-16>	Specifies the name of the VRF. The total number of ARPs listed in the summary line of the show ip arp display represents the total number of ARPs on the chassis including all VRFs (which includes the Mgmt Router VRF).
vrfids WORD<0-512>	Specifies the VRF ID. The total number of ARPs listed in the summary line of the show ip arp display represents the total number of ARPs on the chassis,

including all VRFs (which includes the Mgmt Router VRF).

©Avaya Inc. 2015 All Rights Reserved.

show ip arp interface

Show ARP port information to display data about the specified port, all ports, or the VLAN. Use this command to display loop-detect configurations.

Syntax

- `show ip arp interface [vlan <1-4084>]`
- `show ip arp interface gigabitethernet [{slot/port[-slot/port][,...]}]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-4084>`	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip arp static-mcastmac

Display Layer 3 multicast MAC ARP data.

Syntax

- `show ip arp static-mcastmac [-s <A.B.C.D/X>] [vrf WORD<1-16>] [vrfids WORD<0-512>] [<A.B.C.D>]`

Default

None

Command mode

User EXEC

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.

show ip as-list

Show the AS path lists on the Global Router.

Syntax

- `show ip as-list [<1-1024>] [vrf WORD<1-16>] [vrfids WORD<0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<1-1024>`	Specifies the list ID.
`vrf WORD<1-16>`	Specifies the name of the VRF.
`vrfids WORD<0-512>`	Specifies the VRF ID in the range of 0 to 512.

©Avaya Inc. 2015 All Rights Reserved.

show ip bgp aggregates

Display information about current aggregate addresses.

Syntax

- `show ip bgp aggregates [<prefix/len>] [vrf WORD<1-16>] [vrfids WORD<0-255>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<prefix/len>`	Specifies the IP address and the mask length (the length can be 0 to 32).
`vrf WORD<1-16>`	Specifies a VRF instance by name.
`vrfids WORD <0-512>`	Specifies a range of VRFs by ID number.

©Avaya Inc. 2015 All Rights Reserved.

show ip bgp cidr-only

Display information about classless interdomain routing (CIDR) routes.

Syntax

- `show ip bgp cidr-only [<prefix/len>] [vrf WORD<1-16>] [vrfids WORD<0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<prefix/len>`	Specifies an exact match of the prefix. This is an IP address and an integer value between 0 and 32 in the format a.b.c.d/xx.
`vrf WORD<1-16>`	Specifies a VRF instance by name.
`vrfids WORD<0-512>`	Specifies a range of VRFs by ID number.

©Avaya Inc. 2015 All Rights Reserved.

show ip bgp conf

View BGP configuration information on the switch.

Syntax

- `show ip bgp conf [vrf WORD< 1-16>] [vrfids WORD<0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF instance by name.
`vrfids WORD<0-512>`	Specifies a range of VRFs by ID number.

©Avaya Inc. 2015 All Rights Reserved.

show ip bgp confederation

View BGP confederation information on the switch.

Syntax

- `show ip bgp confederation`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ip bgp dampened-paths

Display information about flap-dampened routes to determine unreliable routes.

Syntax

- `show ip bgp dampened-paths <A.B.C.D> [<prefix/len>] [longer-prefixes] [vrf WORD<1-16>] [vrfids WORD<0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<prefix/len>`	Shows paths with this prefix. The prefix is the IP address and exact mask length (must be an integer value between 0 and 32).
`longer-prefixes`	Shows long prefixes. The longer-prefixes indicate the mask length from any specified prefix to 32 (for example, show from prefix a.b.c.d/len to a.b.c./32).
`vrf WORD<1-16>`	Specifies a VRF instance by name.
`vrfids WORD<0-512>`	Specifies a range of VRFs by ID number.

©Avaya Inc. 2015 All Rights Reserved.

show ip bgp flap-damp-config

Display global information about flap-dampening.

Syntax

- `show ip bgp flap-damp-config [<prefix/len>] [vrf WORD<1-16>] [vrfids WORD<0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`[<prefix/len>]`	Specifies the exact match the prefix {a,b,c,d/len}.
`vrf WORD<1-16>`	Displays BGP configuration for a particular VRF.
`vrfids WORD<0-512>`	Specifies the VRF ID in the range of 0 to 512.

©Avaya Inc. 2015 All Rights Reserved.

show ip bgp imported-routes

Display information about BGP imported routes.

Syntax

- `show ip bgp imported-routes [<prefix/len>][longer-prefixes] [vrf WORD<1-16>] [vrfids WORD<0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<prefix/len>`	Shows paths with this prefix. The prefix is the IP address and exact mask length (must be an integer value between 0 and 32).
`longer-prefixes`	Shows long prefixes. The longer-prefixes indicate the mask length from any specified prefix to 32 (for example, show from prefix a.b.c.d/len to a.b.c./32).
`vrf WORD<1-16>`	Specifies a VRF instance by name.
`vrfids WORD<0-512>`	Specifies a range of VRFs by ID number.

©Avaya Inc. 2015 All Rights Reserved.

show ip bgp neighbors

Display information about BGP peer advertised routes, peer routes, and IP VPN BGP peers.

Syntax

- `show ip bgp neighbors [{A.B.C.D}] [advertised-routes][<prefix/len>] [vrf WORD<1-16>] [vrfids WORD<0-512>]`
- `show ip bgp neighbors [{A.B.C.D}][vrf WORD<1-16>][vrfids WORD<0-512>]`
- `show ip bgp neighbors {A.B.C.D} routes [<prefix/len>][community <disable|enable>] [longer-prefixes] [vrf WORD<1-16>] [vrfids WORD<0-512>]`
- `show ip bgp neighbors {A.B.C.D} stats [vrf WORD<1-16>][vrfids WORD<0-512>]`
- `show ip bgp neighbors {A.B.C.D} vpnv4 [<prefix/len>][community <disable|enable>] [ext-community][longer-prefixes] [vrf WORD<1-16>] [vrfids WORD<0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<prefix/len>	Shows paths with this prefix. The prefix is the IP address and exact mask length (must be an integer value between 0 and 32).
advertised-routes	Displays information about BGP peer advertised routes.
community	Enables the display of community attributes.
ext-community	Enables the display of extended community attributes.
longer-prefixes	Shows long prefixes. The longer-prefixes indicate the mask length from any specified prefix to 32 (for example, show from prefix a.b.c.d/len to a.b.c.d/32).
routes	Displays information about BGP peer routes.
stats	Displays statistics information for BGP peers.
vpnv4	Displays information about IP VPN BGP peers.
vrf WORD<1-16>	Specifies a VRF instance by name.
vrfids WORD<0-512>	Specifies a range of VRFs by ID number.

©Avaya Inc. 2015 All Rights Reserved.

show ip bgp networks

Display information about BGP network configurations.

Syntax

- `show ip bgp networks [<prefix/len>] [vrf WORD<1-16>] [vrfids WORD<0-255>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<prefix/len>`	Shows networks with this prefix. The prefix is the IP address and exact mask length (must be an integer value between 0 and 32).
`vrf WORD<1-16>`	Specifies a VRF instance by name.
`vrfids WORD<0-255>`	Specifies a range of VRFs by ID number.

©Avaya Inc. 2015 All Rights Reserved.

show ip bgp peer-group

Display information about BGP peer groups.

Syntax

- `show ip bgp peer-group [WORD<0-1536>] [vrf WORD<1-16>] [vrfids WORD<0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF instance by name.
`vrfids WORD<0-512>`	Specifies a range of VRFs by ID number.
`WORD<0-1536>`	Specifies the name of the peer group.

©Avaya Inc. 2015 All Rights Reserved.

show ip bgp redistributed-routes

View BGP redistribution information on the switch.

Syntax

- `show ip bgp redistributed-routes <prefix/len> vrf WORD<1-16> vrfids WORD<0-512>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<prefix/len>`	Shows paths with this prefix. The prefix is the IP address and exact mask length (must be an integer value between 0 and 32).
`vrf WORD<1-16>`	Specifies a VRF instance by name.
`vrfids WORD<0-512>`	Specifies a range of VRFs by ID number.

©Avaya Inc. 2015 All Rights Reserved.

show ip bgp route

Display information about BGP routes.

Syntax

- `show ip bgp route [<prefix/len>] [longer-prefixes][community <enable|disable>] [ip <A.B.C.D>][vrf WORD<1-16>] [vrfids WORD<0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<prefix/len>`	Shows paths with this prefix. The prefix is the IP address and exact mask length (must be an integer value between 0 and 32).
`community <enable|disable>`	Enables or disables the display of community attributes.
`ip <A.B.C.D>`	Specifies an IP address.
`longer-prefixes`	Shows long prefixes. The longer-prefixes indicate the mask length from any specified prefix to 32 (for example, show from prefix a.b.c.d/len to a.b.c./32).
`vrf WORD<1-16>`	Specifies a VRF instance by name.
`vrfids WORD<0-512>`	Specifies a range of VRFs by ID number.

©Avaya Inc. 2015 All Rights Reserved.

show ip bgp stats

View Border Gateway Protocol (BGP) statistics.

Syntax

- `show ip bgp stats`
- `show ip bgp stats vrf WORD<1-16>`
- `show ip bgp stats vrf WORD<1-16> vrfids WORD<0-512>`
- `show ip bgp stats vrfids WORD<0-512>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF instance by name.
`vrfids WORD<0-512>`	Specifies a range of VRFs by ID number.

©Avaya Inc. 2015 All Rights Reserved.

show ip bgp summary

Display summarized information about Border Gateway Protocol (BGP).

Syntax

- `show ip bgp summary [vrf WORD<1-16>] [vrfids WORD<0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF instance by name.
`vrfids WORD <0-512>`	Specifies a range of VRFs by ID number.

©Avaya Inc. 2015 All Rights Reserved.

show ip bgp vpnv4

Display information about IP VPN routes.

Syntax

- `show ip bgp vpnv4 [<prefix/len>] [longer-prefixes][community] [ext-community] [ip {A.B.C.D}][vrf WORD<1-16>][vrfids WORD<0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<prefix/len>`	Shows paths with this prefix. The prefix is the IP address and exact mask length (must be an integer value between 0 and 32).
`community`	Enables the display of community attributes.
`ext-community`	Enables the display of extended community attributes.
`ip {A.B.C.D}`	Specifies the IP address.
`longer-prefixes`	Shows long prefixes. The longer-prefixes indicate the mask length from any specified prefix to 32 (for example, show from prefix a.b.c.d/len to a.b.c./32).
`vrf WORD<1-16>`	Specifies a VRF instance by name.
`vrfids WORD<0-512>`	Specifies a range of VRFs by ID number.

©Avaya Inc. 2015 All Rights Reserved.

show ip community-list

Show the community lists on the Global Router.

Syntax

- `show ip community-list [<1-1024>] [vrf WORD<1-16>] [vrfids WORD<0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<1-1024>`	Specifies the list ID.
`vrf WORD<1-16>`	Specifies the name of the VRF.
`vrfids WORD<0-512>`	Specifies the VRF ID in the range of 0 to 512.

©Avaya Inc. 2015 All Rights Reserved.

show ip dhcp-relay

Display relay information to show relay information about Dynamic Host Configuration Protocol (DHCP) routes and counters.

Syntax

- `show ip dhcp-relay counters [option82] [vrf WORD<1-16>] [vrfids <0-512>]`
- `show ip dhcp-relay fwd-path [vrf WORD<1-16>] [vrfids <0-512>]`
- `show ip dhcp-relay interface [vrf WORD<1-16>] [vrfids <0-512>]`
- `show ip dhcp-relay interface gigabitethernet [{slot/port[-slot/port][,...]}][<1-4084>] [vrf WORD<1-16>] [vrfids <0-512>]`
- `show ip dhcp-relay interface vlan [<1-4084>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
counters	Displays the count of DHCP Relay requests and replies.
fwd-path	Displays information about DHCP Relay forward paths.
gigabitethernet {slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
interface	Specifies the interface.
option82	Shows statistics for the relay agent option.
vlan <1-4084>	Specifies the VLAN ID.
vrf WORD<1-16>	Specifies the name of the VRF.
vrfids <0-512>	Specifies the ID of the VRF. The value is an integer in the range of 0 to 512.

©Avaya Inc. 2015 All Rights Reserved.

show ip directed-broadcast

Show the interface status for direct broadcast.

Syntax

- `show ip directed-broadcast interface [GigabitEthernet]`
- `show ip directed-broadcast interface GigabitEthernet [{slot/port}]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot[-slot][,...]}`	Identifies the slot in one of the following formats: a single slot (3), a range of slots (3-4), or a series of slots (3,5,6).

©Avaya Inc. 2015 All Rights Reserved.

show ip dns

View the DNS client system status.

Syntax

- `show ip dns`

Default

None

Command mode

User EXEC

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

show ip ecmp

Display the prefix list of routes with number of ECMP paths.

Syntax

- show ip ecmp max-path
- show ip ecmp max-path vrf WORD<1-16>
- show ip ecmp max-path vrf WORD<1-16> vrfids WORD<0-512>
- show ip ecmp max-path vrfids WORD<0-512>
- show ip ecmp pathlist-1
- show ip ecmp pathlist-1 vrf WORD<1-16>
- show ip ecmp pathlist-1 vrfids WORD<0-512>
- show ip ecmp pathlist-2
- show ip ecmp pathlist-2 vrf WORD<1-16>
- show ip ecmp pathlist-2 vrfids WORD<0-512>
- show ip ecmp pathlist-3
- show ip ecmp pathlist-3 vrf WORD<1-16>
- show ip ecmp pathlist-3 vrfids WORD<0-512>
- show ip ecmp pathlist-4
- show ip ecmp pathlist-4 vrf WORD<1-16>
- show ip ecmp pathlist-4 vrfids WORD<0-512>
- show ip ecmp pathlist-5
- show ip ecmp pathlist-5 vrf WORD<1-16>
- show ip ecmp pathlist-5 vrfids WORD<0-512>
- show ip ecmp pathlist-6
- show ip ecmp pathlist-6 vrf WORD<1-16>
- show ip ecmp pathlist-6 vrfids WORD<0-512>
- show ip ecmp pathlist-7
- show ip ecmp pathlist-7 vrf WORD<1-16>
- show ip ecmp pathlist-7 vrfids WORD<0-512>
- show ip ecmp pathlist-8

- `show ip ecmp pathlist-8 vrf WORD<1-16>`
- `show ip ecmp pathlist-8 vrfids WORD<0-512>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`max-path`	Configures the maximum number of Equal Cost Multipath (ECMP) paths.
`vrf WORD<1-16>`	Displays the prefix list of routes for a particular VRF. WORD<1-16> specifies the VRF name.
`vrfids WORD<0-512>`	Displays the prefix list of routes for a particular VRF ID. WORD<0-512> specifies the VRF ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip extcommunity-list

Show extended community list information.

Syntax

- `show ip extcommunity-list`
- `show ip extcommunity-list <1-1024>`
- `show ip extcommunity-list <1-1024> vrf WORD<1-16>`
- `show ip extcommunity-list <1-1024> vrfids WORD<0-512>`
- `show ip extcommunity-list vrf WORD<1-16>`
- `show ip extcommunity-list WORD<0-512>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<1-1024>`	Specifies the extended community list ID.
`vrf WORD<1-16>`	Displays extended community list for a particular VRF.
`vrfids WORD<0-512>`	Specifies VRF IDs.

©Avaya Inc. 2015 All Rights Reserved.

show ip forward-protocol udp

Display the UDP protocol table with the UDP port numbers for each supported or designated protocol.

Syntax

- `show ip forward-protocol udp [vrf WORD<1-16>] [vrfids <0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`interface <A.B.C.D>`	Displays information about the UDP interface for all IP addresses or a specified IP address.
`portfwd`	Displays the UDP port forwarding table.
`portfwdlist <1-1000>`	Displays the UDP port forwarding list table for the specified list or all lists on the switch. <1-1000> specifies the port forward list ID.
`vrf WORD<1-16>`	Specifies the name of the VRF in the range of 0 to 16 characters.
`vrfids <0-512>`	Specifies the ID of the VRF and is an integer in the range of 0 to 512.

©Avaya Inc. 2015 All Rights Reserved.

show ip forward-protocol udp portfwd

View and confirm the port forward entry configuration.

Syntax

- `show ip forward-protocol udp portfwd [vrf WORD<1-16>][vrfids <0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies the name of the VRF in the range of 0 to 16 characters.
`vrfids <0-512>`	Specifies the ID of VRF and is an integer between 0 and 512.

©Avaya Inc. 2015 All Rights Reserved.

show ip forward-protocol udp portfwdlist

View and confirm the configuration setting on the IP forwarding list.

Syntax

- `show ip forward-protocol udp portfwdlist <1-1000> [vrf WORD<1-16>] [vrfids <0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<1-1000>`	Specifies the port forward list id which is an integer in the range of 1 to 1000.
`vrf WORD<1-16>`	Specifies the name of the VRF in the range of 0 to 16 characters.
`vrfids <0-512>`	Specifies the ID of the VRF and is an integer in the range of 0 to 512.

©Avaya Inc. 2015 All Rights Reserved.

show ip igmp access

Displays information about the Internet Group Management Protocol (IGMP) multicast access control groups. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

Syntax

- `show ip igmp access`
- `show ip igmp access vrf WORD<1-16>`
- `show ip igmp access vrfids WORD<0-512>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids <0-512>`	Specifies a VRF by ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip igmp cache

Displays information about the IGMP cache. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

Syntax

- `show ip igmp cache`
- `show ip igmp cache vrf WORD<1-16>`
- `show ip igmp cache vrfids WORD<0-512>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids <0-512>`	Specifies a VRF by ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip igmp group

Displays information about a statically configured or dynamically learned IGMP group. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

Syntax

- `show ip igmp group`
- `show ip igmp group vrf WORD<1-16>`
- `show ip igmp group vrfids WORD<0-512>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids <0-512>`	Specifies a VRF by ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip igmp group count

Displays the number of entries in the IGMP group. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

Syntax

- `show ip igmp group count`
- `show ip igmp group count vrf WORD<1-16>`
- `show ip igmp group count vrfids WORD<0-512>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids <0-512>`	Specifies a VRF by ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip igmp group count group <A.B.C.D>

Displays the number of entries in the IGMP group for a specific group address. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

Syntax

- `show ip igmp group count group {A.B.C.D}`

Default

None

Command mode

Privileged EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ip igmp group group <A.B.C.D>

Displays information for a specific group address. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

Syntax

- `show ip igmp group group {A.B.C.D}`
- `show ip igmp group group {A.B.C.D} detail`
- `show ip igmp group group {A.B.C.D} detail port {slot/port[-slot/port][,...]}`
- `show ip igmp group group {A.B.C.D} detail port {slot/port[-slot/port][,...]} vlan <1-4084>`
- `show ip igmp group group {A.B.C.D} detail port {slot/port[-slot/port][,...]} vrf WORD<1-16>`
- `show ip igmp group group {A.B.C.D} detail port {slot/port[-slot/port][,...]} vrfids WORD<0-512>`
- `show ip igmp group group {A.B.C.D} detail vlan <1-4084>`
- `show ip igmp group group {A.B.C.D} detail vlan <1-4084> port {slot/port[-slot/port][,...]}`
- `show ip igmp group group {A.B.C.D} detail vrf WORD<1-16>`
- `show ip igmp group group {A.B.C.D} detail vrfids WORD<0-512>`
- `show ip igmp group group {A.B.C.D} vrf WORD<1-16>`
- `show ip igmp group group {A.B.C.D} vrfids WORD<0-512>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`detail`	Displays Internet Group Management Protocol version 3 (IGMPv3)-specific data
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`vlan <1-4084>`	Specifies a VLAN ID.
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids <0-512>`	Specifies a VRF by ID.

NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

show ip igmp group group <A.B.C.D> tracked-members

Displays all the tracked members for a specific group. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

Syntax

- `show ip igmp group group {A.B.C.D} tracked-members`
- `show ip igmp group group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X}`
- `show ip igmp group group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]}`
- `show ip igmp group group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]} source-subnet {A.B.C.D/X}`
- `show ip igmp group group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]} source-subnet {A.B.C.D/X} vlan <1-4084>`
- `show ip igmp group group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]} source-subnet {A.B.C.D/X} vrf WORD<1-16>`
- `show ip igmp group group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]} source-subnet {A.B.C.D/X} vrfids WORD<0-512>`
- `show ip igmp group group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]} vlan <1-4084>`
- `show ip igmp group group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]} vlan <1-4084> source-subnet {A.B.C.D/X}`
- `show ip igmp group group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]} vrf WORD<1-16>`
- `show ip igmp group group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]} vrfids WORD<0-512>`
- `show ip igmp group group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X} source-subnet {A.B.C.D/X}`
- `show ip igmp group group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X} source-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]}`
- `show ip igmp group group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X} source-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]} vlan <1-4084>`
- `show ip igmp group group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X} source-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]} vrf WORD<1-16>`
- `show ip igmp group group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X} source-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]} vrfids WORD<0-512>`
- `show ip igmp group group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X} source-subnet {A.B.C.D/X} vlan <1-4084>`
- `show ip igmp group group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X} source-subnet {A.B.C.D/X} vlan <1-4084> port {slot/port[-slot/port][,...]}`

- show ip igmp group group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X} source-subnet {A.B.C.D/X} vrf WORD<1-16>
- show ip igmp group group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X} source-subnet {A.B.C.D/X} vrfids WORD<0-512>
- show ip igmp group group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X} vlan <1-4084>
- show ip igmp group group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X} vlan <1-4084> port {slot/port[-slot/port][,...]}
- show ip igmp group group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X} vlan <1-4084> port {slot/port[-slot/port][,...]} source-subnet {A.B.C.D/X}
- show ip igmp group group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X} vlan <1-4084> source-subnet {A.B.C.D/X}
- show ip igmp group group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X} vlan <1-4084> source-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]}
- show ip igmp group group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X} vrf WORD<1-16>
- show ip igmp group group {A.B.C.D} tracked-members member-subnet {A.B.C.D/X} vrfids WORD<0-512>
- show ip igmp group group {A.B.C.D} tracked-members port {slot/port[-slot/port][,...]}
- show ip igmp group group {A.B.C.D} tracked-members port {slot/port[-slot/port][,...]} member-subnet {A.B.C.D/X}
- show ip igmp group group {A.B.C.D} tracked-members port {slot/port[-slot/port][,...]} member-subnet {A.B.C.D/X} source-subnet {A.B.C.D/X}
- show ip igmp group group {A.B.C.D} tracked-members port {slot/port[-slot/port][,...]} member-subnet {A.B.C.D/X} source-subnet {A.B.C.D/X} vlan <1-4084>
- show ip igmp group group {A.B.C.D} tracked-members port {slot/port[-slot/port][,...]} member-subnet {A.B.C.D/X} source-subnet {A.B.C.D/X} vrf WORD<1-16>
- show ip igmp group group {A.B.C.D} tracked-members port {slot/port[-slot/port][,...]} member-subnet {A.B.C.D/X} source-subnet {A.B.C.D/X} vrfids WORD<0-512>
- show ip igmp group group {A.B.C.D} tracked-members port {slot/port[-slot/port][,...]} member-subnet {A.B.C.D/X} vlan <1-4084>
- show ip igmp group group {A.B.C.D} tracked-members port {slot/port[-slot/port][,...]} member-subnet {A.B.C.D/X} vlan <1-4084> source-subnet {A.B.C.D/X}
- show ip igmp group group {A.B.C.D} tracked-members port {slot/port[-slot/port][,...]} member-subnet {A.B.C.D/X} vrf WORD<1-16>
- show ip igmp group group {A.B.C.D} tracked-members port {slot/port[-slot/port][,...]} member-subnet {A.B.C.D/X} vrfids WORD<0-512>
- show ip igmp group group {A.B.C.D} tracked-members port {slot/port[-slot/port][,...]} source-subnet {A.B.C.D/X}
- show ip igmp group group {A.B.C.D} tracked-members port {slot/port[-slot/port][,...]} source-subnet {A.B.C.D/X} member-subnet {A.B.C.D/X}
- show ip igmp group group {A.B.C.D} tracked-members port {slot/port[-slot/port][,...]} source-subnet {A.B.C.D/X} member-subnet {A.B.C.D/X} vlan <1-4084>
- show ip igmp group group {A.B.C.D} tracked-members port {slot/port[-slot/port][,...]} source-subnet {A.B.C.D/X} member-subnet {A.B.C.D/X} vrf WORD<1-16>
- show ip igmp group group {A.B.C.D} tracked-members port {slot/port[-slot/port][,...]} source-subnet {A.B.C.D/X} member-subnet {A.B.C.D/X} vrfids WORD<0-512>
- show ip igmp group group {A.B.C.D} tracked-members port {slot/port[-slot/port][,...]} source-subnet {A.B.C.D/X} vlan <1-4084>

show ip igmp group group {A.B.C.D} tracked-members port {slot/port[-slot/port][,...]} source-subnet {A.B.C.D/X} vlan <1-4084> member-subnet {A.B.C.D/X}

- show ip igmp group group {A.B.C.D} tracked-members port {slot/port[-slot/port][,...]} source-subnet {A.B.C.D/X} vrf WORD<1-16>
- show ip igmp group group {A.B.C.D} tracked-members port {slot/port[-slot/port][,...]} source-subnet {A.B.C.D/X} vrfids WORD<0-512>
- show ip igmp group group {A.B.C.D} tracked-members port {slot/port[-slot/port][,...]} vlan <1-4084>
- show ip igmp group group {A.B.C.D} tracked-members port {slot/port[-slot/port][,...]} vlan <1-4084> member-subnet {A.B.C.D/X}
- show ip igmp group group {A.B.C.D} tracked-members port {slot/port[-slot/port][,...]} vlan <1-4084> member-subnet {A.B.C.D/X} source-subnet {A.B.C.D/X}
- show ip igmp group group {A.B.C.D} tracked-members port {slot/port[-slot/port][,...]} vlan <1-4084> source-subnet {A.B.C.D/X}
- show ip igmp group group {A.B.C.D} tracked-members port {slot/port[-slot/port][,...]} vlan <1-4084> source-subnet {A.B.C.D/X} member-subnet {A.B.C.D/X}
- show ip igmp group group {A.B.C.D} tracked-members port {slot/port[-slot/port][,...]} vrf WORD<1-16>
- show ip igmp group group {A.B.C.D} tracked-members port {slot/port[-slot/port][,...]} vrfids WORD<0-512>
- show ip igmp group group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X}
- show ip igmp group group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} member-subnet {A.B.C.D/X}
- show ip igmp group group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} member-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]}
- show ip igmp group group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} member-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]} vlan <1-4084>
- show ip igmp group group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} member-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]} vrf WORD<1-16>
- show ip igmp group group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} member-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]} vrfids WORD<0-512>
- show ip igmp group group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} member-subnet {A.B.C.D/X} vlan <1-4084>
- show ip igmp group group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} member-subnet {A.B.C.D/X} vlan <1-4084> port {slot/port[-slot/port][,...]}
- show ip igmp group group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} member-subnet {A.B.C.D/X} vrf WORD<1-16>
- show ip igmp group group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} member-subnet {A.B.C.D/X} vrfids WORD<0-512>
- show ip igmp group group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]}
- show ip igmp group group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]} member-subnet {A.B.C.D/X}
- show ip igmp group group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]} member-subnet {A.B.C.D/X} vlan <1-4084>
- show ip igmp group group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]} member-subnet {A.B.C.D/X} vrf WORD<1-16>
- show ip igmp group group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]} member-subnet {A.B.C.D/X} vrfids WORD<0-512>

- show ip igmp group group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]} vlan <1-4084>
- show ip igmp group group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]} vlan <1-4084> member-subnet {A.B.C.D/X}
- show ip igmp group group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]} vrf WORD<1-16>
- show ip igmp group group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]} vrfids WORD<0-512>
- show ip igmp group group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} vlan <1-4084>
- show ip igmp group group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} vlan <1-4084> member-subnet {A.B.C.D/X}
- show ip igmp group group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} vlan <1-4084> member-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]}
- show ip igmp group group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} vlan <1-4084> port {slot/port[-slot/port][,...]}
- show ip igmp group group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} vlan <1-4084> port {slot/port[-slot/port][,...]} member-subnet {A.B.C.D/X}
- show ip igmp group group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} vrf WORD<1-16>
- show ip igmp group group {A.B.C.D} tracked-members source-subnet {A.B.C.D/X} vrfids WORD<0-512>
- show ip igmp group group {A.B.C.D} tracked-members vlan <1-4084>
- show ip igmp group group {A.B.C.D} tracked-members vlan <1-4084> member-subnet {A.B.C.D/X}
- show ip igmp group group {A.B.C.D} tracked-members vlan <1-4084> member-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]}
- show ip igmp group group {A.B.C.D} tracked-members vlan <1-4084> member-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]} source-subnet {A.B.C.D/X}
- show ip igmp group group {A.B.C.D} tracked-members vlan <1-4084> member-subnet {A.B.C.D/X} source-subnet {A.B.C.D/X}
- show ip igmp group group {A.B.C.D} tracked-members vlan <1-4084> member-subnet {A.B.C.D/X} source-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]}
- show ip igmp group group {A.B.C.D} tracked-members vlan <1-4084> port {slot/port[-slot/port][,...]}
- show ip igmp group group {A.B.C.D} tracked-members vlan <1-4084> port {slot/port[-slot/port][,...]} member-subnet {A.B.C.D/X}
- show ip igmp group group {A.B.C.D} tracked-members vlan <1-4084> port {slot/port[-slot/port][,...]} member-subnet {A.B.C.D/X} source-subnet {A.B.C.D/X}
- show ip igmp group group {A.B.C.D} tracked-members vlan <1-4084> port {slot/port[-slot/port][,...]} source-subnet {A.B.C.D/X}
- show ip igmp group group {A.B.C.D} tracked-members vlan <1-4084> port {slot/port[-slot/port][,...]} source-subnet {A.B.C.D/X} member-subnet {A.B.C.D/X}
- show ip igmp group group {A.B.C.D} tracked-members vlan <1-4084> source-subnet {A.B.C.D/X}
- show ip igmp group group {A.B.C.D} tracked-members vlan <1-4084> source-subnet {A.B.C.D/X} member-subnet {A.B.C.D/X}
- show ip igmp group group {A.B.C.D} tracked-members vlan <1-4084> source-subnet {A.B.C.D/X} member-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]}
- show ip igmp group group {A.B.C.D} tracked-members vlan <1-4084> source-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]}

- `show ip igmp group group {A.B.C.D} tracked-members vlan <1-4084> source-subnet {A.B.C.D/X} port {slot/port[-slot/port][,...]} member-subnet {A.B.C.D/X}`
- `show ip igmp group group {A.B.C.D} tracked-members vrf WORD<1-16>`
- `show ip igmp group group {A.B.C.D} tracked-members vrfids WORD<0-512>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`member-subnet {A.B.C.D/X}`	Specifies the IP address and mask of the IGMP member.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`source-subnet {A.B.C.D/X}`	Specifies the source IP address and the subnet mask.
`vlan <1-4084>`	Specifies a VLAN ID.
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids <0-512>`	Specifies a VRF by ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip igmp group member-subnet

Displays information for a specific IP address and mask of the IGMP member. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

Syntax

- `show ip igmp group member-subnet {A.B.C.D/X}`
- `show ip igmp group member-subnet {A.B.C.D/X} vrf WORD<1-16>`
- `show ip igmp group member-subnet {A.B.C.D/X} vrfids WORD<0-512>`
- `show ip igmp group member-subnet default`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
{A.B.C.D/X}	Specifies the IP address and mask of the IGMP member.
default	Shows information for the default IP address.
vrf WORD<1-16>	Specifies a VRF by name.
vrfids <0-512>	Specifies a VRF by ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip igmp interface

Displays information about the interfaces where Internet Group Management Protocol (IGMP) is enabled. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

Syntax

- `show ip igmp interface`
- `show ip igmp interface gigabitethernet`
- `show ip igmp interface gigabitethernet <1-4084>`
- `show ip igmp interface gigabitethernet {slot/port[-slot/port][,...]}`
- `show ip igmp interface vlan`
- `show ip igmp interface vlan <1-4084>`
- `show ip igmp interface vlan vrf WORD<1-16>`
- `show ip igmp interface vlan vrfids WORD<0-512>`
- `show ip igmp interface vrf WORD<1-16>`
- `show ip igmp interface vrfids WORD<0-512>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`<1-4084>`	Specifies the VLAN ID.
`gigabitethernet {slot/port[-slot/port][,...]}`	Specifies the port.
`interface`	Shows Internet Group Management Protocol (IGMP) interfaces.
`vlan <1-4084>`	Specifies the VLAN ID.
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids <0-512>`	Specifies a VRF by ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip igmp mrdisc

Displays information about the Internet Group Management Protocol (IGMP) multicast discovery routes. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

Syntax

- `show ip igmp mrdisc`
- `show ip igmp mrdisc vrf WORD<1-16>`
- `show ip igmp mrdisc vrfids WORD<0-512>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids <0-512>`	Specifies a VRF by ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip igmp mrdisc neighbors

Display information about the Internet Group Management Protocol (IGMP) multicast router discovery neighbors. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

Syntax

- `show ip igmp mrdisc neighbors`
- `show ip igmp mrdisc neighbors vrf WORD<1-16>`
- `show ip igmp mrdisc neighbors vrfids WORD<0-512>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids <0-512>`	Specifies a VRF by ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip igmp router-alert

Display the status of Internet Group Management Protocol (IGMP) router alert. If you do not specify a VRF name or range of VRF IDs, the results show information for the Global Router. If you do specify a VRF name or range of VRF IDs, the results show information only for the VRFs you specify.

Syntax

- `show ip igmp router-alert`
- `show ip igmp router-alert vrf WORD<1-16>`
- `show ip igmp router-alert vrfids WORD<0-512>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids <0-512>`	Specifies a VRF by ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip igmp sender

Display information about the Internet Group Management Protocol (IGMP) senders.

Syntax

- `show ip igmp sender`
- `show ip igmp sender group {A.B.C.D}`
- `show ip igmp sender group {A.B.C.D} vrf WORD<1-16>`
- `show ip igmp sender group {A.B.C.D} vrfids WORD<0-512>`
- `show ip igmp sender member-subnet {A.B.C.D/X}`
- `show ip igmp sender member-subnet {A.B.C.D/X} vrf WORD<1-16>`
- `show ip igmp sender member-subnet {A.B.C.D/X} vrfids WORD<0-512>`
- `show ip igmp sender member-subnet default`
- `show ip igmp sender vrf WORD<1-16>`
- `show ip igmp sender vrfids WORD<0-512>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids <0-512>`	Specifies a VRF by ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip igmp snooping

Display the status of Internet Group Management Protocol (IGMP) snoop.

Syntax

- `show ip igmp snooping`
- `show ip igmp snooping vrf WORD<1-16>`
- `show ip igmp snooping vrfids WORD<0-512>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids <0-512>`	Specifies a VRF by ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip igmp snoop-trace

View multicast group trace information for Internet Group Management Protocol (IGMP) snoop.

Syntax

- `show ip igmp snoop-trace [source <A.B.C.D>] [group <A.B.C.D>]`
- `show ip igmp snoop-trace group {A.B.C.D} vrf WORD<1-16>`
- `show ip igmp snoop-trace group {A.B.C.D} vrfids WORD<0-512>`
- `show ip igmp snoop-trace source {A.B.C.D} vrf WORD<1-16>`
- `show ip igmp snoop-trace source {A.B.C.D} vrfids WORD<0-512>`
- `show ip igmp snoop-trace vrf WORD<1-16>`
- `show ip igmp snoop-trace vrfids WORD<0-512>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`group <A.B.C.D>`	Specifies the multicast group address.
`source <A.B.C.D>`	Specifies the multicast source address.
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids <0-512>`	Specifies a VRF by ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip igmp ssm

Display the Source Specific Multicast (SSM) group range and the status of dynamic learning.

Syntax

- `show ip igmp ssm`
- `show ip igmp ssm vrf WORD<1-16>`
- `show ip igmp ssm vrfids WORD<0-512>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids <0-512>`	Specifies a VRF by ID.

©Avaya Inc. 2015 All Rights Reserved.

Home | Command modes | Alphabetical listing

show ip igmp ssm-map

Display the list of Source Specific Multicast (SSM) channels.

Syntax

- `show ip igmp ssm-map`
- `show ip igmp ssm-map vrf WORD<1-16>`
- `show ip igmp ssm-map vrfids WORD<0-512>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids <0-512>`	Specifies a VRF by ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip igmp static

Display information about the static and blocked ports for the Internet Group Management Protocol (IGMP)-enabled interfaces.

Syntax

- `show ip igmp static`
- `show ip igmp static vrf WORD<1-16>`
- `show ip igmp static vrfids WORD<0-512>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids <0-512>`	Specifies a VRF by ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip igmp stream-limit

Display multicast stream limitation information for the ports on a specific interface.

Syntax

- `show ip igmp stream-limit interface`
- `show ip igmp stream-limit interface vrf WORD<1-16>`
- `show ip igmp stream-limit interface vrfids WORD<0-512>`
- `show ip igmp stream-limit port`
- `show ip igmp stream-limit port vrf WORD<1-16>`
- `show ip igmp stream-limit port vrfids WORD<0-512>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`interface`	Specifies the type of interface to include in the output. The results display all ports using stream limitation on the selected interface type.
`port`	Specifies the Internet Group Management Protocol (IGMP) stream limitation port details.
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids <0-512>`	Specifies a VRF by ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip igmp sys

View the current fast leave mode configuration and Internet Group Management Protocol (IGMP) system parameters on the switch.

Syntax

- `show ip igmp sys`
- `show ip igmp sys vrf WORD<1-16>`
- `show ip igmp sys vrfids WORD<0-512>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids <0-512>`	Specifies a VRF by ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip interface

Shows the IP configuration for an interface.

Syntax

- `show ip interface`
- `show ip interface [vrf WORD<1-16>] [vrfids WORD <0-512>]`
- `show ip interface gigabitethernet [<1-4084>] [{slot/port[-slot/port][,...]}]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-4084>`	Specifies the VLAN ID.
`vrf WORD<1-16>`	Specifies the name of the VRF.
`vrfids WORD <0-512>`	Specifies the VRF ID in the range of 0 to 512.

©Avaya Inc. 2015 All Rights Reserved.

show ip ipfix

View global Internet Protocol Flow Information eXport (IPFIX) information to see the global administrative state of IPFIX for the chassis.

Syntax

- `show ip ipfix`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ip ipfix collector

View collector information to verify the collector configuration.

Syntax

- `show ip ipfix collector [{slot[-slot][,...]}] [<A.B.C.D>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot[-slot][,...]}`	Identifies the slot in one of the following formats: a single slot (3), a range of slots (3-4), or a series of slots (3,5,6). Valid slots are 3-12.
`{slot[-slot][,...]}<A.B.C.D>`	Displays the collector info for the IP address and slot.

©Avaya Inc. 2015 All Rights Reserved.

show ip ipfix export

View the exporter statistics for each slot to see the following information: collector IP address packets sent since you enabled Internet Protocol Flow Information eXport (IPFIX) bytes sent since you enabled IPFIX packets lost within the device IPFIX protocol status If you do not specify a slot, all slots appear in the command output.

Syntax

- `show ip ipfix export [{slot[-slot][,...]}]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot[-slot][,...]}`	Identifies the slot in one of the following formats: a single slot (3), a range of slots (3-4), or a series of slots (3,5,6). Valid slots are 3-12.

©Avaya Inc. 2015 All Rights Reserved.

show ip ipfix exporter

View the exporter configuration to show the following information: the administrative state of the exporter the template refresh rate the export interval the aging time the active timeout value

Syntax

- `show ip ipfix exporter [{slot[-slot][,...]}]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot[-slot][,...]}`	Identifies the slot in one of the following formats: a single slot (3), a range of slots (3-4), or a series of slots (3,5,6). Valid slots are 3-12

©Avaya Inc. 2015 All Rights Reserved.

show ip ipfix flows

View flow information to see the flow entries for first generation modules. The flow database is large; the functionality is simple in terms of sorting. The response time can be slow for sorted display. This command displays records from only one interface module at a time. This command uses the following type of optional fields: Fields that specify match fields. These fields can be an exact match or an operator like LE, GE, EQ, NE. Second generation I/O modules do not support the show ip ipfix flows command. For second generation modules use an IPFIX collector for IPFIX flow information.

Syntax

- `show ip ipfix flows {slot[-slot][,...]} [byte-count WORD<1-2> <0-4294967295>] [dest-addr WORD<1-2> {A.B.C.D}] [first-pkt-time WORD<1-2> <MMddyyyyhhmmss>] [last-pkt-time WORD<1-2> <MMddyyyyhhmmss>] [monitor<false|true>] [numflows <0-16000>][pkt-count WORD<1-2> <0-4294967295>] [port WORD<1-2> {slot/port}] [protocol WORD<1-2> <0-255>] [source-addr WORD<1-2> {A.B.C.D}][TCP-UDP-dest-port WORD<1-2> <0-65535>][TCP-UDP-src-port WORD<1-2> <0-65535>] [TOS WORD<1-2> <0-255>] [vlan WORD<1-2> <1-4084>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
byte-count WORD<1-2> <0-4294967295>	Shows the flows that match a number of bytes. Use the format oper{=|!=|<=|>=} and byte-count {0-4294967295}; for example, {>=a}.
dest-addr WORD<1-2> {A.B.C.D}	Shows the flows for a destination address. Use the format oper{=|!=|<=|>=} and ip address {A.B.C.D}; for example, {<=A.B.C.D}.
first-pkt-time WORD<1-2> <MMddyyyyhhmmss>	Shows the flows that match a timestamp for when the flow was first observed. Use the format oper{=|!=|<=|>=} and time {MMddyyyyhhmmss}; for example, {>=a}.
last-pkt-time WORD<1-2> <MMddyyyyhhmmss>	Shows the flows that match a timestamp for when the flow was last observed. Use the format oper{=|!=|<=|>=} and time {MMddyyyyhhmmss}; for example, {>=a}.
monitor <false|true>	Monitors the top 10 flows (by byte count) if you configure this variable to true. The maximum number of flows you can monitor is 100.
numflows <0-16000>	Shows the number of flows you specify. Specify zero (0) to show a flow summary. If you enter 0, the command output contains two extra lines at the bottom. The first line is all dashes and the second line is the total number of flows based on the slots you specify. The numflows parameter displays the number of IPFIX flows in the RSPs IPFIX flow table.
pkt-count WORD<1-2> <0-4294967295>	Shows the flows that match a packet count. Use the format oper{=|!=|<=|>=} and pktcount {0- 4294967295}; for example, {>=a}.
port WORD<1-2> {slot/port}	Shows the flows for a particular port. Use the format oper{=|!=|<=|>=} and {slot/port}; for example, {=a/b}.

`protocol WORD<1-2> <0-255>`	Shows the flows for a particular protocol. Use the format oper{=|!=|<=|>=} and protocol {0- 255}; for example, {>=a}. The mapping values for some protocol types are: icmp:1, tcp:6, udp:17, ipsecesp:50, ipsecah:51, ospf: 89, vrrp:112, snmp:254, undefined:256.
`source-addr WORD<1-2> {A.B.C.D}`	Shows the flows for a source address. Use the format oper{=|!=|<=|>=} and ip address {A.B.C.D}; for example, {<=A.B.C.D}.
`TCP-UDP-dest-port WORD<1-2> <0-65535>`	Shows the flows for a destination port. Use the format oper{=|!=|<=|>=} and port {0- 65535}; for example, {>=a}.
`TCP-UDP-src-port WORD<1-2> <0-65535>`	Shows the flows for a source port. Use the format oper{=|!=|<=|>=} and port {0-65535}; for example, {>=a}.
`TOS WORD<1-2> <0-255>`	Shows the flows that match a type of service. Use the format oper{=|!=|<=|>=} and TOS{0-255}; for example, {>=a}
`vlan WORD<1-2> <1-4084>`	Shows the flows for a particular VLAN. Use the format oper{=|!=|<=|>=} and vlan{1- 4084}; for example, {!=10}.

©Avaya Inc. 2015 All Rights Reserved.

show ip ipfix hash-statistics

View the hashing statistics to view total hash overflows for first generation modules. If you do not specify a slot, all slots appear in the command output. Second generation I/O modules do not support this command.

Syntax

- `show ip ipfix hash-statistics [{slot[-slot][,...]}]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot[-slot][,...]}`	Identifies the slot in one of the following formats: a single slot (3), a range of slots (3-4), or a series of slots (3,5,6). Valid slots are 3-12.

©Avaya Inc. 2015 All Rights Reserved.

show ip ipfix interface

View Internet Protocol Flow Information eXport (IPFIX) information for an interface to see the sampling rate and the IPFIX administrative status for the interface.

Syntax

- `show ip ipfix interface [gigabitethernet slot/port[-slot/port] [,...]}]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot[-slot][,...]}`	Identifies the slot in one of the following formats: a single slot (3), a range of slots (3-4), or a series of slots (3,5,6).

©Avaya Inc. 2015 All Rights Reserved.

show ip ipvpn

Display the configuration for IP VPN enabled VRFs.

Syntax

- `show ip ipvpn`
- `show ip ipvpn vrf WORD<1-16>`
- `show ip ipvpn vrf WORD<1-16> vrfids WORD<0-512>`
- `show ip ipvpn vrfids WORD<0-512>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF.
`vrfids WORD<0-512>`	Specifies a VRF ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip irdp

Confirm that the Router Discovery is enabled.

Syntax

- `show ip irdp`
- `show ip irdp [vrf WORD<1-16>] [vrfids WORD<0-512>]`
- `show ip irdp interface gigabitethernet [{slot/port[-slot/port][,...]}] [<1-4084>]`
- `show ip irdp interface vlan [<1-4084>]`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`<1-4084>`	Specifies the VLAN ID.
`interface gigabitethernet [{slot/port [-slot/port][,…]}]`	Specifies ports route discovery information.
`interface vlan <1-4084>`	Specifies VLAN route discovry information.
`vrf WORD<1-16>`	Specifies the VRF name.
`vrfids WORD<0-512>`	Specifies a VRF ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip isid-list

Display the I-SID list information.

Syntax

- `show ip isid-list [vrf WORD<1-16>][vrfids WORD<0-512>][WORD<1-32>]`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Displays I-SID list information for a particular VRF name.
`vrfids WORD<0-512>`	Displays I-SID list information for a particular VRF ID.
`WORD<1-32>`	Displays I-SID information for a particular I-SID list name.

©Avaya Inc. 2015 All Rights Reserved.

show ip isis accept

Display IS-IS accept information.

Syntax

- `show ip isis accept`
- `show ip isis accept vrf WORD<1-16>`
- `show ip isis accept vrf WORD<1-16> vrfids WORD<0-512>`
- `show ip isis accept vrfids WORD<0-512>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a particular VRF. Type a name between 1-16 characters in length.
`vrfids WORD<0-512>`	Specifies the VRF ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip isis redistribute

Display the redistribution configuration.

Syntax

- `show ip isis redistribute`
- `show ip isis redistribute vrf WORD<1-16>`
- `show ip isis redistribute vrf WORD<1-16> vrfids WORD<0-512>`
- `show ip isis redistribute vrfids WORD<0-512>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a particular VRF. Type a name between 1-16 characters in length.
`vrfids WORD<0-512>`	Specifies the VRF ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip mroute hw-resource-usage

View multicast hardware resource usage.

Syntax

- `show ip mroute hw-resource-usage`
- `show ip mroute hw-resource-usage vrf WORD<1-16>`
- `show ip mroute hw-resource-usage vrfids WORD<0-512>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids WORD<0-512>`	Specifies a VRF by ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip mroute interface

Display information about the multicast routes set up on the switch for a specific interface.

Syntax

- `show ip mroute interface gigabitethernet {slot/port[-slot/port][,...]}`
- `show ip mroute interface vrf WORD<1-16>`
- `show ip mroute interface vrfids WORD<0-512>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids WORD<0-512>`	Specifies a VRF by ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip mroute next-hop

Display information about the next hop for the multicast routes set up on the switch.

Syntax

- `show ip mroute next-hop`
- `show ip mroute next-hop vrf WORD<1-16>`
- `show ip mroute next-hop vrfids WORD<0-512>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids WORD<0-512>`	Specifies a VRF by ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip mroute route

Display information about the multicast routes set up on the switch.

Syntax

- `show ip mroute route`
- `show ip mroute route vrf WORD<1-16>`
- `show ip mroute route vrfids WORD<0-512>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF.
`vrfids WORD<0-512>`	Specifies a VRF ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip mroute static-source-group

Display information about the static source groups on the current interface.

Syntax

- `show ip mroute static-source-group`
- `show ip mroute static-source-group <A.B.C.D>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<A.B.C.D>	Specifies the IP address.

©Avaya Inc. 2015 All Rights Reserved.

show ip mroute stats

View multicast routing process statistics.

Syntax

- `show ip mroute stats [WORD<7-160>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
WORD<7-160>	Specifies the group IP address in the format {A.B.C.D[,E.F.G.H][,...]} . The maximum number of group IP addresses is 10. To view statistics, the group IP address is optional. To monitor statistics, the group IP address is required.

©Avaya Inc. 2015 All Rights Reserved.

show ip ospf

Display OSPF configuration information to ensure accuracy.

Syntax

- `show ip ospf`
- `show ip ospf vrf WORD<1-16>`
- `show ip ospf vrfids WORD <0-512>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids WORD <0-512>`	Specifies a range of VRF IDs.

©Avaya Inc. 2015 All Rights Reserved.

show ip ospf accept

Display information about the configured OSPF entries.

Syntax

- `show ip ospf accept`
- `show ip ospf accept vrf WORD<1-16>`
- `show ip ospf accept vrfids WORD<0-512>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies the name of the VRF.
`vrfids WORD<0-512>`	Specifies the ID of the VRF. The value is an integer between 0 and 512.

©Avaya Inc. 2015 All Rights Reserved.

show ip ospf area

Display OSPF area information to ensure accuracy.

Syntax

- `show ip ospf area`
- `show ip ospf area vrf WORD<1-16>`
- `show ip ospf area vrfids WORD<0-512>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids WORD <0-512>`	Specifies a range of VRF IDs.

©Avaya Inc. 2015 All Rights Reserved.

show ip ospf area-range

Display OSPF area range configuration information to ensure accuracy.

Syntax

- `show ip ospf area-range`
- `show ip ospf area-range vrf WORD<1-16>`
- `show ip ospf area-range vrfids <WORD 0-512>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf <WORD 1-16>`	Specifies a VRF by name.
`vrfids <WORD 0-512>`	Specifies a range of VRF IDs.

©Avaya Inc. 2015 All Rights Reserved.

show ip ospf ase

View the link-state database to determine externally learned routing information.

Syntax

- `show ip ospf ase`
- `show ip ospf ase metric-type <1-2>`
- `show ip ospf ase vrf WORD<1-16>`
- `show ip ospf ase vrfids WORD<0-512>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`metric-type <1-2>`	Specifies the metric type as a string of 1 to 2 characters.
`vrf WORD<1-16>`	Identifies the VRF by name.
`vrfids WORD<0-512>`	Specifies a VRF by ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip ospf authentication

Display OSPF authentication information to ensure accuracy.

Syntax

- `show ip ospf authentication interface`
- `show ip ospf authentication interface gigabitethernet {slot/port}`
- `show ip ospf authentication interface vlan <1-4084>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`gigabitethernet {slot/port} vlan <1-4084>`	Specifies the authentication interface type.

©Avaya Inc. 2015 All Rights Reserved.

show ip ospf default-cost

Display OSPF default cost information to ensure accuracy.

Syntax

- `show ip ospf default-cost`
- `show ip ospf default-cost vrf WORD<1-16>`
- `show ip ospf default-cost vrfids WORD<0-512>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids WORD<0-512>`	Specifies a range of VRF IDs.

©Avaya Inc. 2015 All Rights Reserved.

show ip ospf host-route

Display the host route OSPF information to ensure accuracy.

Syntax

- `show ip ospf host-route`
- `show ip ospf host-route vrf WORD<1-16>`
- `show ip ospf host-route vrfids WORD<0-512>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids WORD<0-512>`	Specifies a range of VRF IDs.

©Avaya Inc. 2015 All Rights Reserved.

show ip ospf ifstats

Use statistics to help you monitor Open Shortest Path First (OSPF) performance.

Syntax

- `show ip ospf ifstats`
- `show ip ospf ifstats detail`
- `show ip ospf ifstats mismatch`
- `show ip ospf ifstats vlan <1-4084>`
- `show ip ospf ifstats vrf WORD<1-16>`
- `show ip ospf ifstats vrfids WORD<0-512>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`detail`	Displays the details of the OSPF.
`mismatch`	Specifies the number of times the area ID is not matched.
`vlan <1-4084>`	Specifies a VLAN ID.
`vrf WORD<1-16>`	Specifies a VRF instance by VRF name.
`vrfids WORD<0-512>`	Specifies a VRF or range of VRFs by ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip ospf int-auth

Display OSPF authentication information to ensure accuracy.

Syntax

- `show ip ospf int-auth [vrf WORD<1-16>] [vrfids WORD<0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Displays ospf authentication configuration for a particular VRF.
`vrfids WORD<0-512>`	Specifies a range of VRF IDs.

©Avaya Inc. 2015 All Rights Reserved.

show ip ospf interface

Display OSPF information on a particular interface to ensure accuracy.

Syntax

- `show ip ospf interface [gigabitethernet {slot/port}|vlan <1-4084>] [vrf WORD<1-16>] [vrfids WORD<0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`gigabitethernet {slot/[port} |vlan <1-4084>`	Displays gigabitethernet port and VLAN IDs information.
`vrf WORD<1-16>`	Displays ospf configuration for a particular VRF.
`vrfids WORD<0-512>`	Specifies a range of VRF IDs.

©Avaya Inc. 2015 All Rights Reserved.

show ip ospf int-timers

Display OSPF timers information to ensure accuracy.

Syntax

- `show ip ospf int-timers [vrf WORD<1-16>] [vrfids WORD<0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Displays ospf timer configuration for a particular VRF.
`vrfids WORD<0-512>`	Specifies a range of VRF IDs.

©Avaya Inc. 2015 All Rights Reserved.

show ip ospf lsdb

View the area advertisements and other information contained in the link-state database (LSD) to ensure correct OSPF operations.

Syntax

- `show ip ospf lsdb [area <A.B.C.D>] [lsa-type <0-7>] [lsid <A.B.C.D>] [adv-rtr <A.B.C.D>] [vrf WORD<1-16>] [vrfids WORD<0-512>] [detail]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`adv-rtr <A.B.C.D>`	Specifies the advertising router.
`area <A.B.C.D>`	Specifies the OSPF area.
`detail`	Provides detailed output.
`lsa-type <0-7>`	Specifies the link-state advertisement type in the range of 0 to 7.
`lsid <A.B.C.D>`	Specifies the link-state ID.
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids WORD<0-512>`	Specifies a range of VRF IDs.

©Avaya Inc. 2015 All Rights Reserved.

show ip ospf neighbor

Displays OSPF NBMA neighbor information.

Syntax

- `show ip ospf neighbor [vrf WORD<1-16>] [vrfids WORD <0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids WORD<0-512>`	Specifies a range of VRF IDs.

©Avaya Inc. 2015 All Rights Reserved.

show ip ospf port-error

Check OSPF errors for administrative and troubleshooting purposes.

Syntax

- `show ip ospf port-error [port <portList>] [vrf WORD<1-16>] [vrfids WORD<0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`port {slot/port [-slot/port][,...]}`	Specifies the slot and the port number.
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids WORD<0-512>`	Specifies a range of VRF IDs.

©Avaya Inc. 2015 All Rights Reserved.

show ip ospf redistribute

Displays the OSPF redistribution configuration information.

Syntax

- `show ip ospf redistribute [vrf WORD<1-16>] [vrfids WORD<1-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids WORD <0-512>`	Specifies a range of VRF IDs.

©Avaya Inc. 2015 All Rights Reserved.

show ip ospf stats

Use statistics to help you monitor Open Shortest Path First (OSPF) performance.

Syntax

- `show ip ospf stats [vrf WORD<1-16>] [vrfids WORD<0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF instance by VRF name.
`vrfids WORD<0-512>`	Specifies a VRF or range of VRFs by ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip ospf virtual-link

Displays the OSPF virtual link information to ensure accuracy.

Syntax

- `show ip ospf virtual-link {A.B.C.D} {A.B.C.D} [vrf WORD<1-16>] [vrfids WORD<0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
{A.B.C.D} {A.B.C.D}	Specifies the area ID and the virtual interface ID. The first IP address specifies the area ID and the second specifies the virtual interface ID.
vrf WORD<1-16>	Displays OSPF configuration for a particular VRF. Specifies a VRF by name.
vrfids WORD<0-512>	Specifies a range of VRF IDs.

©Avaya Inc. 2015 All Rights Reserved.

show ip pim

Verify the configuration by displaying the global status of PIM on the switch.

Syntax

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ip pim active-rp

Displays information about the active rendezvous point (RP) for all groups or a specific group.

Syntax

- `show ip pim active-rp group <A.B.C.D>`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ip pim bsr

Displays information about the bootstrap router (BSR) for this PIM-SM domain.

Syntax

- `show ip pim bsr`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ip pim interface

Displays information about the PIM-SM interface setup on the switch.

Syntax

- `show ip pim interface [gigabitethernet [{slot/port [-slot/port][,...]}] [<1-4084>]`
- `show ip pim interface vlan [<1-4084>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<1-4084>`	Specifies the VLAN ID.
`gigabitethernet {slot/port [-slot/port][,...]}`	Displays configuration settings for the gigabitethernet interface.
`vlan [<1-4084>]`	Displays configuration setting for a VLAN interface.

©Avaya Inc. 2015 All Rights Reserved.

show ip pim mode

Show the PIM mode (SM or SSM) configuration on the switch.

Syntax

- `show ip pim mode`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ip pim mroute

Displays PIM multicast route information from the route table.

Syntax

- `show ip pim mroute terse`
- `show ip pim mroute terse group {A.B.C.D}`
- `show ip pim mroute terse source {A.B.C.D}`
- `show ip pim mroute terse source {A.B.C.D} group {A.B.C.D}`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`group {A.B.C.D}`	Specifies the multicast group address.
`source {A.B.C.D}`	Specifies the source IP address.
`terse`	Excludes the VLAN timers from the command output.

©Avaya Inc. 2015 All Rights Reserved.

show ip pim neighbor

Displays information about the neighboring routers configured with PIM-SM.

Syntax

- `show ip pim neighbor`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ip pim rp-candidate

Displays information about the candidate rendezvous points for the PIM-SM domain.

Syntax

- `show ip pim rp-candidate`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ip pim rp-hash

Displays information about the rendezvous points (RPs) for this PIM-SM domain.

Syntax

- `show ip pim rp-hash`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ip pim static-rp

Displays the static rendezvous point (RP) table.

Syntax

- `show ip pim static-rp`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ip pim virtual-neighbor

Display the virtual neighbor.

Syntax

- `show ip pim virtual-neighbor`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ip prefix-list

Display the prefix list.

Syntax

- `show ip prefix-list [WORD<1-64>] [prefix <A.B.C.D>] [vrf WORD<1-16>] [vrfids WORD<0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`prefix {A.B.C.D}`	Adds a prefix entry to the prefix list. {A.B.C.D} is the IP address.
`vrf WORD<1-16>`	Shows prefix list information for a particular VRF.
`vrfids WORD <0-512>`	Shows prefix list for particular VRF ids. The ID of the VRF and is an integer in the range of 0 to 512.
`WORD <1-64>`	Renames the specified prefix list. The name length is from 1 to 64 characters.

©Avaya Inc. 2015 All Rights Reserved.

show ip redistribute

Display and ensure the accuracy of the configuration settings.

Syntax

- `show ip <rip|ospf|bgp> redistribute [interface] [vrf WORD<1-16>] [vrfids WORD<0-512>]`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`<ospf|bgp|static|direct|rip>`	Specifies the type of routes to redistribute-the protocol source.
`interface`	Shows rip information for each interface.
`vrf WORD<1-16>`	Displays rip configuration for a particular VRF.
`vrfids WORD<0-512>`	Specifies a list of VRF IDs.

©Avaya Inc. 2015 All Rights Reserved.

show ip rip

Display RIP configuration information to ensure the configuration is accurate.

Syntax

- `show ip rip [vrf WORD<1-16>] [vrfids WORD<0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF by name.
`vrfids WORD<0-512>`	Specifies a range of VRF IDs.

©Avaya Inc. 2015 All Rights Reserved.

show ip rip interface

Display Routing Information Protocol (RIP) information for each interface.

Syntax

- `show ip rip interface {A.B.C.D}`
- `show ip rip interface ports [{slot/port [-slot/port][,...]}]`
- `show ip rip interface ports [{slot/port [-slot/port][,...]}] vlan <1-4084>`
- `show ip rip interface vlan <1-4084>`
- `show ip rip interface vrf WORD<1-16>`
- `show ip rip interface vrf WORD<1-16> vrfids WORD<0-512>`
- `show ip rip interface vrfids WORD<0-512>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
{A.B.C.D}	Shows configurations based on an IP address assigned to a VLAN.
{A.B.C.D}	Specifies an IP address.
ports {slot/port [-slot/port][,...]}	Shows RIP information for port configurations. {slot/port [-slot/port][,...]} specifies the port.
vlan <1-4084>	Shows RIP configuration information for a particular VLAN. <1-4084> specifies the VLAN ID.
vrf WORD<1-16>	Specifies the VRF instance by name. When applying a redistribution instance that redistributes from a nonzero VRF to VRF 0 (the global router), do not specify the destination VRF; only specify the source VRF.
vrfids WORD<0-512>	Specifies a range of VRF IDs.

©Avaya Inc. 2015 All Rights Reserved.

show ip rip redistribute

Display the RIP redistribution configuration information.

Syntax

- `show ip rip redistribute [vrf WORD<1-16>] [vrfids WORD<1-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies the VRF instance by name. When applying a redistribution instance that redistributes from a nonzero VRF to VRF 0 (the global router), do not specify the destination VRF; only specify the source VRF.
`vrfids WORD<0-512>`	Specifies a range of VRF IDs.

©Avaya Inc. 2015 All Rights Reserved.

show ip route

Display the IP route information.

Syntax

- show ip route
- show ip route {A.B.C.D}
- show ip route alternative
- show ip route count-summary
- show ip route -s {A.B.C.D/X}
- show ip route -s default
- show ip route spbm-nh-as-mac
- show ip route static
- show ip route static {A.B.C.D}
- show ip route static {A.B.C.D} -s {A.B.C.D} {A.B.C.D}
- show ip route static {A.B.C.D} vrf WORD<1-16>
- show ip route static {A.B.C.D} vrfids WORD<0-512>
- show ip route static -s {A.B.C.D} {A.B.C.D}
- show ip route static -s {A.B.C.D} {A.B.C.D} vrf WORD<1-16>
- show ip route static -s {A.B.C.D} {A.B.C.D} vrfids WORD<0-512>
- show ip route static vrf WORD<1-16>
- show ip route static vrfids WORD<0-512>
- show ip route vrf WORD<1-16>
- show ip route vrfids WORD<0-512>

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<A.B.C.D>	Specifies the IP address of the route to the network.

alternative	Displays the alternative routes.
count-summary	Displays ip route count summary.
-s <A.B.C.D/X>	Indicates the IP address and subnet mask for which to display routes.
-s default	Specifies the default subnet.
static	Shows static route information.
vrf WORD<1-16>	Specifies a VRF instance by VRF name.
vrfids WORD<0-512>	Specifies a VRF instance by VRF number.

©Avaya Inc. 2015 All Rights Reserved.

show ip route preference

Display the IP route preference information to confirm that the configuration is correct.

Syntax

- `show ip route preference [vrf WORD<1-16>] [vrfids WORD<0-255>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF instance by VRF name.
`vrfids WORD<0-255>`	Specifies a VRF instance by VRF number.

©Avaya Inc. 2015 All Rights Reserved.

show ip routing

Display the ip routing configuration information.

Syntax

- `show ip routing [vrf WORD<1-16>] [vrfids WORD<0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies a VRF instance by VRF name.
`vrfids WORD<0-512>`	Specifies a VRF instance by VRF number.

©Avaya Inc. 2015 All Rights Reserved.

show ip rsmlt

Show IP Routed Split MultiLink Trunking (RSMLT) information to view data about all RSMLT interfaces.

Syntax

- `show ip rsmlt [<local|peer>] [vrf WORD<1-16>] [vrfids WORD<0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`[<local|peer>]`	Specifies values for the local or peer switch.
`vrf WORD<1-16>`	Displays IP routing for a VRF.
`vrfids WORD<0-512>`	Displays IP routing for a range of VRFs.

©Avaya Inc. 2015 All Rights Reserved.

show ip rsmlt edge-support

Display Routed Split MultiLink Trunking (RSMLT)-edge status information.

Syntax

- `show ip rsmlt edge-support`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`edge-support`	Displays RSMLT edge support and peer information.

©Avaya Inc. 2015 All Rights Reserved.

show ip tcp statistics

View TCP statistics to manage network performance.

Syntax

- `show ip tcp connections`
- `show ip tcp properties`
- `show ip tcp statistics`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`connections`	Displays IP TCP connections information command.
`properties`	Displays IP TCP global properties.
`statistics`	Displays IP TCP global statistics command.

©Avaya Inc. 2015 All Rights Reserved.

show ip udp statistics

Display UDP statistics information.

Syntax

- `show ip udp endpoints`
- `show ip udp statistics`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`endpoints`	Displays IP UDP endpoints information.
`statistics`	Displays IP UDP statistics information.

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 address

View IPv6 address entries.

Syntax

- `show ipv6 address interface`
- `show ipv6 address interface gigabitethernet [{slot/port[-slot/port][,...]}]`
- `show ipv6 address interface ip WORD<0-46>`
- `show ipv6 address interface tunnel <1-2000>`
- `show ipv6 address interface vlan [ <1-4084>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-4084>`	Specifies the VLAN ID.
`tunnel <1-2000>`	Displays the address entries specific to a tunnel ID.
`WORD<0-46>`	Specifies an IPv6 address.

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 dcache

Display the destination cache to see next-hop addresses for destinations. The destination cache is only populated or updated when IPv6 packets originate locally on the central processor of the switch.

Syntax

- `show ipv6 dcache [gigabitethernet {slot/port}] [mgmtethernet {slot/port}] [tunnel <1-2000>] [vlan <1-4084>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
{slot/port}	Identifies the slot and port.
<1-2000>	Specifies the tunnel ID.
<1-4084>	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 dhcp-relay

Display IPv6 Dynamic Host Configuration Protocol (DHCP) Relay information to show relay information about DHCP routes and counters.

Syntax

- `show ipv6 dhcp-relay counters`
- `show ipv6 dhcp-relay fwd-path`
- `show ipv6 dhcp-relay interface [gigabitethernet {slot/port[-slot/port][,...]}] [vlan <1-4084>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`counters`	Displays the count of DHCP Relay requests and replies.
`fwd-path`	Displays information about DHCP Relay forward paths.
`gigabitethernet {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`vlan <1-4084>`	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 forwarding

Show IPv6 forwarding information.

Syntax

- `show ipv6 forwarding`

Default

`The default is disabled.`

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 global

Show global IPv6 configuration information.

Syntax

- `show ipv6 global`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 interface

Show IPv6 information for all or specific interfaces.

Syntax

- `show ipv6 interface gigabitethernet [{slot/port[-slot/port][,...]}]`
- `show ipv6 interface icmpstatistics`
- `show ipv6 interface icmpstatistics [ vlan <1-4084>]`
- `show ipv6 interface icmpstatistics gigabitEthernet [{slot/port[-slot/port][,...]}]`
- `show ipv6 interface icmpstatistics mgmtEthernet [{slot/port[-slot/port][,...]}]`
- `show ipv6 interface icmpstatistics tunnel <1-2000>`
- `show ipv6 interface mgmtEthernet [{slot/port[-slot/port][,...]}]`
- `show ipv6 interface statistics`
- `show ipv6 interface statistics gigabitEthernet [{slot/port[-slot/port][,...]}]`
- `show ipv6 interface statistics mgmtEthernet [{slot/port[-slot/port][,...]}]`
- `show ipv6 interface statistics tunnel <1-2000>`
- `show ipv6 interface statistics vlan <1-4084>`
- `show ipv6 interface tunnel <1-2000>`
- `show ipv6 interface vlan [<1-4084>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`gigabitEthernet {slot/port[-slot/port][,...]}`	Displays IPv6 interface information for gigabitEthernet as one of the following: a single slot and port (3/1) a range of slots and ports (3/2-3/4, a series of slots and ports (3/2,5/3,6/2)
`icmpstatistics [gigabitEthernet | mgmtEthernet | tunnel | vlan]`	Shows IPv6 ICMP statistics for the interface as follows: gigabitEthernet-displays interface gigabitEthernet configurations, mgmtEthernet-displays interface mgmtEthernet configurations, tunnel-displays interface tunnel configurations, vlan -displays vlan interface configurations.
`mgmtEthernet {slot/port[-`	Displays IPv6 interface information for mgmtEthernet as one of the following: a single slot and port (3/1) a range of slots and ports (3/2-3/4, a series of

slot/port][,...]}	slots and ports (3/2,5/3,6/2)
statistics [gigabitEthernet | mgmtEthernet | tunnel | vlan]	Shows IPv6 interface statistics as follows: gigabitEthernet- displays interface gigabitEthernet configurations mgmtEthernet-displays interface mgmtEthernet configurations tunnel- displays interface tunnel configurations vlan -displays vlan interface configurations
tunnel <1-2000>	Displays IPv6 interface information for a tunnel. The tunnel ID is expressed as a value from 1 to 2000.
vlan <1-4084>	Displays IPv6 interface information for a VLAN. The VLAN ID is expressed as a value from 1 to 4084.

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 nd

View neighbor discovery interface configuration.

Syntax

- `show ipv6 nd interface gigabitethernet [{slot/port[-slot/port][,...]}]`
- `show ipv6 nd interface vlan [<1-4084>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-4084>`	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 nd-prefix

View all configured neighbor discovery prefixes.

Syntax

- `show ipv6 nd-prefix [detail]`
- `show ipv6 nd-prefix interface gigabitethernet [{slot/port[-slot/port][,...]}]`
- `show ipv6 nd-prefix interface vlan [<1-4084>]`
- `show ipv6 nd-prefix vlan [<1-4084>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-4084>`	Specifies the VLAN ID.
`detail`	Shows detailed information.

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 neighbor

View entries in the neighbor cache.

Syntax

- `show ipv6 neighbor`
- `show ipv6 neighbor interface gigbitethernet {slot/port}`
- `show ipv6 neighbor interface mgmtEthernet {slot/port}`
- `show ipv6 neighbor interface mlt <1-512>`
- `show ipv6 neighbor interface vlan <1-4084>`
- `show ipv6 neighbor type <1-4>`
- `show ipv6 neighbor WORD<0-46>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
{slot/port}	Identifies the slot and port for the interface.
<1-4084>	Specifies the VLAN ID.
<1-512>	Specifies the MLT ID.
type <1-4>	Specifies the type of mapping: 1: other, 2: dynamic, 3: static, or 4: local.
WORD<0-46>	Specifies the neighbor address.

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 ospf

Show the IPv6 OSPFv3 global configuration.

Syntax

- `show ipv6 ospf`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 ospf area

Show the IPv6 OSPFv3 area configuration.

Syntax

- `show ipv6 ospf area`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 ospf area-range

Show the IPv6 OSPFv3 range configuration.

Syntax

- `show ipv6 ospf area-range`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 ospf ase

Show the IPv6 OSPFv3 as-external LSAs.

Syntax

- `show ipv6 ospf ase [metric-type <1-2>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`metric-type <1-2>`	Specifies the external type.

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 ospf interface

Show the IPv6 OSPFv3 interface configuration.

Syntax

- `show ipv6 ospf interface [gigabitEthernet {slot/port}] [vlan <1-4084>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
{slot/port]	Specifies the slot and port.
<1-4084>	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 ospf int-timers

Show the IPv6 OSPFv3 interface timers.

Syntax

- `show ipv6 ospf int-timers`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 ospf lsdb

Show the IPv6 OSPFv3 Link-state database configuration.

Syntax

- `show ipv6 ospf lsdb [adv-rtr {A.B.C.D}] [area {A.B.C.D}] [detail][interface gigabitEthernet {slot/port}] [interface vlan <1-4084>] [lsa-type <1-9>] [lsid <0-4294967295>] [scope <1-3>] [tunnel <1-2000>]`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 ospf nbma-nbr interface

Show the IPv6 OSPFv3 NBMA neighbor configuration.

Syntax

- `show ipv6 ospf nbma-nbr interface gigabitEthernet {slot/port} [WORD<1-46>]`
- `show ipv6 ospf nbma-nbr interface vlan <1-4084> [WORD<1-46>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port}`	Specifies the slot and port.
`<1-4084>`	Specifies the VLAN ID.
`WORD<1-46>`	Specifies an IPv6 address.

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 ospf neighbor

Show the IPv6 OSPFv3 neighbor configuration.

Syntax

- `show ipv6 ospf neighbor`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 ospf redistribute

Show the IPv6 OSPFv3 redistribution configuration.

Syntax

- `show ipv6 ospf redistribute`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 ospf statistics

Show the IPv6 OSPFv3 statistics.

Syntax

- `show ipv6 ospf statistics`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 prefix-list

Show IPv6 prefix-list information.

Syntax

- `show ipv6 prefix-list`
- `show ipv6 prefix-list prefix WORD<1-256>`
- `show ipv6 prefix-list WORD<1-64>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`prefix`	Specifies the prefix.
`prefix-list`	Shows IPv6 prefix-list information.
`WORD<1-64>`	Specifies the prefix-list name.

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 route

Show IPv6 routes for the switch.

Syntax

- `show ipv6 route [count-summary] [dest WORD<0-46> ][gigabitethernet {slot/port}] [next-hop WORD<0-46> ][static] [tunnel <1-2000>] [vlan <1-4084>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
{slot/port}	Identifies the slot and port for the interface.
count-summary	Shows the total number of OSPF, RIP, BGP, static, and local routes.
dest WORD<0-46>	Shows the route to a specific IPv6 address.
next-hop WORD<0-46>	Shows the route to a specific IPv6 next hop.
static	Shows static IPv6 routes.
tunnel <1-2147477248>	Shows route entries for a specific tunnel ID.
vlan <1-4084>	Shows route entries for a specific VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 tcp

You can display IPv6 TCP information. Check the health of connections, from the switch perspective, as they traverse the network detect intermittent connectivity detect attacks on resources determine which applications are active by checking the port numbers view statistics about TCP connections

Syntax

- `show ipv6 tcp <connections|listener|properties|statistics>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
connections	Displays IPv6 TCP connection table information that includes: local port remote port local address remote address state.
listener	Displays IPv6 TCP listener table information that includes: local port and local address.
properties	Displays IPv6 TCP global properties information that includes: RtoAlgorithm - the timeout value used for retransmitting unacknowledged octets. RtoMin -the minimum time, in milliseconds, permitted by a TCP implementation for the retransmission timeout. RtoMax - the maximum time (in milliseconds) permitted by a TCP implementation for the transmissions timeout. MaxConn - the maximum connections for the device
statistics	Displays IPv6 TCP global statistics information that includes: ActiveOpens, PassiveOpens, AttemptFails, EstabResets, CurrEstab, InSegs, OutSegs, RetransSegs, InErrs, OutRsts, HCInSegs, and HCOutSegs.

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 trace

Show the status of IPv6 trace commands.

Syntax

- `show ipv6 trace <base|forwarding|nd|ospf|rtm|transport>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<base|forwarding|nd|ospf|rtm|transport>`	Shows the status for the selected type of trace command.

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 tunnel

Shows information about configured IPv6 tunnels, for example, operational state or addresses.

Syntax

- `show ipv6 tunnel [<1-2000>] [detail] [local {A.B.C.D}][remote {A.B.C.D}]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<1-2000>`	Shows configuration information for a specific tunnel ID.
`detail`	Shows detailed configuration information, for example, the operational status and origin.
`local {A.B.C.D}`	Shows configuration information for a specific local endpoint address.
`remote {A.B.C.D}`	Shows configuration information for a specific remote endpoint address.

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 udp

Show IPv6 User Datagram Protocol (UDP) information.

Syntax

- `show ipv6 udp`
- `show ipv6 udp endpoints`
- `show ipv6 udp local_addr WORD<0-128> [{slot/port}]`
- `show ipv6 udp remote_addr WORD<0-128> [{slot/port}]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`endpoints`	Shows IPv6 UDP information for the endpoints.
`local_addr WORD<0-128> [{slot/port}]`	Shows IPv6 UDP information for a local IPv6 address or slot and port.
`remote_addr WORD<0-128> [{slot/port}]`	Shows IPv6 UDP information for a remote IPv6 address or slot and port.

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 vrrp

Shows the global status of Virtual Router Redundancy Protocol (VRRP) for IPv6.

Syntax

- `show ipv6 vrrp`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 vrrp address

Display address information for a specific link-local address or virtual router ID.

Syntax

- `show ipv6 vrrp address`
- `show ipv6 vrrp address link-local WORD<0-127>`
- `show ipv6 vrrp address vrid <1-255>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`link-local WORD<0-127>`	Displays information by link-local IPv6 address.
`vrid <1-255>`	Displays information by virtual router ID.

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 vrrp interface

Shows the extended Virtual Router Redundancy Protocol (VRRP) configuration for all interfaces or for a specific interface.

Syntax

- `show ipv6 vrrp interface [verbose]`
- `show ipv6 vrrp interface gigabitethernet[{slot/port[-slot/port][,...]}] [verbose]`
- `show ipv6 vrrp interface vlan [<1-4084>] [verbose]`
- `show ipv6 vrrp interface vrid <1-255> [verbose]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-255>`	Displays information by virtual router ID.
`<1-4084>`	Specifies the VLAN ID.
`verbose`	Displays extended information.

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 vrrp interface gigabitethernet statistics

Shows the IPv6 gigabitEthernet interface statistics.

Syntax

- `show ipv6 vrrp interface gigabitethernet statistics [slot/port[-slot/port][,...]] [verbose]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`statistics`	Displays the IPv6 interface gigabitEthernet statistics.
`statistics[slot/port[-slot/port][,...]]`	Displays the IPv6 statistics for a port.
`verbose`	Displays extended information.

©Avaya Inc. 2015 All Rights Reserved.

show ipv6 vrrp statistics

Views VRRP for IPv6 statistics to manage network performance.

Syntax

- `show ipv6 vrrp statistics [link-local WORD<0-127>][vrid <1-255>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<1-255>	Displays information by virtual router ID.
WORD<0-127>	Displays information by link-local IPv6 address.

©Avaya Inc. 2015 All Rights Reserved.

show ip vrf

Use the following command to view VRF configurations.

Syntax

- `show ip vrf`
- `show ip vrf max-routes [vrfids WORD <1-512>] [WORD <1-16>]`
- `show ip vrf vrfids WORD<1-512>`
- `show ip vrf WORD <1-16>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`max-routes`	Displays the maximum routes for the VRF.
`mvpn`	Displays MVPN information for the VRF.
`vrfids WORD<1-512>`	Displays VRF information for a particular VRF ID.
`WORD<1-16>`	Displays VRF information for a particular VRF by name.

©Avaya Inc. 2015 All Rights Reserved.

show ip vrf mvpn

Displays information about all VRFS with MVPN enabled.

Syntax

- `show ip vrf mvpn`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ip vrrp

Display the global Virtual Router Redundancy Protocol (VRRP) configuration.

Syntax

- `show ip vrrp`
- `show ip vrrp vrf WORD<1-16>`
- `show ip vrrp vrfids WORD<0-512>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Displays VRF information for a particular VRF by name.
`vrfids WORD<0-512>`	Displays VRF information for a particular VRF ID.

©Avaya Inc. 2015 All Rights Reserved.

show ip vrrp address

Display basic Virtual Router Redundancy Protocol (VRRP) configuration information about the specified port, all ports, or the VLAN.

Syntax

- `show ip vrrp address [addr {A.B.C.D}][vrid <1-255>][addr <A.B.C.D>] [vrf WORD<1-16>] [vrfids WORD<0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
addr {A.B.C.D}	Specifies the IP address of the master VRRP.
vrf WORD<1-16>	Specifies the name of the VRF.
vrfids WORD<0-512>	Specifies the ID of the VRF and is an integer in the range of 0 to 512.
vrid <1-255>	Specifies a unique integer value that represents the virtual router ID in the range 1 to 255. The virtual router acts as the default router for one or more assigned addresses.

©Avaya Inc. 2015 All Rights Reserved.

show ip vrrp interface

Display Virtual Router Redundancy Protocol (VRRP) information about the interface.

Syntax

- `show ip vrrp interface`
- `show ip vrrp interface verbose`
- `show ip vrrp interface vrf WORD<1-16>`
- `show ip vrrp interface vrf WORD<1-16> vrfids WORD<0-512>`
- `show ip vrrp interface vrfids WORD<0-512>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`gigabitEthernet {slot/port [-slot/port][,...]}`	Shows the VRRP interface gigabitEthernet configurations.
`verbose`	Shows all available information about the VRRP interfaces.
`vlan <1-4084>`	Specifies the VLAN that contains the VRRP. <1-4084> specifies the VLAN ID n the range of 1 to 4084.
`vrf WORD<1-16>`	Specifies a unique integer value that represents the virtual router ID in the range of 1-255. The virtual router acts as the default router for one or more assigned addresses.
`vrfids WORD<0-512>`	Specifies the ID of the VRF and is an integer in the range of 0 to 512.

©Avaya Inc. 2015 All Rights Reserved.

show ip vrrp interface gigabitEthernet

Display the Virtual Router Redundancy Protocol (VRRP) interface gigabitEthernet configurations.

Syntax

- `show ip vrrp interface gigabitEthernet verbose`
- `show ip vrrp interface gigabitEthernet[{slot/port[-slot/port][,...]}] [1-4084>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
{slot/port[-slot/port][,...]}	Specifies the slot/port number of a range of ports.
<1-4084>	Specifies the VLAN ID in the range of 1 to 4084.
verbose	Displays all available information about the VRRP interface gigabitEthernet configurations.

©Avaya Inc. 2015 All Rights Reserved.

show ip vrrp interface gigabitEthernet statistics

Display statistics for Virtual Router Redundancy Protocol (VRRP) ports.

Syntax

- `show ip vrrp interface gigabitEthernet statistics`
- `show ip vrrp interface gigabitEthernet statistics {slot/port[-slot/port][,...]}`
- `show ip vrrp interface gigabitEthernet statistics verbose`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Specifies the slot/port number of a range of ports.
`verbose`	Displays all available information about the VRRP interface gigabitEthernet configurations.

©Avaya Inc. 2015 All Rights Reserved.

show ip vrrp interface vlan

Show the extended Virtual Router Redundancy Protocol (VRRP) configuration for all VLANs on the switch or for the specified VLAN.

Syntax

- `show ip vrrp interface vlan [<1-4084>] [verbose] [vrf WORD<1-16>] [vrfids WORD<0-512>][{slot/port [-slot/port][,...]}]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Specifies the slot/port number of a range of ports.
`vlan <1-4084>`	Specifies the VLAN ID in the range of 1 to 4084.
`vrf WORD<1-16>`	Specifies the name of the VRF.
`vrfids WORD<0-512>`	Specifies the ID of the VRF and is an integer in the range of 0 to 512.

©Avaya Inc. 2015 All Rights Reserved.

show ip vrrp statistics

Display Virtual Router Redundancy Protocol (VRRP) statistics.

Syntax

- `show ip vrrp statistics [address {A.B.C.D}] [vrf WORD<1-16>] [vrfids WORD<0-512>] [vrid<1-255>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
address {A.B.C.D}	Specifies the address of the backup VRRP.
vrf WORD<1-16>	Specifies the VRF name.
vrfids WORD<0-512>	Specifies the ID of the VRF and is an integer in the range of 0 to 512.
vrid WORD<1-255>	Specifies a unique integar value that represents the virtual router ID in the range of 1 to 255. The virtual router acts as the default router for one or more assigned addresses.

©Avaya Inc. 2015 All Rights Reserved.

show isis

Display the global Intermediate-System-to-Intermediate-System (IS-IS) configuration.

Syntax

- `show isis`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show isis adjacencies

Display Intermediate-System-to-Intermediate-System (IS-IS) adjacencies.

Syntax

- `show isis adjacencies`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show isis area

Display the Intermediate-System-to-Intermediate-System (IS-IS) area address.

Syntax

- `show isis area`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show isis int-auth

Display the Intermediate-System-to-Intermediate-System (IS-IS) interface authentication configuration.

Syntax

- `show isis int-auth`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show isis int-ckt-level

Display the Intermediate-System-to-Intermediate-System (IS-IS) circuit level parameters.

Syntax

- `show isis int-ckt-level`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show isis int-counters

Display Intermediate-System-to-Intermediate-System (IS-IS) interface counters.

Syntax

- `show isis int-counters`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show isis interface

Display Intermediate-System-to-Intermediate-System (IS-IS) interface configuration and status parameters (including adjacencies).

Syntax

- `show isis interface`
- `show isis interface { l1 | l2 | l12 }`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{ l1 | l2 | l12 }`	Displays the interface information for the specified level: l1 (Level 1), l2 (Level 2), l12 (Level 1 and 2). The Avaya Virtual Services Platform 9000 is a Level 1 router, which means it has only Level 1 links and can route within only one area. Level 1 routers route only within their assigned area and cannot route outside that area. Level 2 routers route between areas and toward other domains. Level 1/Level 2 routers route within an assigned area and between areas. Level 1/Level 2 routers maintain both a Level 1 Link State Database and a Level 2 Link State Database.

©Avaya Inc. 2015 All Rights Reserved.

show isis int-l1-cntl-pkts

Display Intermediate-System-to-Intermediate-System (IS-IS) Level 1 control packet counters.

Syntax

- `show isis int-l1-cntl-pkts`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show isis int-l2-cntl-pkts

Display Intermediate-System-to-Intermediate-System (IS-IS) Level 2 control packet counters. This command is not supported in the current release. The current release supports only IS-IS level 1.

Syntax

- `show isis int-l2-cntl-pkts`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show isis int-timers

Display Intermediate-System-to-Intermediate-System (IS-IS) interface timers.

Syntax

- `show isis int-timers`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show isis lsdb

Display the Intermediate-System-to-Intermediate-System (IS-IS) Link State Database (LSDB).

Syntax

- `show isis lsdb`
- `show isis lsdb detail`
- `show isis lsdb ip-unicast`
- `show isis lsdb level { l1 | l2 | l12 }`
- `show isis lsdb local`
- `show isis lsdb lspid xxxx.xxxx.xxxx.xx-xx - 8 bytes`
- `show isis lsdb sysid xxxx.xxxx.xxxx - 6 bytes`
- `show isis lsdb tlv <1-186>`
- `show isis lsdb tlv <1-186> sub-tlv <1-3>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`detail`	Displays detailed information, which includes the Link State Packet (LSP) ID, the level of the external router, the maximum age of the LSP, the LSP sequence number and the LSP checksum.
`ip-unicast`	Displays Intermediate-System-to-Intermediate-System (IS-IS) link state database (LSDB) IP unicast information.
`level { l1 | l2 | l12 }`	Displays the link state database for the specified level: l1 (Level 1), l2 (Level 2), or l12 (Level 1 and 2). The Avaya Virtual Services Platform 9000 is a Level 1 router, which means it has only Level 1 links and can route within only one area. Level 1 routers route only within their assigned area and cannot route outside that area. Level 2 routers route between areas and toward other domains. Level 1/Level 2 routers route within an assigned area and between areas. Level 1/Level 2 routers maintain both a Level 1 link state database and a Level 2 Link State database.
`local`	Displays information on the local link state database.
`lspid xxxx.xxxx.xxxx.xx-xx - 8 bytes`	Displays the link state database for the specified Link State Packet (LSP) ID. The LSP ID is assigned to external IS-IS routing devices.

sub-tlv <1-3>	Displays the link state database for a specified sub-Type-Length-Value (TLV). Shortest Path Bridging MAC (SPBM) employs Intermediate-System-to-Intermediate-System (IS-IS) as the interior gateway protocol and implements additional TLVs to support additional functionality. TLVs exist inside IS-IS packets and Sub-TLVs exist as additional information in TLVs.
sysid xxxx.xxxx.xxxx - 6 bytes	Displays the link state database for the specified system ID.
tlv <1-186>	Displays the link state database for a specified Type-Length-Value (TLV). Shortest Path Bridging MAC (SPBM) employs Intermediate-System-to-Intermediate-System (IS-IS) as the interior gateway protocol and implements additional TLVs to support additional functionality. TLVs exist inside IS-IS packets and give additional information.

©Avaya Inc. 2015 All Rights Reserved.

show isis lsdb ip-unicast

Display the Intermediate-System-to-Intermediate-System (IS-IS) Link State Database (LSDB) IP unicast information.

Syntax

- `show isis lsdb ip-unicast`
- `show isis lsdb ip-unicast i-sid <0-16777215>`
- `show isis lsdb ip-unicast lspid xxxx.xxxx.xxxx.xx-xx`
- `show isis lsdb ip-unicast sysid xxxx.xxxx.xxxx`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`i-sid <0-16777215>`	Displays link state database (LSDB) IP unicast information by I-SID.
`lspid <xxxx.xxxx.xxxx.xx-xx>`	Displays the link state database (LSDB) IP unicast information for the specified Link State Packet (LSP) ID. The LSP ID is assigned to external IS-IS routing devices.
`sysid <xxxx.xxxx.xxxx>`	Displays the link state database (LSDB) IP unicast information for the specified system ID.

©Avaya Inc. 2015 All Rights Reserved.

show isis manual-area

Display Intermediate-System-to-Intermediate-System (IS-IS) areas.

Syntax

- `show isis manual-area`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show isis net

Display Intermediate-System-to-Intermediate-System (IS-IS) net information.

Syntax

- `show isis net`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show isis spbm

Display the Shortest Path Bridging MAC (SPBM) configuration.

Syntax

- `show isis spbm`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show isis spb-mcast-summary

Displays multicast over SPBM summary information for each S, G, V tuple.

Syntax

- `show isis spb-mcast-summary`
- `show isis spb-mcast-summary host-name WORD<0-255>`
- `show isis spb-mcast-summary lspid xxxx.xxxx.xxxx.xx-xx`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`host-name WORD<0-255>`	Specifies the host name of the source.
`lspid xxxx.xxxx.xxxx.xx-xx`	Specifies the LSP ID in xxx.xxx.xxx.xx-xx — 8 byte format.

©Avaya Inc. 2015 All Rights Reserved.

show isis spbm drop-stats port

Shows packet drop statistics on a per-port basis.

Syntax

- `show isis spbm drop-stats port last-drop`
- `show isis spbm drop-stats port last-drop {slot/port[-slot/port][,...]}`
- `show isis spbm drop-stats port rpfc-multicast-sa`
- `show isis spbm drop-stats port rpfc-multicast-sa {slot/port[-slot/port][,...]}`
- `show isis spbm drop-stats port rpfc-unicast-sa`
- `show isis spbm drop-stats port rpfc-unicast-sa {slot/port[-slot/port][,...]}`
- `show isis spbm drop-stats port unknown-multicast-da`
- `show isis spbm drop-stats port unknown-multicast-da {slot/port[-slot/port][,...]}`
- `show isis spbm drop-stats port unknown-unicast-da`
- `show isis spbm drop-stats port unknown-unicast-da {slot/port[-slot/port][,...]}`
- `show isis spbm drop-stats port unknown-unicast-sa`
- `show isis spbm drop-stats port unknown-unicast-sa {slot/port[-slot/port][,...]}`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`last-drop`	Displays information for the last packets dropped.
`rpfc-multicast-sa`	Displays the total number of SPBM RPFC multicast packets dropped. These drops occur when packets with a specific source MAC address ingress on a port different than what IS-IS expected.
`rpfc-unicast-sa`	Displays the total number of SPBM RPFC unicast packets dropped. These drops occur when packets with a specific source MAC address ingress on a port different than what IS-IS expected.
`unknown-multicast-da`	Displays the total number of SPBM unknown multicast DA packets dropped. These drops occur when the multicast destination MAC address of the packet

	is not known.
unknown-unicast-da	Displays the total number of SPBM unknown unicast DA packets dropped. These drops occur when the unicast destination MAC address of the packet is not known.
unknown-unicast-sa	Displays the total number of SPBM unknown unicast SA packets dropped. These drops occur when the unicast source MAC address of the packet is not known.

©Avaya Inc. 2015 All Rights Reserved.

show isis spbm ip-multicast-route

Displays IP multicast over SPBM route information.

Syntax

- `show isis spbm ip-multicast-route`
- `show isis spbm ip-multicast-route all`
- `show isis spbm ip-multicast-route detail`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`all`	Displays all route information.
`detail`	Displays detailed route information.

©Avaya Inc. 2015 All Rights Reserved.

show isis spbm ip-multicast-route group

Displays IP multicast route information by multicast group address.

Syntax

- `show isis spbm ip-multicast-route group {A.B.C.D}`
- `show isis spbm ip-multicast-route group {A.B.C.D} detail`
- `show isis spbm ip-multicast-route group {A.B.C.D} source {A.B.C.D}`
- `show isis spbm ip-multicast-route group {A.B.C.D} source {A.B.C.D} detail`
- `show isis spbm ip-multicast-route group {A.B.C.D} source {A.B.C.D} source-beb WORD<0-255>`
- `show isis spbm ip-multicast-route group {A.B.C.D} source {A.B.C.D} source-beb WORD<0-255> detail`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`detail`	Displays detailed route information.
`group {A.B.C.D}`	Displays route information by multicast group address.
`source {A.B.C.D}`	Displays information for the source IP address.
`source-beb WORD<0-255>`	Displays information for a specific backbone edge bridge.

©Avaya Inc. 2015 All Rights Reserved.

show isis spbm ip-multicast-route vlan

Displays IP multicast route information by VLAN.

Syntax

- `show isis spbm ip-multicast-route vlan <0-4084>`
- `show isis spbm ip-multicast-route vlan <0-4084> detail`
- `show isis spbm ip-multicast-route vlan <0-4084> group {A.B.C.D}`
- `show isis spbm ip-multicast-route vlan <0-4084> group {A.B.C.D} detail`
- `show isis spbm ip-multicast-route vlan <0-4084> group {A.B.C.D} source {A.B.C.D}`
- `show isis spbm ip-multicast-route vlan <0-4084> group {A.B.C.D} source {A.B.C.D} detail`
- `show isis spbm ip-multicast-route vlan <0-4084> group {A.B.C.D} source {A.B.C.D} source-beb WORD<0-255>`
- `show isis spbm ip-multicast-route vlan <0-4084> group {A.B.C.D} source {A.B.C.D} source-beb WORD<0-255> detail`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`detail`	Displays detailed route information.
`group {A.B.C.D}`	Specifies the multicast group address.
`source {A.B.C.D}`	Displays information for the source IP address.
`source-beb WORD<0-255>`	Displays information for a specific backbone edge bridge.
`vlan <1-4084>`	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show isis spbm ip-multicast-route vrf

Displays IP multicast route information by VRF.

Syntax

- `show isis spbm ip-multicast-route vrf WORD<1-16>`
- `show isis spbm ip-multicast-route vrf WORD<1-16> detail`
- `show isis spbm ip-multicast-route vrf WORD<1-16> group {A.B.C.D}`
- `show isis spbm ip-multicast-route vrf WORD<1-16> group {A.B.C.D} detail`
- `show isis spbm ip-multicast-route vrf WORD<1-16> group {A.B.C.D} source {A.B.C.D}`
- `show isis spbm ip-multicast-route vrf WORD<1-16> group {A.B.C.D} source {A.B.C.D} detail`
- `show isis spbm ip-multicast-route vrf WORD<1-16> group {A.B.C.D} source {A.B.C.D} source-beb WORD<1-255>`
- `show isis spbm ip-multicast-route vrf WORD<1-16> group {A.B.C.D} source {A.B.C.D} source-beb WORD<1-255> detail`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`detail`	Displays detailed route information.
`group {A.B.C.D}`	Displays route information by multicast group address.
`source {A.B.C.D}`	Displays information for the source IP address.
`source-beb WORD<0-255>`	Displays information for a specific backbone edge bridge.
`vrf WORD<1-16>`	Specifies the VRF name.

©Avaya Inc. 2015 All Rights Reserved.

show isis spbm ip-multicast-route vsn-isid

Displays IP multicast route information by VSN I-SID.

Syntax

- `show isis spbm ip-multicast-route vsn-isid <1-16777215>`
- `show isis spbm ip-multicast-route vsn-isid <1-16777215> detail`
- `show isis spbm ip-multicast-route vsn-isid <1-16777215> group {A.B.C.D}`
- `show isis spbm ip-multicast-route vsn-isid <1-16777215> group {A.B.C.D} detail`
- `show isis spbm ip-multicast-route vsn-isid <1-16777215> group {A.B.C.D} source {A.B.C.D}`
- `show isis spbm ip-multicast-route vsn-isid <1-16777215> group {A.B.C.D} source {A.B.C.D} detail`
- `show isis spbm ip-multicast-route vsn-isid <1-16777215> group {A.B.C.D} source {A.B.C.D} source-beb WORD<1-255>`
- `show isis spbm ip-multicast-route vsn-isid <1-16777215> group {A.B.C.D} source {A.B.C.D} source-beb WORD<1-255> detail`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<1-16777215>`	Specifies the VSN I-SID.
`detail`	Displays detailed route information.
`group {A.B.C.D}`	Displays route information by multicast group address.
`source {A.B.C.D}`	Displays information for the source IP address.
`source-beb WORD<0-255>`	Displays information for a specific backbone edge bridge.

©Avaya Inc. 2015 All Rights Reserved.

show isis spbm ip-unicast-fib

Display the Intermediate-System-to-Intermediate-System (IS-IS) Shortest Path Bridging MAC (SPBM) IP unicast Forwarding Information Database (FIB) entries. If you do not use an optional parameter, the command output shows entries for the GlobalRouter (GRT).

Syntax

- `show isis spbm ip-unicast-fib`
- `show isis spbm ip-unicast-fib all`
- `show isis spbm ip-unicast-fib id <1-16777215>`
- `show isis spbm ip-unicast-fib spbm-nh-as-mac`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`all`	Displays the IP unicast Forwarding Information Base (FIB) entries for all VRFs.
`id <1-16777215>`	Displays the IP unicast Forwarding Information Base (FIB) for the given service instance identifier (I-SID) value.
`spbm-nh-as-mac`	Displays the next hop Backbone MAC entry in the IP unicast Forwarding Information Base (FIB).

©Avaya Inc. 2015 All Rights Reserved.

show isis spbm i-sid

Display the Intermediate-System-to-Intermediate-System (IS-IS) Shortest Path Bridging MAC (SPBM) multicast Forwarding Information Base (FIB) calculation results by service instance identifier (I-SID).

Syntax

- `show isis spbm i-sid { all | config | discover }`
- `show isis spbm i-sid { all | config | discover } id <1-16777215>`
- `show isis spbm i-sid { all | config | discover } nick-name x.xx.xx - 2.5 bytes`
- `show isis spbm i-sid { all | config | discover } vlan <0-4084>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{ all | config | discover }`	all: Displays all service instance identifier (I-SID) entries; config: Displays the configured I-SID entries; and discover: Displays discovered I-SID entries.
`id <1-16777215>`	Displays service instance identifier (I-SID) information for the specified I-SID.
`nick-name x.xx.xx - 2.5 bytes`	Displays service instance identifier (I-SID) information for the specified nick-name.
`vlan <0-4084>`	Displays service instance identifier (I-SID) information for the specified Shortest Path Bridging MAC (SPBM) VLAN.

©Avaya Inc. 2015 All Rights Reserved.

show isis spbm multicast

Displays the status of the global SPBM multicast configuration.

Syntax

- `show isis spbm multicast`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show isis spbm multicast-fib

Display the Intermediate-System-to-Intermediate-System (IS-IS) Shortest Path Bridging MAC (SPBM) multicast Forwarding Information Database (FIB) entries.

Syntax

- `show isis spbm multicast-fib`
- `show isis spbm multicast-fib i-sid <1-16777215>`
- `show isis spbm multicast-fib nick-name x.xx.xx - 2.5 bytes`
- `show isis spbm multicast-fib summary`
- `show isis spbm multicast-fib vlan <2-4084>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`i-sid <1-16777215>`	Displays the FIB for the specified I-SID.
`nick-name x.xx.xx - 2.5 bytes`	Displays the FIB for the specified nickname.
`summary`	Displays a summary of the FIB.
`vlan <2-4084>`	Specifies the VLAN ID for which to display the FIB.

©Avaya Inc. 2015 All Rights Reserved.

show isis spbm nick-name

Display the Shortest Path Bridging MAC (SPBM) configurations for a specific nick-name.

Syntax

- `show isis spbm nick-name`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show isis spbm unicast-fib

Display the Shortest Path Bridging MAC (SPBM) unicast Forwarding Information Base (FIB).

Syntax

- `show isis spbm unicast-fib`
- `show isis spbm unicast-fib b-mac 0x00:0x00:0x00:0x00:0x00:0x00`
- `show isis spbm unicast-fib summary`
- `show isis spbm unicast-fib vlan <2-4084>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`b-mac 0x00:0x00:0x00:0x00:0x00:0x00`	Displays the Forwarding Information Base (FIB) entry for the specified Backbone MAC (BMAC).
`summary`	Displays a summary of the Forwarding Information Base (FIB).
`vlan <2-4084>`	Displays the Forwarding Information Base (FIB) entry for the specified Shortest Path Bridging MAC (SPBM) VLAN.

©Avaya Inc. 2015 All Rights Reserved.

show isis spbm unicast-tree

Display the Shortest Path Bridging MAC (SPBM) unicast tree.

Syntax

- `show isis spbm unicast-tree <2-4084>`
- `show isis spbm unicast-tree <2-4084> destination xxxx.xxxx.xxxx - 6 bytes`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<2-4084>`	Specifies the Shortest Path Bridging MAC (SPBM) Backbone VLAN ID.
`destination xxxx.xxxx.xxxx - 6 bytes`	Displays the unicast tree for the specified destination.

©Avaya Inc. 2015 All Rights Reserved.

show isis statistics

Display Intermediate-System-to-Intermediate-System (IS-IS) statistics.

Syntax

- `show isis statistics`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show isis system-id

Display Intermediate-System-to-Intermediate-System (IS-IS) system ID.

Syntax

- `show isis system-id`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ist mlt

Display MultiLink Trunking (MLT) interswitch Trunk (IST) information.

Syntax

- `show ist mlt`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ist stat

Show IST message statistics.

Syntax

- `show ist stat`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show khi cpp

View key health information about the control processors.

Syntax

- `show khi cpp iocop-statistics [<3-12>]`
- `show khi cpp port-statistics [{slot/port[-slot/port][,...]}]`
- `show khi cpp protocol-drops`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<3-12>	Specifies the slot number.
slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

show khi forwarding

Display forwarding health information on the switch.

Syntax

- `show khi forwarding [<3-12>]`
- `show khi forwarding ifp [<3-12>]`
- `show khi forwarding k2 [<3-12>]`
- `show khi forwarding mac [<3-12>]`
- `show khi forwarding mac-higig [<3-12>]`
- `show khi forwarding qe [<3-12>]`
- `show khi forwarding rsp [<3-12>]`
- `show khi forwarding sierra [<3-12>]`
- `show khi forwarding zagros [<3-12>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<3-12>	Specifies the interface slot on the switch.
ifp <3-12>	Shows IFP statistics.
k2 <3-12>	Shows K2 data path health indicators.
mac <3-12>	Shows MAC data path health indicators.
mac-higig <3-12>	Shows Mac-higig data path health indicators.
qe <3-12>	Shows QE2000 data path health indicators.
rsp <3-12>	Shows RSP data path health indicators. Note: The output displays differently for first generation and second generation modules.
sierra <3-12>	Shows Sierra data path health indicators.
zagros <3-12>	Shows Zagros data path health indicators. The caret (^) symbol is used to denote the peak value in the output for the show khi forwarding zagros command. An entry that

reads 5^ 0 denotes a peak value of 5 and a current value of 0.

©Avaya Inc. 2015 All Rights Reserved.

show khi performance

View the performance of the various components of the switch by checking their key health indicators.

Syntax

- `show khi performance [buffer-pool|cpu|memory|process|pthread|slabinfo] {slot [-slot] [,...]}`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`buffer-pool {slot [-slot] [,...]}`	Indicates khi of the buffer-pool on the switch. {slot [-slot] [,...]} specifies the slot number. Valid slots are 1 to 12,or SF1 to SF6, or all.
`cpu {slot [-slot] [,...]}`	Indicates khi of the CPU on the switch. {slot [-slot][,...]} specifies the slot number. Valid slots are 1 to 12, or SF1 to SF6, or all.
`memory{slot [-slot] [,...]}`	Indicates khi of memory on the switch. {slot [-slot][,...]} specifies the slot number. Valid slots are 1 to 12, or SF1 to SF6, or all.
`process{slot [-slot] [,...]}`	Indicates khi of the process on the switch. {slot [-slot][,...]} specifies the slot number. Valid slots are 1 to 12, or SF1 to SF6, or all.
`pthread{slot [-slot] [,...]}`	Indicates khi of pthread on the switch. {slot [-slot][,...]} specifies the slot number. Valid slots are 1 to 12, or SF1 to SF6, or all.
`slabinfo{slot [-slot] [,...]}`	Indicates khi of the slab information on the switch. {slot[-slot] [,...]} specifies the slot number. Valid slots are 1 to 12, or SF1 to SF6, or all.

©Avaya Inc. 2015 All Rights Reserved.

show lacp

View Link Aggregation Control Protocol (LACP) configuration information to determine the LACP parameters and to ensure your configuration is correct.

Syntax

- `show lacp`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`actor-admin interface [gigabitethernet][vid<1-4084>] {slot/port[-slot/port][,...]}`	Shows LACP actor administrative information for all interfaces or the specified interface. <1-4084> is the VLAN ID or list of VLAN IDs to show only ports attached to a particular VLAN. {slot/port[-slot/port][,...]} is the slot and port list.
`actor-oper interface [gigabitethernet] [vid <1-4084>] {slot/port[-slot/port][,...]}`	Shows LACP actor operational information for all interfaces or the specified interface. <1-4084> is the VLAN ID or list of VLAN IDs to show only ports attached to a particular VLAN. {slot/port[-slot/port][,...]} is the slot and port list.
`extension interface [gigabitethernet] [vid <1-4084>] {slot/port[-slot/port][,...]}`	Shows LACP timer information for all interfaces or the specified interface. <1-4084> is the VLAN ID or list of VLAN IDs to show only ports attached to a particular VLAN. {slot/port[-slot/port][,...]} is the slot and port list.
`interface [gigabitethernet] [vid <1-4084>] {slot/port[-slot/port][,...]}`	Shows all LACP port configuration information for all interfaces or the specified interface.
`interface mlt [<64-6399>]`	Shows the MLT LACP information for all MLTs or the specific MLT index.
`partner-admin interface [gigabitethernet][vid<1-4084>] {slot/port[-slot/port][,...]}`	Shows LACP partner administrative information for all interfaces or the specified interface. <1-4084> is the VLAN ID or list of VLAN IDs to show only ports attached to a particular VLAN. {slot/port[-slot/port][,...]} is the slot and port list.
`partner-oper interface [gigabitethernet][vid<1-4084>] {slot/port[-slot/port][,...]}`	Shows LACP partner operational information for all interfaces or the specified interface. <1-4084> is the VLAN ID or list of VLAN IDs to show only ports attached to a particular VLAN. {slot/port[-slot/port][,...]} is the slot and port list.

©Avaya Inc. 2015 All Rights Reserved.

show lacp interface

View Link Aggregation Control Protocol (LACP) statistics for each port to monitor LACP performance of the port.

Syntax

- `show lacp interface`
- `show lacp interface gigabitethernet`
- `show lacp interface gigabitethernet {slot/port[-slot/port][,...]}`
- `show lacp interface gigabitethernet vid <1-4084>`
- `show lacp interface gigabitethernet vid <1-4084> {slot/port[-slot/port][,...]}`
- `show lacp interface mlt`
- `show lacp interface mlt <64-6399>`
- `show lacp interface mlt id <1-512>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Specifies the slot and the port number.
`<mlt|gigabitethernet>`	Specifies the interface type for LACP. The ifindex of the MLT ranges from 64 to 6399.
`vid <1-4084>`	Shows only ports attached to a particular VLAN id in the range of 1 to 4084.

©Avaya Inc. 2015 All Rights Reserved.

show license

Display the existing software licenses on the platform.

Syntax

- `show license`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show link-flap-detect

Show link-flap-detect configuration.

Syntax

- `show link-flap-detect`

Default

None

Command mode

Privileged EXEC

©Avaya Inc. 2015 All Rights Reserved.

show logging

Use this command to display logging information.

Syntax

- `show logging config`
- `show logging info`
- `show logging level`
- `show logging transferFile <1-10>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`config`	Displays the global logging information.
`info`	Displays the logging information.
`level`	Displays the configuration of event logging.
`transferFile <1-10>`	Displays the current level parameter settings and next level directories. <1-10> specifies the TFTP/FTP host IP address.

©Avaya Inc. 2015 All Rights Reserved.

show logging file

View log files by file name, category, severity, or CP module to identify possible problems. Note: Unprintable characters in log and trace messages are encoded in C language hexadecimal notation in the string and surrounded with <UNPRINTABLE> ... </UNPRINTABLE> tag. For example, the device converts a 4-byte sequence of 0x01, 0x02, 0xfe, 0xff to \x01\x02\xfe\xff, and adds the <UNPRINTABLE>...</UNPRINTABLE> tag to the log or trace message.

Syntax

- `show logging file [alarm][CPU WORD<0-100>] [event-code WORD<0-10>}] [module WORD<0-100>][name-of-file WORD<1-99>] [save-to-file WORD<1-99>] [severity WORD<0-25>] [tail][vrf WORD<0-32>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
alarm	Displays alarm log entries.
CPU WORD <0-100>	Filters and list the logs according to the CP module that generated it. Specify a string length of 0-100 characters. To specify multiple filters, separate each CP module by the vertical bar (|), for example, CPU1|CPU2.
event-code WORD<0-10>	Specifies a number that precisely identifies the event reported. WORD<0-10> specifies the event code in the format: {0x0-0x00FFFFFF| 0x0-0x00FFFFFF}.
module <WORD 0-100>	Filters and list the logs according to module. Specify a string length of 0-100 characters. Categories include SNMP, EAP, RADIUS, RMON, WEB, STG, IGMP, HW, MLT, FILTER, QOS, CLILOG, SW, CPU, IP, VLAN, IPMC, IP-RIP, OSPF, PIM, POLICY, RIP, and SNMPLOG. To specify multiple filters, separate each category by the vertical bar (|), for example, OSPF|FILTER|QOS. Use the command show logging file module clilog to view the ACLI log. Use the command show logging file module snmplog to view the SNMP log.
name-of-file WORD <1-99>	Displays the valid logs from this file. For example, /intflash/logcopy.txt. You cannot use this command on the current log file-the file into which the messages are currently logged). Specify a string length of 1-99 characters.
save-to-file WORD <1-99>	Redirects the output to the specified file and removes all encrypted information. The tail option is not supported with the save-to-file option. Specify a string length of 1-99 characters. The format for the file name is: /intflash/<file>, /extflash/<file>, /usb/<file>, /mnt/intflahs/<file>, and /mnt/extflash/<file>. /mnt/intflash is the internal flash of the second CP module (the one to which you are not connected) /mnt/extflash is the external flash of the second CP module (the one to which you are not connected) WORD<1-99> is a string of 1-99 characters.
severity WORD <0-	Filters and list the logs according to severity. Choices include INFO, ERROR, WARNING, FATAL. To specify multiple filters, separate each severity by the vertical bar (|), for

25>	example, ERROR|WARNING|FATAL.
tail	Shows the last results first.
vrf WORD<0-32>	Specifies the name of a VRF instance to show log messages that only pertain to that VRF.

©Avaya Inc. 2015 All Rights Reserved.

show mac-security mac-da-filter

Display the global level MAC addresses to be filtered.

Syntax

- `show mac-security mac-da-filter`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show mirror-by-port

Show mirror-by-port diagnostic information.

Syntax

- `show mirror-by-port WORD<1-1024>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
WORD<1-1024>	Displays mirror-by-port diagnostic information. Mirror ID list {1-479}.

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

show mlt

Display MultiLink Trunking (MLT) information, including port type, port members and designated ports.

Syntax

- `show mlt <1-512>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<1-512>	Specifies the MLT ID. The value ranges from 1-512.

©Avaya Inc. 2015 All Rights Reserved.

show mlt error collision

View information about collision errors to obtain information about collision errors in the specified MLT, or for all MLTs.

Syntax

- `show mlt error collision [<1-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<1-512>	Specifies the MLT ID. The value ranges from 1-512.

©Avaya Inc. 2015 All Rights Reserved.

show mlt error main

View information about Ethernet errors to display information about the types of Ethernet errors sent and received by the specified MLT or all MLTs.

Syntax

- `show mlt error main [<1-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<1-512>	Specifies the MLT ID. The value ranges from 1-512.

©Avaya Inc. 2015 All Rights Reserved.

show mlt stats

View MLT statistics to display MultiLinkTrunking statistics for the switch or for the specified MLT ID.

Syntax

- `show mlt stats <1-512>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<1-512>	Specifies the MLT ID. The value ranges from 1-512.

©Avaya Inc. 2015 All Rights Reserved.

show monitor-statistics

Display monitor timer configurations, including duration and interval.

Syntax

- `show monitor-statistics`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show multicast software-forwarding

Show the software forwarding configuration.

Syntax

- `show multicast software-forwarding`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show multicast square-smlt

Show the multicast square MLT distribution configuration.

Syntax

- `show multicast square-smlt`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ntp

View the Network Time Protocol (NTP) server status statistics.

Syntax

- `show ntp [key]`
- `show ntp [server]`
- `show ntp [statistics]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`key`	Specifies to show NTP authentication key information.
`server`	Specifies to show NTP server information.
`statistics`	Specifies to show NTP statistics information.

©Avaya Inc. 2015 All Rights Reserved.

show pcap

Display Packet Capture tool (PCAP) information.

Syntax

- `show pcap`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show pcap capture-filter

Display packet capture (PCAP) filter configurations.

Syntax

- `show pcap capture-filter <1-1000>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<1-10>	Specifies the capture filter ID.

©Avaya Inc. 2015 All Rights Reserved.

show pcap dump

You can view packets using a ACLI session and the Secondary CPU. Dumping a large number of captured packets is CPU intensive. The switch does not respond to any commands while the dump is in progress. Avaya recommends you use this command only when it is absolutely necessary. However, there is no degradation in normal traffic handling or switch failover. Note: If a PCAP dump is in progress on the standby, you will encounter the following error if you try to make a PCAP configuration change: Error: PCAP dump in progress. Command not allowed.

Syntax

- `show pcap dump`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show pcap port

Display Packet Control (PCAP) port information to ensure accuracy.

Syntax

- `show pcap port`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show pcap stats

View Packet Control (PCAP) statistics to manage network performance.

Syntax

- `show pcap stats`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show pluggable-optical-modules

View Digital Diagnostic Interface (DDI) module information to view SFP and SFP+ manufacturing information and characteristics, temperature and voltage information, and configuration details.

Syntax

- `show pluggable-optical-modules basic [{slot/port [-slot/port][,...]}]`
- `show pluggable-optical-modules config`
- `show pluggable-optical-modules detail [{slot/port [-slot/port][,...]}]`
- `show pluggable-optical-modules temperature [{slot/port [-slot/port][,...]}]`
- `show pluggable-optical-modules voltage [{slot/port [-slot/port][,...]}]`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Optionally, identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`basic`	Shows basic SFP and SFP+ information. The device reports qualified optics as Avaya in the type field. The device reports non-qualified best-effort optics as a different manufacturer in the type field. Unsupported optics display as unsupported in the type field, and do not operate in the system.
`config`	Shows pluggable optical modules configuration information.
`detail`	Shows detailed SFP and SFP+ information. Note: Digital Diagnostic Interface (DDI) module information for RxPower can output false alerts. The MSA (Multi-source Agreement) between manufacturers of SFP and SFP+ devices specifies a +/- 3dB accuracy tolerance for optical power measurements. To minimize false warnings or alarms due to this inaccuracy, the thresholds for low and high TxPower and for low RxPower are offset by this tolerance. High RxPower thresholds are not offset due to the potential for receiver saturation and damage that can result over the long-term, however, this increases the possibility of false alerts. If high RxPower alerts occur, but the link operates normally, consider this tolerance. If the link fails to operate, consider the possibility that the optical receiver is being over-driven, and attempt to correct the condition.
`temperature`	Shows SFP and SFP+ temperature information.
`voltage`	Shows SFP and SFP+ voltage information.

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

show ports statistics ospf extended

Use statistics to help you monitor Open Shortest Path First (OSPF) performance.

Syntax

- `show ports statistics ospf extended {slot/port [-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Specifies the slot and the port number or a range of ports.

©Avaya Inc. 2015 All Rights Reserved.

show ports statistics ospf main

Use statistics to help you monitor Open Shortest Path First (OSPF) performance.

Syntax

- `show ports statistics ospf main {slot/port [-slot/port][,...]}`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Specifies the slot and the port number or a range of ports.

©Avaya Inc. 2015 All Rights Reserved.

show qos 802.1p-override

Display the 802.1p override status for a port or VLAN.

Syntax

- `show qos 802.1p-override gigabitethernet {slot/port[-slot/port][,...]}`
- `show qos 802.1p-override vlan <1-4084>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-4084>`	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show qos egressmap

Display the Quality of Service (QoS) egress mappings.

Syntax

- `show qos egressmap`
- `show qos egressmap 1p [<0-7>]`
- `show qos egressmap ds [<0-7]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
1p	Displays the QoS level to IEEE 802.1p priority mapping.
1p<0-7>	Displays the QoS level to IEEE 802.1p priority mapping. Specifies the QoS level. Each QoS level has a default IEEE 1P value: level 0 - 1 , level 1 - 0, level 2 - 2, level 3 - 3, level 4 - 4, level 5 - 5, level 6 - 6, and level 7 - 7. The system reserves level 7 for Network Control.
ds	Displays the QoS level to DS byte mapping.
ds<0-7>	Displays the QoS level to DS byte mapping. Each QoS level has a default DSCP mapping: level 0 - 0, level 1 - 0, level 2 - 10, level 3 - 18, level 4 - 26, level 5 - 34, level 6 - 46, and level 7 - 46.

©Avaya Inc. 2015 All Rights Reserved.

show qos ingressmap

Ensure the accuracy of the ingress configuration.

Syntax

- `show qos ingressmap`
- `show qos ingressmap 1p [<0-7>]`
- `show qos ingressmap ds [<0-63]`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show qos lossless-802.1p

Display the 802.1p value used for Lossless Ethernet.

Syntax

- `show qos lossless-802.1p`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show qos policer

Display ingress rate-limiting information for an interface.

Syntax

- `show qos policer interface gigabitethernet [{slot/port[-slot/port][,...]}]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

show qos policy-config

Ensure the accuracy of the Quality of Service (QoS) policy configuration.

Syntax

- `show qos policy-config [<1-16000>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<1-16000>	Specifies the policer ID number.

©Avaya Inc. 2015 All Rights Reserved.

show qos shaper

Display egress rate-limiting information for an interface.

Syntax

- `show qos shaper interface gigabitethernet [{slot/port[-slot/port][,...]}]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

show qos statistics policy

Display individual queue statistics with the following procedure.

Syntax

- `show qos statistics policy <1-16000> slot {slot [-slot][,...]}`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<1-16000>`	Specifies the policy id in the range of 1 to 16000.
`slot {slot [-slot][,...]}`	Specifies the slot number for statistics collection. The valid slots are between 3 to 12.

©Avaya Inc. 2015 All Rights Reserved.

show radius

Display the global status of Remote Access Dial-In User Services (RADIUS) information.

Syntax

- `show radius`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show radius-server

Display the Remote Access Dial-In User Services (RADIUS) server information.

Syntax

- `show radius-server`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show radius-server statistics

Display current Remote Access Dial-In User Services (RADIUS) server configurations.

Syntax

- `show radius-server statistics`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show radius snmp

Display the global status of Remote Access Dial-In User Services (RADIUS) information.

Syntax

- `show radius snmp`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show remote-mirroring

Display the remote mirroring configuration information.

Syntax

- `show remote-mirroring interfaces <gigabitEthernet>[enable] [mode <source|termination>] [srcMac <0x00:0x00:0x00:0x00:0x00:0x00>] [dstMac <0x00:0x00:0x00:0x00:0x00:0x00>] [ether-type <0x00-0xffff>] [vlan-id <1-4084>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`dstMac <0x00:0x00:0x00:0x00:0x00:0x00>`	Sets the destination MAC address for use in the remote mirroring encapsulation header. The mirrored packet is sent to this MAC address. The DstMac is used only for RMS ports. For RMT ports, one of the unused MAC addresses from the switch port MAC address range is used. This MAC address is saved in the configuration file.
`enable`	Enables remote mirroring on the port. When remote mirroring is enabled, the following events occur: A static entry for the DstMac is added to the Forwarding Database (FDB). All packets that come with this remote mirroring DstMac are sent to the RMT port. The switch periodically (once in 10 seconds) transmits broadcast Layer 2 packets in the associated VLAN so that all nodes in the network can learn the DstMac.
`ether-type <0x00-0xffff>`	Specifies the Ethertype of the remote mirrored packet. The default value is 0x8103.
`mode <source|termination>`	Specifies whether the port is an RMT (mode is termination) or an RMS (mode is source).
`srcMac <0x00:0x00:0x00:0x00:0x00:0x00>`	Sets the source MAC address for use in the remote mirroring encapsulation header. The mirrored packet is sent from the RMS port, and the source MAC parameter in the header is derived from this address. The source MAC address of the encapsulated frame contains the first 45 bits of this MAC address. The three least significant bits are derived from the port number of the RMS port. The MAC address of the port is used as the default value.
`vlan-id <1-4084>`	Specifies to which VLAN the remote mirroring destination MAC address belongs. This must be a port-based VLAN.

Used only for Remote Mirroring Termination (RMT) ports. When the RMT port is removed from the last VLAN in the list, RMT is disabled on the port.

©Avaya Inc. 2015 All Rights Reserved.

show rmon

View Remote Network Monitoring (RMON) settings to see information about alarms, statistics, events, or the status of RMON on the switch.

Syntax

- `show rmon [alarm|event|history|log|stats]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`alarm`	Displays Remote Network Monitoring (RMON) alarm information on the switch.
`event`	Displays Remote Network Monitoring (RMON) events information on the switch.
`history`	Displays Remote Network Monitoring (RMON) history on the switch.
`log`	Displays Remote Network Monitoring (RMON) log information on the switch.
`stats`	Displays Remote Network Monitoring (RMON) statistics information on the switch.

©Avaya Inc. 2015 All Rights Reserved.

show rmon stats

View Remote Network Monitoring (RMON) statistics to manage network performance.

Syntax

- `show rmon stats`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show route-map

Display current information about the IP route policy.

Syntax

- `show route-map [WORD <1-64>] [seq <1-65535>] [vrf WORD<1-16>] [vrfids WORD<0-512>]`
- `show route-map detail [vrf WORD<1-16>] [vrfids WORD<0-512>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`detail`	Specifies the long format information of the route map.
`vrf WORD<1-16>`	Specifies the name of the VRF.
`vrfids WORD<0-512>`	Specifies the ID of the VRF and is an integer in the range of 0 to 512.
`WORD<1-64> seq <1-65535>`	Displays a route policy with a policy name and a sequence number. WORD<1-64> is the policy name. seq <1-65535> is the sequence number.

©Avaya Inc. 2015 All Rights Reserved.

show routing statistics

View port routing statistics to manage network performance.

Syntax

- `show routing statistics interface`
- `show routing statistics interface gigabitethernet [{slot/port [-slot/port][,...]}]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`gigabitethernet{slot/port [-slot/port][,...]}`	Indicates the interface type and the slot and the port number.

©Avaya Inc. 2015 All Rights Reserved.

show running-config

Display the current switch configuration.

Syntax

- `show running-config`
- `show running-config module {boot | cfm | cli | cluster | diag | filter | ip | ipv6 | isis | lacp | mlt | naap | nsna | ntp | port | qos | radius | rmon | slamon | slpp | spbm | stg | sys | tacacs | vlan | vsptalk | web}`
- `show running-config verbose`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`module {boot | cfm | cli | cluster | diag | filter | ip | ipv6 | isis | lacp | mlt | naap | nsna | ntp | port | qos | radius | rmon | slamon | slpp | spbm | stg | sys | tacacs | vlan | vsptalk | web}`	Specifies the command group for which you request configuration settings.
`verbose`	Specifies the complete list of configuration information on the switch.

©Avaya Inc. 2015 All Rights Reserved.

show slot

Show slot configuration for the interface modules.

Syntax

- `show slot <3-12>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
<3-12>	Specifies the interface slot number.

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

show slpp

Use Simple Loop Prevention Protocol (SLPP) information to view loop information.

Syntax

- `show slpp`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show slpp interface

Show Simple Loop Prevention Protocol (SLPP) information for a port so that you can view the loop information for a port.

Syntax

- `show slpp interface gigabitethernet [ {slot/port[-slot /port][,...]}]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

show smlt

View all ports for a single port SMLT to ensure the correct ports are configured.

Syntax

- `show smlt mlt`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`mlt`	Displays SMLT information for the MLT interface.

©Avaya Inc. 2015 All Rights Reserved.

show snmplog

View the contents of the Simple Network Management Protocol (SNMP) log. This command only applies to log files generated by releases prior to Release 3.2. The command is replaced by show logging file module snmplog

Syntax

- `show snmplog`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show snmp-server

Display Simple Network Management Protocol (SNMP) system information to view trap and authentication profiles.

Syntax

- `show snmp-server`
- `show snmp-server community`
- `show snmp-server context`
- `show snmp-server group`
- `show snmp-server host`
- `show snmp-server notify-filter`
- `show snmp-server user`
- `show snmp-server view`
- `show snmp-server view viewname WORD<0-32>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`community`	Displays the SNMP community table.
`context`	Displays vacm context table.
`group`	Displays SNMP group access table.
`host`	Displays SNMP host details.
`notify-filter`	Displays SNMP notify-filter details.
`user`	Displays SNMP users.
`view`	Displays SNMP MIB view table.
`viewname WORD<0-32>`	Displays the view for a particular view name.

©Avaya Inc. 2015 All Rights Reserved.

show software

Display unpacked software releases information.

Syntax

- `show software`
- `show software detail`
- `show software release WORD<1-99>`
- `show software verbose`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`detail`	Displays software release in detail mode.
`release <WORD 1-99>`	Specifies a specific software release to be displayed in the range of 1 to 99.
`verbose`	Includes a date and time stamp to indicate when you last added, activated, and committed a software release. The output also indicates if you manually committed the software release, or if you used the automatic commit feature.

©Avaya Inc. 2015 All Rights Reserved.

show software patch

Display the unpacked software patching information that is to be updated on the chassis of the switch.

Syntax

- show software patch
- show software patch all
- show software patch all detail
- show software patch all patch-ids WORD<1-255>
- show software patch all patch-ids WORD<1-255> WORD<1-255>
- show software patch all patch-ids WORD<1-255> WORD<1-255> WORD<1-255>
- show software patch all patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255>
- show software patch all patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255>
- show software patch all patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255>
- show software patch all patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255>
- show software patch all patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255>
- show software patch all verbose
- show software patch all version WORD<1-255>
- show software patch applied
- show software patch candidate
- show software patch detail
- show software patch patch-ids WORD<1-255>
- show software patch patch-ids WORD<1-255> WORD<1-255>
- show software patch patch-ids WORD<1-255> WORD<1-255> WORD<1-255>
- show software patch patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255>
- show software patch patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255>
- show software patch patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255>
- show software patch patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255>

- `show software patch patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255>`
- `show software patch verbose`
- `show software patch version WORD<1-255>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`all`	Displays the patch status for all the valid patches.
`applied`	Displays patches that are currently applied and active.
`candidate`	Displays patches that are eligible for activation against the active software version.
`detail`	Displays detailed patch status information.
`patch-ids WORD <1-255>`	Displays information for the specified patch ids. WORD <1-255> specifies the name of the patch file for the information to be displayed.
`verbose`	Displays verbose patch status information.
`version WORD <1-255>`	Specifies the software version used to display the software patches that are candidate or applied.

©Avaya Inc. 2015 All Rights Reserved.

show spanning-tree bpdu-filtering

View the BPDU Filtering configuration.

Syntax

- `show spanning-tree bpdu-filtering`
- `show spanning-tree bpdu-filtering {slot/port[-slot/port][,...]}`
- `show spanning-tree bpdu-filtering GigabitEthernet`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`GigabitEthernet`	Shows information for all GigabitEthernet interfaces.

©Avaya Inc. 2015 All Rights Reserved.

show spanning-tree config

Query the change detection setting to show the port information.

Syntax

- `show spanning-tree config`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show spanning-tree mstp config

View the Multiple Spanning Tree Protocol (MSTP) configurations to display the MSTP-related bridge-level VLAN and region information.

Syntax

- `show spanning-tree mstp config`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show spanning-tree mstp msti config

Display the configuration for one or all Multiple Spanning Tree Protocol (MSTP) instance IDs.

Syntax

- `show spanning-tree mstp msti config [<1-63>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<1-63>	Specifies the MSTP instance ID.

©Avaya Inc. 2015 All Rights Reserved.

show spanning-tree mstp msti port

Shows the configuration, role, or statistics information of an MSTP port.

Syntax

- `show spanning-tree mstp msti port config [{slot/port [-slot/port][,...]}]`
- `show spanning-tree mstp msti port role [{slot/port [-slot/port][,...]}]`
- `show spanning-tree mstp msti port statistics [{slot/port [-slot/port][,...]}]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`config {slot/port [-slot/port][,...]}`	Shows the configuration information of an MSTP port.
`role {slot/port [-slot/port][,...]}`	Shows the role information of an MSTP port.
`statistics {slot/port [-slot/port][,...]}`	Shows the statistics information of an MSTP port.

©Avaya Inc. 2015 All Rights Reserved.

show spanning-tree mstp port role

Display Multiple Spanning Tree Protocol (MSTP) port information.

Syntax

- `show spanning-tree mstp port config [{slot/port[-slot/port][,...]} ]`
- `show spanning-tree mstp port role [{slot/port[-slot/port][,...]} ]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Displays the MSTP port information.
`config [{slot/port[-slot/port][,...]} ]`	Displays the MSTP port configurations, which display MSTP-related bridge-level VLAN and region information.
`role [{slot/port[-slot/port][,...]} ]`	Displays the MSTP port information to display the MSTP, CIST port, and MSTI port information maintained by every port of the common spanning tree.

©Avaya Inc. 2015 All Rights Reserved.

show spanning-tree mstp port statistics

Display Multiple Spanning Tree Protocol (MSTP) Multiple Spanning Tree Instance (MSTI) information to ensure the feature is configured correctly for your network.

Syntax

- `show spanning-tree mstp port statistics [{slot/port [-slot/port][,...]}]`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show spanning-tree mstp statistics

Display Multiple Spanning Tree Protocol (MSTP) statistics to see MSTP related bridge-level statistics.

Syntax

- `show spanning-tree mstp statistics`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show spanning-tree mstp status

View the Multiple Spanning Tree Protocol (MSTP) status to display the MSTP- related status information known by the selected bridge.

Syntax

- `show spanning-tree mstp status`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show spanning-tree rstp config

View the global Rapid Spanning Tree Protocol (RSTP) configuration information to display the RSTP configuration details.

Syntax

- `show spanning-tree rstp config`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show spanning-tree rstp port config

Configure Ethernet Rapid Spanning Tree Protocol (RSTP) parameters to set RSTP parameters for the port.

Syntax

- `show spanning-tree rstp port config [{slot/port[-slot/port][,...]} ]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Shows RSTP port configuration.

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

show spanning-tree rstp port role

View the Rapid Spanning Tree Protocol (RSTP) port role to display the RSTP information show spanning-tree rstp port statistics. View the Rapid Spanning Tree Protocol (RSTP) information for a selected port to display the RSTP related statistics information for the selected port.

Syntax

- `show spanning-tree rstp port role [{slot/port[-slot/port][,...]} ]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Shows the RSTP port role.

©Avaya Inc. 2015 All Rights Reserved.

show spanning-tree rstp port statistics

View the Rapid Spanning Tree Protocol (RSTP) information for a selected port to display the RSTP related configuration information for the selected port.

Syntax

- `show spanning-tree rstp port statistics [{slot/port[-slot/port][,...]}]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Shows RSTP port statistics.

©Avaya Inc. 2015 All Rights Reserved.

show spanning-tree rstp port status

View the Rapid Spanning Tree Protocol (RSTP) status for a port to display the RSTP related status information for a selected port.

Syntax

- `show spanning-tree rstp port status [{slot/port[-slot/port][,...]}]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

show spanning-tree rstp statistics

View Rapid Spanning Tree Protocol (RSTP) statistics to manage network performance.

Syntax

- `show spanning-tree rstp statistics`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show spanning-tree rstp status

View the Rapid Spanning Tree Protocol (RSTP) status to display the RSTP related status information for the selected bridge.

Syntax

- `show spanning-tree rstp status`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show spanning-tree status

View spanning-tree status information.

Syntax

- `show spanning-tree status`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show spbm

Display the status (enabled or disabled) and the ethertype for Shortest Path Bridging MAC (SPBM).

Syntax

- `show spbm`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show ssh

Verify that Secure Shell (SSH) services are enabled on the Virtual Services Platform 9000 and display SSH configuration information to ensure that the SSH parameters are properly configured.

Syntax

- `show ssh global`
- `show ssh session`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`global`	Displays global system SSH information.
`session`	Displays the current session SSH information.

©Avaya Inc. 2015 All Rights Reserved.

show sys dns

Shows the DNS default domain name.

Syntax

- `show sys dns`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show sys force-msg

Shows the message control force message pattern settings.

Syntax

- `show sys force-msg`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show sys-info

Display the system status and technical information on the hardware components of the switch.

Syntax

- `show sys-info`
- `show sys-info asic`
- `show sys-info card`
- `show sys-info fan`
- `show sys-info power`
- `show sys-info temperature`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`asic`	Specifies information about the application-specific integrated circuit (ASIC) installed on each module.
`card`	Specifies information about all the installed modules, including cooling modules, and firmware for the CF devices. The output may incorrectly identify the SF cooling module as the 9012FC. The correct model name is the 9012RC.
`fan`	Specifies information about installed cooling modules.
`power`	Specifies information about installed power supplies.
`temperature`	Specifies information about temperature.

©Avaya Inc. 2015 All Rights Reserved.

show syslog

View the syslog information to ensure accuracy.

Syntax

- `show syslog`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show syslog host

View the syslog host information to ensure accuracy.

Syntax

- `show syslog host <1-10>`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show sys mgid-usage

Shows the multicast group ID (MGID) usage for VLANs, SPBM, and multicast traffic.

Syntax

- `show sys mgid-usage`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show sys msg-control

Shows the system message control function status (activated or disabled).

Syntax

- `show sys msg-control`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show sys mtu

Shows system maximum transmission unit (MTU) information.

Syntax

- `show sys mtu`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show sys power

View power information for the chassis.

Syntax

- `show sys power`
- `show sys power global`
- `show sys power power-supply`
- `show sys power slot`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`global`	Shows a summary of the power redundancy settings.
`power-supply`	Shows detailed power information for each power supply.
`slot`	Shows detailed power information for each slot.

©Avaya Inc. 2015 All Rights Reserved.

show sys setting

Shows system settings.

Syntax

- `show sys setting`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show sys software

Verify that the image and configuration are loaded properly.

Syntax

- `show sys software`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show sys stats ipmc-threshold-exceeded-cnt

Display IP multicast exceeded threshold counters.

Syntax

- `show sys stats ipmc-threshold-exceeded-cnt`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show sys topology-ip

Shows the circuitless IP set.

Syntax

- `show sys topology-ip`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show tacacs

Displays the status of the TACACS+ configuration.

Syntax

- `show tacacs`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show tech

Display technical information about the status of the system and complete information about the hardware components, software components, and operation of the system.

Syntax

- `show tech`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show telnet-access

Show the maximum number of Telnet sessions.

Syntax

- `show telnet-access`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show trace cfm

Shows the configuration status for CFM trace.

Syntax

- `show trace cfm`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show trace file

View the trace results.

Syntax

- `show trace file`
- `show trace file tail`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show trace level

Show the current trace level for all modules.

Syntax

- `show trace level`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show trace modid-list

Show the relationship between level number and module ID to use with the trace tool.

Syntax

- `show trace modid-list`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show trace spbm isis

View trace results.

Syntax

- `show trace spbm isis`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show unsupported-lastset

Display the last set of masked commands in the release.

Syntax

- `show unsupported-lastset`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show users

Display a list of users who are logged on to the system.

Syntax

- `show users`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show vlacp

Display Virtual Link Aggregation Control Protocol (VLACP) global information.

Syntax

- `show vlacp`
- `show vlacp interface`
- `show vlacp interface [vid <1-4084>]`
- `show vlacp interface gigabitethernet {slot/port[-slot/port][,...]}`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	{slot/port [-slot/port][,...]} is the slot and port list.
`gigabitethernet`	Displays the VLACP configuration for the GigabitEthernet port interface.
`interface`	Displays the VLACP port configuration to show the port VLACP configuration.
`vid <1-4084>`	<1-4084> is the VLAN ID or list of VLAN IDs to show only ports attached to a particular VLAN.

©Avaya Inc. 2015 All Rights Reserved.

show vlan advance

View the advanced parameters to display the advanced parameters for the specified VLAN or for all VLANs.

Syntax

- `show vlan advance [<1-4084>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<1-4084>`	Specifies the VLAN ID in a range of 1 to 4084.
`port <value>`	Specifies the port or range of ports.

©Avaya Inc. 2015 All Rights Reserved.

show vlan autolearn-mac

View autolearned MAC addresses.

Syntax

- `show vlan autolearn-mac`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show vlan basic

View the VLAN information to display the basic configuration for all VLANs or a specified VLAN.

Syntax

- `show vlan basic <1-4084>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<1-4084>	Specifies the VLAN ID in a range of 1 to 4084.

©Avaya Inc. 2015 All Rights Reserved.

show vlan brouter-port

View the brouter port information to display the brouter port VLAN information for all VLANs on the switch or for the specified VLAN.

Syntax

- `show vlan brouter-port`

Default

None

Command mode

User EXEC

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

show vlan i-sid

Display the customer VLAN (C-VLAN) to instance service identifier (I-SID) associations.

Syntax

- `show vlan i-sid`
- `show vlan i-sid <1-4084>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<1-4084>	Specifies the VLAN ID. If you do not specify the VLAN ID, the output includes all VLANs.

©Avaya Inc. 2015 All Rights Reserved.

Home | Command modes | Alphabetical listing

show vlan mac-address-entry

View forwarding database (FDB) filters to display the FDB filters for the specified VLAN.

Syntax

- `show vlan mac-address-entry [<1-4084>]`
- `show vlan mac-address-entry mac 0x00:0x00:0x00:0x00:0x00:0x00`
- `show vlan mac-address-entry port {slot/port[-slot/port][,...]}`
- `show vlan mac-address-entry spbm-tunnel-as-mac`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<1-4084>`	Specifies the VLAN ID in a range of 1 to 4084.
`mac 0x00:0x00:0x00:0x00:0x00:0x00`	Specifies the MAC address.
`port {slot/port[-slot/port][,...]}`	Specifies the port or range of ports in either slot or port format.
`spbm-tunnel-as-mac`	Discovers where entries are learned. The TUNNEL column indicates where in the SPBM network an entry is learned.

©Avaya Inc. 2015 All Rights Reserved.

show vlan mac-address-static

View the database status, MAC address, and QoS levels to display the static forwarding database status.

Syntax

- `show vlan mac-address-static [<1-4084>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<1-4084>`	Specifies the VLAN ID in a range of 1 to 4084.
`mac <value>`	Specifies the MAC address.
`port <portList>`	Specifies the port or range of ports in either slot or port format.

©Avaya Inc. 2015 All Rights Reserved.

show vlan manual-edit-mac

Show the list of manually edited MAC addresses and the associated ports.

Syntax

- `show vlan manual-edit-mac`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show vlan members

View the VLAN port member status to display the port member status for all VLANs on the switch or for the specified VLAN.

Syntax

- `show vlan members [<1-4084>][null-vlan] [port {slot/port[-slot/port] [,...]}]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<1-4084>`	Specifies the VLAN ID in the range of 1 to 4084. Entering a VLAN ID is optional. When you enter a VLAN ID, the command shows information for the specified VLAN or port. Without the VLAN ID the command shows information for all the configured VLANs.
`null-vlan`	Displays ports in a null VLAN. The Virtual Services Platform 9000 supports a placeholder for ports that is called a null port-based VLAN or unassigned VLAN.
`port {slot/port[-slot/port][,...]}`	Specifies the port or range of ports. Important: Entering a port {slot/port[-slot/port][,...]} is optional. If you enter a port{slot/port[-slot/port] [,...]}, the command shows information for the port. Without the port {slot/port[-slot/port][,...]}, the command shows information for all the ports.

©Avaya Inc. 2015 All Rights Reserved.

show vlan nodal-mep

Display the nodal Maintenance Endpoint (MEP) configuration. The Nodal B-VLAN MEPs created on the CP and function as if they are connected to the virtual interface of the given B-VLAN. Because of this they are supported for both port and MLT based B-VLANs. To support this behavior a MAC entry is added to the FDB and a new CFM data path table containing the B-VLAN and MP level are added to direct CFM frames to the CP as required.

Syntax

- `show vlan nodal-mep`
- `show vlan nodal-mep <1-4084>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<1-4084>	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

show vlan nodal-mip-level

Display the nodal Maintenance Intermediate Point (MIP) level configuration. The Nodal MIP is associated with a B-VLAN. VLAN and level are sufficient to specify the Nodal MIP entity. The Nodal MIP MAC address is the SPBM system ID for the node on which it resides. If the fastpath sends a message to the CP, the MIP responds if it is not the target and the MEP responds if it is the target.

Syntax

- `show vlan nodal-mip-level`
- `show vlan nodal-mip-level <1-4084>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<1-4084>	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

Home | Command modes | Alphabetical listing

show vlan remote-mac-table

Display customer VLAN (C-VLAN) remote-mac-table information.

Syntax

- `show vlan remote-mac-table <1-4084>`
- `show vlan remote-mac-table <1-4084> alternative`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<1-4084>`	Specifies the VLAN ID.
`alternative`	Shows the table in the alternative way.

©Avaya Inc. 2015 All Rights Reserved.

show vlan src-mac

View the VLAN source MAC addresses to display the source MAC address for any source MAC-based VLANs on the switch or for the specified VLAN.

Syntax

- `show vlan src-mac <1-4084>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<1-4084>	Specifies the VLAN ID. The value ranges from 1 to 4084.Important The entry of a VLAN ID is optional. When you enter a VLAN ID, the command shows information for the specified VLAN or port. Without the VLAN ID the command shows information for all the configured VLANs.

©Avaya Inc. 2015 All Rights Reserved.

show vlan static-mcastmac

Display the Layer 2 multicast media access control (MAC) filters.

Syntax

- `show vlan static-mcastmac [<1-4084>]`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

show web-server

Display the web server information.

Syntax

- `show web-server`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

shutdown

Disable an Ethernet module before you remove it from the chassis to minimize traffic loss. Traffic does not flow on a disabled module.

Syntax

- `default shutdown`
- `default shutdown port {slot/port[-slot/port][,...]}`
- `no shutdown`
- `no shutdown port {slot/port[-slot/port][,...]}`
- `shutdown`
- `shutdown port {slot/port[-slot/port][,...]}`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
<{slot/port[-slot/port][,...]}>	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

shutdown (for the management port)

Disable the Ethernet management port on the CP module.

Syntax

- `default shutdown [port {slot/port[-slot/port][,...]}]`
- `no shutdown [port {slot/port[-slot/port][,...]}]`
- `shutdown [port {slot/port[-slot/port][,...]}]`

Default

`The default is enabled.`

Command mode

mgmtEthernet Interface Configuration

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port to disable the management port. The slots available are 1 and 2 in the format 1/2 or 2/1.

©Avaya Inc. 2015 All Rights Reserved.

slamon agent

Configures the SLA Mon™ agent.

Syntax

- `default slamon agent ip address`
- `default slamon agent port`
- `slamon agent ip address {A.B.C.D}`
- `slamon agent ip address {A.B.C.D} vrf WORD<1-16>`
- `slamon agent port <0-65535>`

Default

None

Command mode

Application Configuration

Command parameters

Parameter	Description
`ip address {A.B.C.D}`	Configures the agent IP address. You must configure the IP address before the agent can process received discovery packets from the server. The agent IP address is a mandatory parameter if you enable SLA Mon™. The default value is 0.0.0.0. Note: If you configure the SLA Mon™ agent address under an IP address for a VLAN or brouter, you must remove the SLA Mon™ address before you can remove the IP address for the VLAN or brouter.
`port <0-65535>`	Configures the UDP port for agent-server communication. The agent receives discovery packets on this port. The default is port 50011. The server must use the same port.
`vrf WORD<1-16>`	Specifies a VRF name. The VRF parameter is optional.

©Avaya Inc. 2015 All Rights Reserved.

slamon agent-comm-port <0-65535>

Controls the port used for Real Time Protocol (RTP) and New Trace Route (NTR) testing.

Syntax

- `default slamon agent-comm-port`
- `slamon agent-comm-port <0-65535>`

Default

`The default is 50012.`

Command mode

Application Configuration

©Avaya Inc. 2015 All Rights Reserved.

slamon install-cert-file

Installs a Secure Sockets Layer (SSL) certificate.

Syntax

- `no slamon install-cert-file`
- `slamon install-cert-file WORD<0-128>`

Default

By default, the agent uses an Avaya SIP certificate to secure communications with the Avaya Diagnostic Server with SLA Mon™ technology.

Command mode

Application Configuration

Command parameters

Parameter	Description
WORD<0-128>	Specifies the file name and path of the certificate to install.

©Avaya Inc. 2015 All Rights Reserved.

slamon oper-mode enable

Enables the SLA Mon™ agent.

Syntax

- `default slamon oper-mode`
- `no slamon oper-mode`
- `no slamon oper-mode enable`
- `slamon oper-mode`
- `slamon oper-mode enable`

Default

`The default is disabled.`

Command mode

Application Configuration

©Avaya Inc. 2015 All Rights Reserved.

slamon server

Configures information about the Avaya Diagnostic Server with SLA Mon™ technology, with which the agent communicates.

Syntax

- `default slamon server ip address`
- `default slamon server port`
- `slamon server ip address {A.B.C.D}`
- `slamon server ip address {A.B.C.D} {A.B.C.D}`
- `slamon server port <0-65535>`
- `slamon server port <0-65535> <0-65535>`

Default

None

Command mode

Application Configuration

Command parameters

Parameter	Description
`ip address {A.B.C.D} {A.B.C.D}`	Restricts the agent to use only this IP address, which is associated with the Avaya Diagnostic Server with SLA Mon™ technology. The default is 0.0.0.0, which means the agent can register with any server. The second {A.B.C.D} represents an optional secondary server. Omit this parameter if you use only one server.
`port <0-65535> <0-65535>`	Restricts the agent to use of this registration port only. The default is 0, which means the agent disregards the source port information in server traffic. The Avaya Diagnostic Server with SLA Mon™ technology must use the same port. The second <0-65535> represents the UDP port for an optional secondary server. Omit this parameter if you use only one server.

©Avaya Inc. 2015 All Rights Reserved.

slot reset

Use the following command after all modules are updated, for the updates to take effect on the switch.

Syntax

- `slot reset <1-12>`
- `slot reset <1-12> -coredump`
- `slot reset SF1`
- `slot reset SF1 -coredump`
- `slot reset SF2`
- `slot reset SF2 -coredump`
- `slot reset SF3`
- `slot reset SF3 -coredump`
- `slot reset SF4`
- `slot reset SF4 -coredump`
- `slot reset SF5`
- `slot reset SF5 -coredump`
- `slot reset SF6`
- `slot reset SF6 -coredump`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
<1-12>	Specifies the slot number. Valid slots are 1 to 12.
-coredump	Creates a coredump for a specific slot or switch fabric before the system resets the slot or swich fabric. Caution: Only use the -coredump parameter if an issue causes you to reset the slot or switch fabric, and you need to contact customer service for analysis of the problem.
SF1	Specifies Switch Fabric 1.
SF2	Specifies Switch Fabric 2.
SF3	Specifies Switch Fabric 3.
SF4	

	Specifies Switch Fabric 4.
SF5	Specifies Switch Fabric 5.
SF6	Specifies Switch Fabric 6.

©Avaya Inc. 2015 All Rights Reserved.

slot shutdown

Enable an Ethernet module to allow traffic to flow through it or disable an Ethernet module before you remove it from the chassis to minimize traffic loss. Traffic does not flow on a disabled module.

Syntax

- `no slot shutdown [port {slot/port[-slot/port][,...]}]`
- `slot shutdown [port {slot/port[-slot/port][,...]}]`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`<{slot/port[-slot/port][,...]}>`	Identifies the slot and port numbers. Valid slot numbers are 3 to 12.

©Avaya Inc. 2015 All Rights Reserved.

slpp (for a port)

Enable Simple Loop Prevention Protocol (SLPP) by port to detect a loop and automatically stop it.

Syntax

- `default slpp`
- `default slpp packet-rx`
- `default slpp packet-rx-threshold`
- `default slpp port {slot/port[-slot/port][,...]}`
- `default slpp port {slot/port[-slot/port][,...]} packet-rx`
- `default slpp port {slot/port[-slot/port][,...]} packet-rx-threshold`
- `no slpp`
- `no slpp packet-rx`
- `no slpp port {slot/port[-slot/port][,...]}`
- `no slpp port {slot/port[-slot/port][,...]} packet-rx`
- `slpp packet-rx`
- `slpp packet-rx-threshold <1-500>`
- `slpp port {slot/port[-slot/port][,...]} packet-rx`
- `slpp port {slot/port[-slot/port][,...]} packet-rx-threshold <1-500>`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`packet-rx`	Enables or disables SLPP packet reception on the port. The default is disabled.
`packet-rx-threshold <1-500>`	Specifies the SLPP reception threshold on the ports, expressed as an integer. The packet reception threshold specifies the number of SLPP packets the port receives before it is administratively disabled. CAUTION: Avaya recommends that you configure the rx-threshold above 50 ms only on lightly loaded switches. If you configure the rx-threshold to a value greater than 50 ms on a

heavily loaded switch and a loop occurs, the system can experience high CPU utilization. The default is 1.

©Avaya Inc. 2015 All Rights Reserved.

slpp (globally)

Enable the Simple Loop Prevention Protocol (SLPP) globally and for a VLAN to detect a loop and automatically stop it. The VLAN configuration controls the boundary of SLPP-PDU transmission.

Syntax

- `default slpp`
- `default slpp enable`
- `default slpp tx-interval`
- `no slpp`
- `no slpp enable`
- `no slpp vid <1-4084>`
- `slpp enable`
- `slpp tx-interval <500-5000>`
- `slpp vid <1-4084>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`enable`	Enables or disables the SLPP operation. You must enable the SLPP operation to enable the SLPP packet transmit and receive process. If you disable the SLPP operation, the system sends no SLPP packets and discards received SLPP packets. The default is disabled.
`tx-interval <500-5000>`	Configures the SLPP packet transmit interval, expressed in milliseconds, in a range from 500-5000. The default is 500.
`vid <1-4084>`	Adds a VLAN, by VLAN ID, to a SLPP transmission list.

©Avaya Inc. 2015 All Rights Reserved.

slpp (on a VLAN)

Enable the Simple Loop Prevention Protocol (SLPP) globally and for a VLAN to detect a loop and automatically stop it. The VLAN configuration controls the boundary of SLPP-PDU transmission.

Syntax

- `default slpp`
- `default slpp enable`
- `default slpp tx-interval`
- `no slpp`
- `no slpp enable`
- `no slpp vid <1-4084>`
- `slpp enable`
- `slpp tx-interval <500-5000>`
- `slpp vid <1-4084>`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables or disables the SLPP operation. You must enable the SLPP operation to enable the SLPP packet transmit and receive process. If you disable the SLPP operation, the system sends no SLPP packets and discards received SLPP packets. The default is disabled.
`tx-interval <500-5000>`	Configures the SLPP packet transmit interval, expressed in milliseconds, in a range from 500-5000. The default is 500.
`vid <1-408>`	Adds a VLAN, by VLAN ID, to a SLPP transmission list.

©Avaya Inc. 2015 All Rights Reserved.

smlt

Create a SMLT from an existing MLT to split physical ports between two switches to improve resiliency and provide active load sharing.

Syntax

- `default smlt`
- `no smlt`
- `smlt`

Default

None

Command mode

MLT Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

snmplog

Use SNMP trap logging to log to the system log file. This allows you to send SNMP logs to a system log server.

Syntax

- `snmplog disable`
- `snmplog enable`

Default

`The default is disabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

snmp-server authentication-trap enable

Activate the generation of authentication traps.

Syntax

- `default snmp-server authentication-trap`
- `snmp-server authentication-trap enable`

Default

None

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

snmp-server community

Create a community to use in forming a relationship between an SNMP agent and one or more SNMP managers. You require SNMP community strings to access the system using an SNMP-based management software.

Syntax

- `no snmp-server community WORD<1-32>`
- `no snmp-server community-by-index WORD<1-32>`
- `snmp-server community WORD<1-32> group WORD<0-32>`
- `snmp-server community WORD<1-32> group WORD<0-32> secname WORD<1-32>`
- `snmp-server community WORD<1-32> index WORD<1-32> secname WORD<1-32>`
- `snmp-server community WORD<1-32> index WORD<1-32> secname WORD<1-32> context WORD<0-32>`
- `snmp-server community WORD<1-32> secname WORD<1-32>`
- `snmp-server community WORD<1-32> secname WORD<1-32> context WORD<0-32>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`community-by-index WORD<1-32>`	Specifies the community string by index to delete.
`context WORD<0-32>`	Specifies the context in which management information is accessed when you use the specified community string, for example, the VRF name.
`group WORD<0-32>`	Specifies the group name.
`index WORD<0-32>`	Specifies the unique index value of a row in this table.
`secname WORD<0-32>`	Maps the community string to the security name in the VACM Group Member Table. The range is 0-32 characters.
`WORD<1-32>`	Specifies a community string, from 1-32 characters.

©Avaya Inc. 2015 All Rights Reserved.

snmp-server contact

Configure the contact information for the system.

Syntax

- `default snmp-server contact`
- `no snmp-server contact`
- `snmp-server contact WORD<0-255>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
WORD<0-255>	Changes the sysContact information for VSP 9000. WORD<0-255> is an ASCII string from 0-255 characters (for example a phone extension or e-mail address.)

©Avaya Inc. 2015 All Rights Reserved.

snmp-server force-iphdr-sender enable

Configure the SNMP and IP sender flag to the same value.

Syntax

- `default snmp-server force-iphdr-sender`
- `default snmp-server force-iphdr-sender enable`
- `no snmp-server force-iphdr-sender`
- `no snmp-server force-iphdr-sender enable`
- `snmp-server force-iphdr-sender enable`

Default

None

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

snmp-server force-trap-sender enable

Send the configured source address (sender IP as the sender network in the notification message).

Syntax

- `default snmp-server force-trap-sender`
- `default snmp-server force-trap-sender enable`
- `no snmp-server force-trap-sender`
- `no snmp-server force-trap-sender enable`
- `snmp-server force-trap-sender enable`

Default

None

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

snmp-server group

Create a new user group member to logically group users who require the same level of access. Create new access for a group in the View-based Access Control Model (VACM) table to provide access to managed objects.

Syntax

- `no snmp-server group WORD<1-32>`
- `no snmp-server group WORD<1-32> WORD<0-32>`
- `snmp-server group WORD<1-32> WORD<0-32> auth-no-priv`
- `snmp-server group WORD<1-32> WORD<0-32> auth-no-priv notify-view WORD<0-32>`
- `snmp-server group WORD<1-32> WORD<0-32> auth-no-priv read-view WORD<0-32>`
- `snmp-server group WORD<1-32> WORD<0-32> auth-no-priv write-view WORD<0-32>`
- `snmp-server group WORD<1-32> WORD<0-32> auth-priv`
- `snmp-server group WORD<1-32> WORD<0-32> auth-priv notify-view WORD<0-32>`
- `snmp-server group WORD<1-32> WORD<0-32> auth-priv read-view WORD<0-32>`
- `snmp-server group WORD<1-32> WORD<0-32> auth-priv write-view WORD<0-32>`
- `snmp-server group WORD<1-32> WORD<0-32> no-auth-no-priv`
- `snmp-server group WORD<1-32> WORD<0-32> no-auth-no-priv notify-view WORD<0-32>`
- `snmp-server group WORD<1-32> WORD<0-32> no-auth-no-priv read-view WORD<0-32>`
- `snmp-server group WORD<1-32> WORD<0-32> no-auth-no-priv write-view WORD<0-32>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`auth-no-priv`	Assigns the minimum level of security required to gain the access rights allowed by this conceptual row. If the auth-no-priv parameters is included, it creates one entry for SNMPv3 access.
`auth-priv`	Assigns the minimum level of security required to gain the access rights allowed by this conceptual row. If the auth-priv parameter is included, it creates one entry for SNMPv3 access.
`group WORD<1-`	Assigns the group name for data access. The range is 1-32 characters. Use the no operator to remove this configuration.

32>	
no-auth-no-priv	Assigns the minimum level of security required to gain the access rights allowed by this conceptual row. If the no-auth-no-priv parameter is included, it creates three entries, one for SNMPv1, one for SNMPv2c access, and one for SNMPv3c access.
notify-view WORD<0-32>	Specifies the view name in the range of 0-32 characters. The switch uses elements of this view in the trap messages sent for the communities associated with this group.
read-view WORD<0-32>	Specifies the view name in the range of 0-32 characters. The switch makes elements of this view available for reading for the communities associated with this group.
WORD<1-32> WORD<1-32>	The first WORD<1-32> specifies the group name for data access. The second WORD<1-32> specifies the context name. If you use a particular group name value but with different context names, you create multiple entries for different contexts for the same group. You can omit the context name and use the default. If the context name value ends in the wildcard character (*), the resulting entries match a context name that begins with that context. For example, a context name value of foo* matches contexts starting with foo, such as foo6 and foofofum. Use the no operator to remove this configuration.
write-view WORD<0-32>	Specifies the view name in the range of 0-32 characters. The switch makes elements of this view available to be modified by the communities associated with this group.

©Avaya Inc. 2015 All Rights Reserved.

snmp-server host v1

Configure an SNMP host so that the switch can forward SNMP traps to a host for monitoring.

Syntax

- `no snmp-server host WORD<1-256> port <1-65535> v1 WORD<1-32>`
- `no snmp-server host WORD<1-256> v1 WORD<1-32>`
- `snmp-server host WORD<1-256> port <1-65535> v1 WORD<1-32>`
- `snmp-server host WORD<1-256> port <1-65535> v1 WORD<1-32> filter WORD<1-32>`
- `snmp-server host WORD<1-256> v1 WORD<1-32>`
- `snmp-server host WORD<1-256> v1 WORD<1-32> filter WORD<1-32>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`filter WORD<1-32>`	Specifies a filter profile name.
`port<1-65535>`	Specifies the host server port number.
`v1 WORD <1-32> [filter WORD<1-32>]`	Specifies the SNMP v1 security name.
`WORD<1-256>`	Specifies either an IPv4 or IPv6 address.

©Avaya Inc. 2015 All Rights Reserved.

snmp-server host v2

Configure an SNMPv2 host so that the switch can forward SNMP traps to a host for monitoring.

Syntax

- default snmp-server host WORD<1-256> port <1-65535> v2c WORD<1-32>
- default snmp-server host WORD<1-256> port <1-65535> v2c WORD<1-32> mms
- default snmp-server host WORD<1-256> port <1-65535> v2c WORD<1-32> retries
- default snmp-server host WORD<1-256> port <1-65535> v2c WORD<1-32> timeout
- default snmp-server host WORD<1-256> v2c WORD<1-32>
- default snmp-server host WORD<1-256> v2c WORD<1-32> mms
- default snmp-server host WORD<1-256> v2c WORD<1-32> retries
- default snmp-server host WORD<1-256> v2c WORD<1-32> timeout
- no snmp-server host WORD<1-256> port <1-65535> v2c WORD<1-32>
- no snmp-server host WORD<1-256> v2c WORD<1-32>
- snmp-server host WORD<1-256> port <1-65535> v2c WORD<1-32>
- snmp-server host WORD<1-256> port <1-65535> v2c WORD<1-32> filter WORD<1-32>
- snmp-server host WORD<1-256> port <1-65535> v2c WORD<1-32> inform
- snmp-server host WORD<1-256> port <1-65535> v2c WORD<1-32> inform mms <0-2147483647>
- snmp-server host WORD<1-256> port <1-65535> v2c WORD<1-32> inform retries <0-255>
- snmp-server host WORD<1-256> port <1-65535> v2c WORD<1-32> inform timeout <1-2147483647>
- snmp-server host WORD<1-256> v2c WORD<1-32>
- snmp-server host WORD<1-256> v2c WORD<1-32> filter WORD<1-32>
- snmp-server host WORD<1-256> v2c WORD<1-32> inform
- snmp-server host WORD<1-256> v2c WORD<1-32> inform mms <0-2147483647>
- snmp-server host WORD<1-256> v2c WORD<1-32> inform retries <0-255>
- snmp-server host WORD<1-256> v2c WORD<1-32> inform timeout <1-2147483647>

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
filter WORD<1-32>	Specifies a filter profile name.
inform	Configure this attribute to send an inform message instead of a trap.
mms <0-2147483647>	Specifies the maximum message size.
port <1-65535>	Specifies the port number configured as the destination port at the UDP level in the trap packet.
retries <0-255>	Specifies the number of packets to be sent if no reply is received.
timeout <1-2147483647>	Specifies the time to wait for a reply before resending the inform message. Time is specified in centiseconds.
v2c WORD<1-32>	Specifies the SNMPv2 security name
WORD<1-256>	Specifies the IPv4 or IPv6 host address.

©Avaya Inc. 2015 All Rights Reserved.

snmp-server host v3

Configure an SNMPv3 host so that the switch can forward SNMP traps to a host for monitoring.

Syntax

- `default snmp-server host WORD<1-256> port <1-65535> v3 WORD<1-32>`
- `default snmp-server host WORD<1-256> port <1-65535> v3 WORD<1-32> retries`
- `default snmp-server host WORD<1-256> port <1-65535> v3 WORD<1-32> timeout`
- `default snmp-server host WORD<1-256> v3 WORD<1-32>`
- `default snmp-server host WORD<1-256> v3 WORD<1-32> retries`
- `default snmp-server host WORD<1-256> v3 WORD<1-32> timeout`
- `no snmp-server host WORD<1-256> port <1-65535> v3 WORD<1-32>`
- `no snmp-server host WORD<1-256> v3 WORD<1-32>`
- `snmp-server host WORD<1-256> port <1-65535> v3 { noAuthNoPriv | authNoPriv | authPriv } WORD<1-32>`
- `snmp-server host WORD<1-256> port <1-65535> v3 { noAuthNoPriv | authNoPriv | authPriv } WORD<1-32> filter WORD<1-32>`
- `snmp-server host WORD<1-256> port <1-65535> v3 { noAuthNoPriv | authNoPriv | authPriv } WORD<1-32> inform`
- `snmp-server host WORD<1-256> port <1-65535> v3 { noAuthNoPriv | authNoPriv | authPriv } WORD<1-32> inform retries <0-255>`
- `snmp-server host WORD<1-256> port <1-65535> v3 { noAuthNoPriv | authNoPriv | authPriv } WORD<1-32> inform timeout <1-2147483647>`
- `snmp-server host WORD<1-256> v3 { noAuthNoPriv | authNoPriv | authPriv } WORD<1-32>`
- `snmp-server host WORD<1-256> v3 { noAuthNoPriv | authNoPriv | authPriv } WORD<1-32> filter WORD<1-32>`
- `snmp-server host WORD<1-256> v3 { noAuthNoPriv | authNoPriv | authPriv } WORD<1-32> inform`
- `snmp-server host WORD<1-256> v3 { noAuthNoPriv | authNoPriv | authPriv } WORD<1-32> inform retries <0-255>`
- `snmp-server host WORD<1-256> v3 { noAuthNoPriv | authNoPriv | authPriv } WORD<1-32> inform timeout <1-2147483647>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
{noAuthNoPriv|authNoPriv|authPriv}	Specifies the security level.
filter WORD<1-32>	Specifies a filter profile name.
inform	Specifies the notify type.
mms <0-2147483647>	Specifies the maximum message size.
port <1-65535>	Specifies the port number configured as the destination port at the UDP level in the trap packet.
retries <0-255>	Specifies the number of packets to be sent if no reply is received.
timeout <1-2147483647>	Specifies the time to wait for a reply before resending the inform message. Time is specified in centiseconds.
v3c WORD<1-32>	Specifies the SNMPv3 security name
WORD<1-256>	Specifies the IPv4 or IPv6 host address.

©Avaya Inc. 2015 All Rights Reserved.

snmp-server location

Configure the sysLocation information for the system. <WORD 0-255> is an ASCII string from 0-255 characters.

Syntax

- `default snmp-server location`
- `no snmp-server location`
- `snmp-server location WORD<0-255>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
WORD <0255>	Specifies an ASCII string from 0-255 characters.

©Avaya Inc. 2015 All Rights Reserved.

snmp-server login-success-trap enable

Configure the generation of login success traps.

Syntax

- `default snmp-server login-success-trap`
- `snmp-server login-success-trap enable`

Default

None

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

snmp-server name

Configure the sysName information for the system. WORD<0-255> is an ASCII string from 0-255 characters.

Syntax

- `default snmp-server name`
- `no snmp-server name`
- `snmp-server name WORD<0-255>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
WORD <0255>	Specifies an ASCII string from 0-255 characters.

©Avaya Inc. 2015 All Rights Reserved.

snmp-server notify-filter

Configure the notify table to select management targets to receive notifications, as well as the type of notification to send to each management target.

Syntax

- `no snmp-server notify-filter WORD<1-32> WORD<1-32>`
- `snmp-server notify-filter WORD<1-32> WORD<1-32>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
WORD<1-32> WORD<1-32>	The first WORD<1-32> specifies the name of the filter profile. The second WORD<1-32> identifies the filter subtree OID. If the Subtree OID uses a '+' prefix (or no prefix), this indicates include. The '-' prefix, this indicates exclude.

©Avaya Inc. 2015 All Rights Reserved.

snmp-server sender-ip

Configure the IP interface from which the SNMP traps originate if the Virtual Services Platform 9000 has multiple interfaces.

Syntax

- `snmp-server sender-ip {A.B.C.D} {A.B.C.D}`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
{A.B.C.D} {A.B.C.D}	Specifies the IP address of the destination SNMP server that receives the SNMP trap notification in the first IP address. Specifies the source IP address of the SNMP trap notification packet that is transmitted in the second IP address. If this is set to 0.0.0.0 then the switch uses the IP address of the local interface that is closest (from an IP routing table perspective) to the destination SNMP server.

©Avaya Inc. 2015 All Rights Reserved.

snmp-server user

Create a user on the local system in the USM table to authorize a user on a particular SNMP engine.

Syntax

- no snmp-server user engine-id WORD<16-97> WORD<1-32>
- no snmp-server user WORD<1-32>
- snmp-server user engine-id WORD<16-97> WORD<1-32>
- snmp-server user engine-id WORD<16-97> WORD<1-32> { md5 | sha } WORD<1-32>
- snmp-server user engine-id WORD<16-97> WORD<1-32> { md5 | sha } WORD<1-32> aes WORD<1-32>
- snmp-server user engine-id WORD<16-97> WORD<1-32> { md5 | sha } WORD<1-32> des WORD<1-32>
- snmp-server user WORD<1-32>
- snmp-server user WORD<1-32> { md5 | sha } WORD<1-32>
- snmp-server user WORD<1-32> { md5 | sha } WORD<1-32> aes WORD<1-32>
- snmp-server user WORD<1-32> { md5 | sha } WORD<1-32> aes WORD<1-32> notify-view WORD<0-32>
- snmp-server user WORD<1-32> { md5 | sha } WORD<1-32> aes WORD<1-32> read-view WORD<0-32>
- snmp-server user WORD<1-32> { md5 | sha } WORD<1-32> aes WORD<1-32> write-view WORD<0-32>
- snmp-server user WORD<1-32> { md5 | sha } WORD<1-32> des WORD<1-32>
- snmp-server user WORD<1-32> { md5 | sha } WORD<1-32> des WORD<1-32> notify-view WORD<0-32>
- snmp-server user WORD<1-32> { md5 | sha } WORD<1-32> des WORD<1-32> read-view WORD<0-32>
- snmp-server user WORD<1-32> { md5 | sha } WORD<1-32> des WORD<1-32> write-view WORD<0-32>
- snmp-server user WORD<1-32> { md5 | sha } WORD<1-32> notify-view WORD<0-32>
- snmp-server user WORD<1-32> { md5 | sha } WORD<1-32> read-view WORD<0-32>
- snmp-server user WORD<1-32> { md5 | sha } WORD<1-32> write-view WORD<0-32>
- snmp-server user WORD<1-32> group WORD<1-32>
- snmp-server user WORD<1-32> group WORD<1-32> { md5 | sha } WORD<1-32>
- snmp-server user WORD<1-32> group WORD<1-32> { md5 | sha } WORD<1-32> aes WORD<1-32>
- snmp-server user WORD<1-32> group WORD<1-32> { md5 | sha } WORD<1-32> des WORD<1-32>
- snmp-server user WORD<1-32> notify-view WORD<0-32>
- snmp-server user WORD<1-32> read-view WORD<0-32>
- snmp-server user WORD<1-32> write-view WORD<0-32>

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
{aes|des|3des} WORD<1-32>	Specifies a privacy protocol. If no value is entered, no authentication capability exists. WORD<1-32> assigns a privacy password. If no value is entered, no privacy capability exists. You must set authentication before you can set the privacy option.
{md5|sha} WORD<1-32>	Specifies an authentication protocol. If no value is entered, no authentication capability exists. WORD<1-32> specifies an authentication password. If no value is entered, no authentication capability exists.
engine-id WORD<1-32>	Assigns a Simple Network Management Protocol version 3 (SNMPv3) engine ID. Use the no operator to remove this configuration.
group WORD<1-32>	Specifies the group access name.
notify-view WORD<1-32>	The first instance is a noAuth view. The second instance is an auth view and the last instance is an authPriv view. The switch uses elements from this view in the trap messages sent for the user.
read-view WORD<1-32>	Specifies the view name. The first instance is a noAuth view. The second instance is an auth view and the last instance is an authPriv view. The switch makes elements from this available for reading for the user.
write-view WORD<1-32>	Specifies the view name. The first instance is a noAuth view. The second instance is an auth view and the last instance is an authPriv view. The switch makes elements from this view available to be modified by the user.

©Avaya Inc. 2015 All Rights Reserved.

snmp-server view

Create a new entry in the MIB view table. The default Layer 2 MIB view cannot modify SNMP settings. However, a new MIB view created with Layer2 permission can modify SNMP settings.

Syntax

- `no snmp-server view WORD<1-32> WORD<1-32>`
- `snmp-server view WORD <1-32> WORD <1-32>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
WORD <1-32>	Specifies a new entry with this group name. The range is 1-32 characters.
WORD <1-32> WORD<1-32>	The system uses the first WORD <1-32> to name the view; the system uses the second WORD <1-32> to specify the OID associated with this view. If the subtree OID uses a '+' prefix (or no prefix), this indicates include. The '-' prefix indicates exclude.

©Avaya Inc. 2015 All Rights Reserved.

snmp trap link-status

Enable link trap on the port. When you enable this flag a notification is sent when ports change from operationally up or down.

Syntax

- `default snmp trap link-status`
- `default snmp trap link-status port {slot/port[-slot/port][,...]}`
- `no snmp trap link-status`
- `no snmp trap link-status port {slot/port[-slot/port][,...]}`
- `snmp trap link-status`
- `snmp trap link-status enable`
- `snmp trap link-status port {slot/port[-slot/port][,...]}`
- `snmp trap link-status port {slot/port[-slot/port][,...]} enable`

Default

`The default is enabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables or disables link-trap status for the port.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

software

Perform various software functions on the switch to ensure it is updated with latest versions.

Syntax

- `software [activate WORD<1-99>|add WORD<1-99>|add-modules WORD<1-99>|commit|remove WORD<1-99>]`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
activate	Copies the software version to the boot flash file. When you use the software activate command, the system checks for hardware dependencies and prevents a downgrade if it detects a dependency. For example, if a hardware component has a minimum software version dependency, you cannot downgrade to an incompatible software version or install the hardware component in a chassis that runs an incompatible software version.
add	Unpacks a software release <version>.
add-modules	Adds modules to existing software release in /intflash|release|<version>.
commit	Ensures the running software release is trusted.
remove	Removes the software release <version>.

©Avaya Inc. 2015 All Rights Reserved.

software patch

Perform various software patch functions to keep the switch updated with the latest releases and software versions and utilize the switch optimally.

Syntax

- `software patch abort`
- `software patch add WORD <1-255>`
- `software patch apply all`
- `software patch apply all version WORD<1-255>`
- `software patch apply hitless`
- `software patch apply hitless version WORD<1-255>`
- `software patch apply patch-ids WORD<1-255>`
- `software patch apply patch-ids WORD<1-255> version WORD<1-255>`
- `software patch apply patch-ids WORD<1-255> WORD<1-255>`
- `software patch apply patch-ids WORD<1-255> WORD<1-255> version WORD<1-255>`
- `software patch apply patch-ids WORD<1-255> WORD<1-255> WORD<1-255>`
- `software patch apply patch-ids WORD<1-255> WORD<1-255> WORD<1-255> version WORD<1-255>`
- `software patch apply patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255>`
- `software patch apply patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> version WORD<1-255>`
- `software patch apply patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255>`
- `software patch apply patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> version WORD<1-255>`
- `software patch apply patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255>`
- `software patch apply patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> version WORD<1-255>`
- `software patch apply patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255>`
- `software patch apply patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> version WORD<1-255>`
- `software patch apply patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255>`

- software patch apply reset
- software patch apply reset version WORD<1-255>
- software patch commit
- software patch remove version WORD<1-255> patch-id WORD<1-255>
- software patch revert all
- software patch revert all version WORD<1-255>
- software patch revert hitless
- software patch revert hitless version WORD<1-255>
- software patch revert patch-ids WORD<1-255>
- software patch revert patch-ids WORD<1-255> version WORD<1-255>
- software patch revert patch-ids WORD<1-255> WORD<1-255>
- software patch revert patch-ids WORD<1-255> WORD<1-255> version WORD<1-255>
- software patch revert patch-ids WORD<1-255> WORD<1-255> WORD<1-255>
- software patch revert patch-ids WORD<1-255> WORD<1-255> WORD<1-255> version WORD<1-255>
- software patch revert patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255>
- software patch revert patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> version WORD<1-255>
- software patch revert patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255>
- software patch revert patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> version WORD<1-255>
- software patch revert patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255>
- software patch revert patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> version WORD<1-255>
- software patch revert patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255>
- software patch revert patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> version WORD<1-255>
- software patch revert patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255>
- software patch revert patch-ids WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> WORD<1-255> version WORD<1-255>
- software patch revert reset
- software patch revert reset version WORD<1-255>

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
abort	Cancels the software patch apply/revert.
add WORD <1-255>	Unpacks the software patches to /intflash|release|<version>|patches|<patch-id> where <version> and <patch-id> are extracted from the patch file. WORD <1-255> specifies the patch file name in the range of 1 to 255.
apply [all|hitless|patch-ids <WORD<1-255>|reset] version WORD<1-255>	Applies the latest versions of patches available to the switch. Apply the following: all - all software patches, hitless - hitless software patches, patch-ids - software patch ID, reset - reset software patches. WORD<1-255> specifies the name of the software version that needs to be applied on the switch.
commit	Commits the patch to apply or revert process on the switch.
remove version WORD<1-255> patch-id WORD<1-255>	Removes patches from /intflash|release|<version>|patches|<patch-id>.WORD<1-255> specifies the name of the software version. WORD<1-255> specifies the name of the patch file.
revert [all|hitless|patch-ids WORD<1-255>|reset] version WORD <1-255>	Resets or unapplies all the versions of the patches applied on the switch. Revert the following: all - all software patches, hitless - hitless software patches, patch-ids - software patch ID, reset - reset software patches. WORD <1-255> specifies the name of the software version that needs to be reverted on the switch.

©Avaya Inc. 2015 All Rights Reserved.

software reset-commit-time

Extends or reduces the commit time after you apply a software upgrade or patch. You may need additional time to verify the software works as expected after the upgrade or patch before you commit or roll back.

Syntax

- `software reset-commit-time`
- `software reset-commit-time <1-60>`

Default

`The default is 10 minutes.`

Command mode

Privileged EXEC

Command parameters

Parameter	Description
<1-60>	Extends or reduces the commit timer. By default, the commit timer is 10 minutes. As an example, if you enter the command string of software reset-commit-time 5, you reduce the commit timer to 5 minutes. If you enter the command string of software reset-commit-time 25, you extend the commit timer by 15 minutes, for a total of 25 minutes.

©Avaya Inc. 2015 All Rights Reserved.

source

Source a configuration to merge a script file into the running configuration. Warning: You are not able to source a complete configuration file to merge it with your running configuration because the system can crash. The source command can be used to merge smaller portions of a configuration into the existing configuration.

Syntax

- `source WORD<1-99> [debug] [stop] [syntax]`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
debug	Debugs the script output.
stop	Stops the merge after an error occurs.
syntax	Verifies the script syntax.
WORD<1-99>	Specifies a filename and location in one of the following formats: a.b.c.d:<file>, peer:<file>, /intflash/<file>, /extflash/<file>, or /usb/<file>. The path and <file> can use 1-99 characters.

©Avaya Inc. 2015 All Rights Reserved.

source-mac-vlan

Enable source MAC-based VLAN on the port.

Syntax

- `default source-mac-vlan`
- `default source-mac-vlan enable`
- `default source-mac-vlan port {slot/port[-slot/port][,...]}`
- `no source-mac-vlan`
- `no source-mac-vlan enable`
- `no source-mac-vlan port {slot/port[-slot/port][,...]}`
- `source-mac-vlan`
- `source-mac-vlan enable`
- `source-mac-vlan port {slot/port[-slot/port][,...]}`

Default

`The default is enabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables or disables source MAC-based VLAN for the port.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree bpdu-filtering

Configure BPDU Filtering to block the root selection process or to prevent BPDU flooding from unknown devices.

Syntax

- `default spanning-tree bpdu-filtering enable`
- `default spanning-tree bpdu-filtering port {slot/port[-slot/port][,...]} enable`
- `default spanning-tree bpdu-filtering port {slot/port[-slot/port][,...]} timeout`
- `default spanning-tree bpdu-filtering timeout`
- `no spanning-tree bpdu-filtering enable`
- `no spanning-tree bpdu-filtering port {slot/port[-slot/port][,...]} enable`
- `no spanning-tree bpdu-filtering port {slot/port[-slot/port][,...]} timeout`
- `no spanning-tree bpdu-filtering timeout`
- `spanning-tree bpdu-filtering enable`
- `spanning-tree bpdu-filtering port {slot/port[-slot/port][,...]} enable`
- `spanning-tree bpdu-filtering port {slot/port[-slot/port][,...]} timeout <0-65535>`
- `spanning-tree bpdu-filtering timeout <0-65535>`

Default

The default is disabled.

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables BPDU Filtering on the port. The default is disabled.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`timeout <0-65535>`	Specifies the value to use for port-state recovery. After a BPDU filter disables a port, the port remains in the disabled state until this timer expires. You can configure a value from 10 to 65535. The default is 120 seconds. If you configure the value to 0, you disable the timer.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree mstp cost

Configure the contribution of this port to the path cost value for the link.

Syntax

- `default spanning-tree mstp cost`
- `spanning-tree mstp cost <1-200000000>`

Default

`The default is 2000000.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<1-200000000>`	Specifies the cost value. The default is 2000000.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree mstp edge-port

Configure the port as an edge port.

Syntax

- `default spanning-tree mstp edge-port`
- `spanning-tree mstp edge-port { false | true }`

Default

`The default is disabled (false).`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<false|true>`	Enables or disables the port as an edge port.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree mstp force-port-state

Enable the force-port-state flag.

Syntax

- `default spanning-tree mstp force-port-state`
- `no spanning-tree mstp force-port-state`
- `no spanning-tree mstp force-port-state enable`
- `spanning-tree mstp force-port-state enable`

Default

`The default is enabled.`

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree mstp forward-time

Configure the MSTP forward delay for the bridge.

Syntax

- `default spanning-tree mstp forward-time`
- `spanning-tree mstp forward-time <400-3000>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`<400-3000>`	Configures the MSTP forward delay for the bridge, in hundredths of a second.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree mstp hello-time (on a port)

Configure the hello-time delay for the port.

Syntax

- `default spanning-tree mstp hello-time`
- `spanning-tree mstp hello-time <100-1000>`

Default

`The default is 2.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<100-1000>`	Configures the hello-time for a port in one hundredths of a second. The default is 2.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree mstp max-age

Assign the MSTP maximum age time for the bridge

Syntax

- `spanning-tree mstp max-age <600-4000>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<600-4000>	Assigns the MSTP maximum age time for the bridge, in one hundredths of a second.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree mstp max-hop

Assign the maximum hop count for the bridge..

Syntax

- `spanning-tree mstp max-hop <100-4000>`

Default

`The default is 2000.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<100-4000>`	Assigns the MSTP bridge maximum hop count. The range is 100 to 4000 one hundredths of a second.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree mstp msti (globally)

Configure Multiple Spanning Tree Protocol (MSTP) to set the MSTP configuration version.

Syntax

- `default spanning-tree mstp msti <1-63> priority`
- `spanning-tree mstp msti <1-63> priority <0-65535>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`<1-63>`	Specifies the instance parameter.
`priority <0-65535>`	Configures the MSTP bridge priority. Allowed values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree mstp msti (on a port)

Configure Multiple Spanning Tree Protocol (MSTP) to set the MSTP configuration version.

Syntax

- `default spanning-tree mstp msti <1-63> cost`
- `default spanning-tree mstp msti <1-63> force-port-state enable`
- `default spanning-tree mstp msti <1-63> port {slot/port[-slot/port][,...]} cost`
- `default spanning-tree mstp msti <1-63> port {slot/port[-slot/port][,...]} force-port-state enable`
- `default spanning-tree mstp msti <1-63> port {slot/port[-slot/port][,...]} priority`
- `default spanning-tree mstp msti <1-63> priority`
- `no spanning-tree mstp msti <1-63> force-port-state enable`
- `no spanning-tree mstp msti <1-63> port {slot/port[-slot/port][,...]} force-port-state enable`
- `spanning-tree mstp msti <1-63> cost <1-200000000>`
- `spanning-tree mstp msti <1-63> force-port-state enable`
- `spanning-tree mstp msti <1-63> port {slot/port[-slot/port][,...]} cost <1-200000000>`
- `spanning-tree mstp msti <1-63> port {slot/port[-slot/port][,...]} force-port-state enable`
- `spanning-tree mstp msti <1-63> port {slot/port[-slot/port][,...]} priority <0-240>`
- `spanning-tree mstp msti <1-63> priority <0-240>`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
<1-63>	Specifies the instance parameter.
cost <1-200000000>	Configures the path cost for the port
force-port-state enable	Enables MSTI learning for the port.
port {slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

`priority <0-65535>`	Configures the MSTP bridge priority. Allowed values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960,45056, 49152, 53248, 57344, 61440.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree mstp p2p

Specify the point-to-point status of the LAN segment attached to this port.

Syntax

- `default spanning-tree mstp p2p`
- `spanning-tree mstp p2p auto`
- `spanning-tree mstp p2p force-false`
- `spanning-tree mstp p2p force-true`

Default

`The default is auto.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<auto|force-false|false-true>`	A value of force-true indicates that this port is treated as if it connects to a point-to-point link. A value of force-false indicates that this port is treated as having a shared media connection. A value of auto indicates that this port is considered to have a point-to-point link if it is an aggregator and all of its members are aggregatable, or if the MAC entity is configured for full-duplex operation, either through autonegotation or by management means. The default is auto.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree mstp pathcost-type

Assign the Multiple Spanning Tree Protocol (MSTP) default pathcost version.

Syntax

- `default spanning-tree mstp pathcost-type`
- `spanning-tree mstp pathcost-type <bits16|bits32>`

Default

`The default is 32 bits.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<bits16|bits32>`	Specifies the pathcost value.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree mstp port

Configure all Multiple Spanning Tree Protocol (MSTP) parameters for a port.

Syntax

- `default spanning-tree mstp`
- `default spanning-tree mstp port {slot/port}`
- `default spanning-tree mstp port {slot/port} cost`
- `default spanning-tree mstp port {slot/port} edge-port`
- `default spanning-tree mstp port {slot/port} force-port-state`
- `default spanning-tree mstp port {slot/port} hello-time`
- `default spanning-tree mstp port {slot/port} p2p`
- `default spanning-tree mstp port {slot/port} priority`
- `default spanning-tree mstp port {slot/port} protocol-migration`
- `no spanning-tree mstp`
- `no spanning-tree mstp port {slot/port}`
- `spanning-tree mstp port {slot/port} cost <1-200000000>`
- `spanning-tree mstp port {slot/port} edge-port { false | true }`
- `spanning-tree mstp port {slot/port} force-port-state enable`
- `spanning-tree mstp port {slot/port} hello-time <100-1000>`
- `spanning-tree mstp port {slot/port} p2p auto`
- `spanning-tree mstp port {slot/port} p2p force-false`
- `spanning-tree mstp port {slot/port} p2p force-true`
- `spanning-tree mstp port {slot/port} priority <0-240>`
- `spanning-tree mstp port {slot/port} protocol-migration false`
- `spanning-tree mstp port {slot/port} protocol-migration true`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
<0-240>	Specifies the four most significant bits of the port identifier. The values configured for port priority must be in steps of 16.
<100-1000>	Configures the hello-time for a port in one hundredths of a second.
<1-200000000>	Specifies the cost value.
<auto|force-false|false-true>	A value of force-true indicates that this port is treated as if it connects to a point-to-point link. A value of force-false indicates that this port is treated as having a shared media connection. A value of auto indicates that this port is considered to have a point-to-point link if it is an aggregator and all of its members are aggregatable, or if the MAC entity is configured for full-duplex operation, either through autonegotation or by management means.
edge-port <false|true>	Enables or disables the port as an edge port. The default is disabled (false).
port {slot/port}	Specifies the slot and port to configure.
protocol-migration <false|true>	Configures the protocol migration state of this port. The default is false.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree mstp priority (globally)

Assign the Multiple Spanning Tree Protocol (MSTP) bridge priority.

Syntax

- `default spanning-tree mstp priority`
- `spanning-tree mstp priority <0-61440>`

Default

`The default is 32768.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<0-61440>`	Assigns the MSTP bridge priority. The values configured for port priority must be in steps of 4096.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree mstp priority (on a port)

Specify the four most significant bits of the port identifier for a given spanning tree instance that can be modified independently for each spanning tree instance supported by the bridge.

Syntax

- `default spanning-tree mstp priority`
- `spanning-tree mstp priority <0-240>`

Default

`The default is 128.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<0-240>`	Specifies the four most significant bits of the port identifier. The values configured for port priority must be in steps of 16.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree mstp protocol-migration

Initiates or terminates protocol migration for the port. If enabled, the port transmits BPDUs without instance information.

Syntax

- `default spanning-tree mstp protocol-migration`
- `spanning-tree mstp protocol-migration false`
- `spanning-tree mstp protocol-migration true`

Default

`The default is false.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<false|true>`	Configures the protocol migration state of this port.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree mstp region

Assign the Multiple Spanning Tree Protocol (MSTP) region.

Syntax

- `spanning-tree mstp region config-id-sel <0-255>[region-name WORD<1-32>] [region-version <0-65535>]`

Default

`The default region and version is 0.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`config-id-sel <0-255>`	Assigns the MSTP region configuration ID number.
`region-name WORD<1-32>`	Assigns the MSTP region name.
`region-version <0-65535>`	Assigns the MSTP region version.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree mstp tx-holdcount

Assign the Multiple Spanning Tree Protocol (MSTP) transmit hold count.

Syntax

- `default spanning-tree mstp tx-holdcount`
- `spanning-tree mstp tx-holdcount <1-10>`

Default

`The default is 3.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<1-10>`	Assigns the MSTP transmit hold count.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree mstp version

Assigns the bridge version.

Syntax

- `default spanning-tree mstp version`
- `spanning-tree mstp version mstp`
- `spanning-tree mstp version rstp`
- `spanning-tree mstp version stp-compatible`

Default

`The default is MSTP.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`mstp`	Configures the version as MSTP.
`rstp`	Configures the version as RSTP.
`stp-compatible`	Configures the version as STP compatible. Although STP and MSTP are variations of the same spanning tree protocol, they communicate information differently. A VSP 9000 in MSTI mode cannot recognize the spanning tree groups running on a chassis configured with Nortel STP. MSTP spanning tree groups are not the same as Nortel STP spanning tree groups. Using a VSP 9000 in MSTP mode with another chassis in STP mode can create a loop in the network. You must configure protocol migration to true on all spanning-tree enabled interfaces when you change the spanning tree version from STP-compatible to MSTP for those interfaces to work in the proper mode.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree rstp cost

Configure the contribution of this port to the path cost value for the link.

Syntax

- `default spanning-tree rstp cost`
- `spanning-tree rstp cost <1-200000000>`

Default

`The default is 2000000.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<1-200000000>`	Specifies the cost value.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree rstp edge-port

Configure the port as an edge port.

Syntax

- `default spanning-tree rstp edge-port`
- `spanning-tree rstp edge-port { false | true }`

Default

`The default is disabled (false).`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<false|true>`	Enables or disables the port as an edge port.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree rstp forward-time

Configure the Rapid Spanning Tree Protocol (RSTP) forward delay for the bridge.

Syntax

- `default spanning-tree rstp forward-time`
- `spanning-tree rstp forward-time <400-3000>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`<400-3000>`	Configures the RSTP forward delay for the bridge, in hundredths of a second.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree rstp group-stp enable

Enable or disables Rapid Spanning Tree Protocol (RSTP) for a specific STG.

Syntax

- `default spanning-tree rstp group-stp enable`
- `no spanning-tree rstp group-stp [enable]`
- `spanning-tree rstp group-stp enable`

Default

None

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree rstp hello-time

Configure the hello-time delay for the bridge.

Syntax

- `default spanning-tree rstp hello-time`
- `spanning-tree rstp hello-time <100-1000>`

Default

`The default is 2.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<100-1000>`	Configures the hello-time for a port in one hundredths of a second.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree rstp max-age

Assign the Rapid Spanning Tree Protocol (RSTP) maximum age time for the bridge

Syntax

- `spanning-tree rstp max-age <600-4000>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<600-4000>	Assigns the RSTP maximum age time for the bridge, in one hundredths of a second.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree rstp p2p

Specify the point-to-point status of the LAN segment attached to this port.

Syntax

- `default spanning-tree rstp p2p`
- `spanning-tree rstp p2p auto`
- `spanning-tree rstp p2p force-false`
- `spanning-tree rstp p2p force-true`

Default

`The default is auto.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<auto|force-false|false-true>`	A value of force-true indicates that this port is treated as if it connects to a point-to-point link. A value of force-false indicates that this port is treated as having a shared media connection. A value of auto indicates that this port is considered to have a point-to-point link if it is an aggregator and all of its members are aggregatable, or if the MAC entity is configured for full-duplex operation, either through autonegotation or by management means.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree rstp pathcost-type

Assign the Rapid Spanning Tree Protocol (RSTP) default pathcost version.

Syntax

- `default spanning-tree rstp pathcost-type`
- `spanning-tree rstp pathcost-type <bits16|bits32>`

Default

`The default is 32 bits.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<bits16|bits32>`	Specifies the pathcost value.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree rstp port

Configure all Rapid Spanning Tree Protocol (RSTP) parameters for a port.

Syntax

- `default spanning-tree rstp`
- `default spanning-tree rstp port {slot/port}`
- `no spanning-tree rstp`
- `no spanning-tree rstp port {slot/port}`
- `spanning-tree rstp port {slot/port} cost <1-200000000>`
- `spanning-tree rstp port {slot/port} edge-port { false | true }`
- `spanning-tree rstp port {slot/port} p2p auto`
- `spanning-tree rstp port {slot/port} p2p force-false`
- `spanning-tree rstp port {slot/port} p2p force-true`
- `spanning-tree rstp port {slot/port} priority <0-240>`
- `spanning-tree rstp port {slot/port} protocol-migration false`
- `spanning-tree rstp port {slot/port} protocol-migration true`
- `spanning-tree rstp port {slot/port} stp enable`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`cost <1-200000000>`	Specifies the cost value. The default is 2000000.
`edge-port <false|true>`	Enables or disables the port as an edge port. The default is disabled (false).
`p2p <auto|force-false|false-true>`	A value of force-true indicates that this port is treated as if it connects to a point-to-point link. A value of force-false indicates that this port is treated as having a shared media connection. A value of auto indicates that this port is considered to have a point-to-point link if it is an aggregator and all of its members are aggregatable, or if the MAC entity is configured for full-duplex operation, either through autonegotation or by management means. The default is auto.
`port`	

{slot/port}	Specifies the slot and port to configure.
priority <0-240>	Specifies the four most significant bits of the port identifier. The values configured for port priority must be in steps of 16. The default is 128.
protocol-migration <false|true>	Configures the protocol migration state of this port. The default is false.
stp enable	Enables STP for the port. The default is disabled.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree rstp priority (globally)

Assign the Rapid Spanning Tree Protocol (RSTP) bridge priority.

Syntax

- `default spanning-tree rstp priority`
- `spanning-tree rstp priority <0-61440>`

Default

`The default is 32768.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<0-61440>`	Assigns the RSTP bridge priority in a range of 0 to 61440 in steps of 4096.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree rstp priority (on a port)

Specify the four most significant bits of the port identifier for a given spanning tree instance that can be modified independently for each spanning tree instance supported by the bridge.

Syntax

- `default spanning-tree rstp priority`
- `spanning-tree rstp priority <0-240>`

Default

`The default is 128.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<0-240>`	Specifies the four most significant bits of the port identifier. Assigns RSTP bridge priority in a range of 0-240. The values configured for port priority must be in steps of 16.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree rstp protocol-migration

Initiate or terminate protocol migration for the port. If enabled, the port transmits BPDUs without instance information.

Syntax

- `default spanning-tree rstp protocol-migration`
- `spanning-tree rstp protocol-migration false`
- `spanning-tree rstp protocol-migration true`

Default

`The default is false.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`<false|true>`	Configures the protocol migration state of this port.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree rstp stp

Enable STP on the port.

Syntax

- `default spanning-tree rstp stp`
- `no spanning-tree rstp stp enable`
- `spanning-tree rstp stp enable`

Default

None

Command mode

GigabitEthernet Interface Configuration

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree rstp tx-holdcount

Assign the Rapid Spanning Tree Protocol (RSTP) transmit hold count.

Syntax

- `default spanning-tree rstp tx-holdcount`
- `spanning-tree rstp tx-holdcount <1-10>`

Default

`The default is 6.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<1-10>`	Assigns the RSTP transmit hold count.

©Avaya Inc. 2015 All Rights Reserved.

spanning-tree rstp version

Configure the Rapid Spanning Tree Protocol (RSTP) to set the RSTP configuration.

Syntax

- `default spanning-tree rstp version`
- `spanning-tree rstp version rstp`
- `spanning-tree rstp version stp-compatible`

Default

`The default is RSTP.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`rstp`	Configures the version as RSTP.
`stp-compatible`	Configures the version as STP-compatible.

©Avaya Inc. 2015 All Rights Reserved.

spbm

Enable Shortest Path Bridging MAC (SPBM) globally.

Syntax

- `default spbm`
- `no spbm`
- `spbm`

Default

`The default is disabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

spbm <1-100>

Create the Shortest Path Bridging MAC (SPBM) instance globally. This release supports only one instance. Use the no form of the command to delete the instance globally.

Syntax

- `no spbm <1-100>`
- `spbm <1-100>`

Default

None

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description
<1-100>	Specifies the Shortest Path Bridging MAC (SPBM) instance ID. Creates the SPBM instance. In this release only one SPBM instance is supported.

©Avaya Inc. 2015 All Rights Reserved.

spbm <1-100> b-vid

Add the backbone VLAN (B-VLAN) to the Shortest Path Bridging MAC (SPBM) instance, globally. You can configure a maximum of two B-VLANs. If you add only one B-VLAN to the SPBM instance, it becomes the primary B-VLAN. If you configure two B-VLANs, you must configure one as the primary B-VLAN. Use the no format to remove a B-VLAN from the global SPBM instance.

Syntax

- `no spbm <1-100> b-vid List of VLAN Ids {vlan-id[-vlan-id][,...]}`
- `no spbm <1-100> b-vid List of VLAN Ids {vlan-id[-vlan-id][,...]} primary <1-4084>`
- `spbm <1-100> b-vid List of VLAN Ids {vlan-id[-vlan-id][,...]}`
- `spbm <1-100> b-vid List of VLAN Ids {vlan-id[-vlan-id][,...]} primary <1-4084>`

Default

None

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description
{vlan-id[-vlan-id][,...]}	Specifies the VLANs to add to the Shortest Path Bridging MAC (SPBM) instance as Backbone VLANs (B-VLANs). Sets the IS-IS SPBM instance data VLANs.
<1-100>	Specifies the Shortest Path Bridging MAC (SPBM) instance ID.
primary <1-4084>	Specifies the primary BVLAN by VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

spbm <1-100> ip enable

Configure Shortest Path Bridging MAC (SPBM) IP shortcuts.

Syntax

- `default spbm <1-100> ip enable`
- `no spbm <1-100> ip enable`
- `spbm <1-100> ip enable`

Default

`The default is disabled.`

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description
`ip enable`	Enables Shortest Path Bridging MAC (SPBM) IP shortcuts.

©Avaya Inc. 2015 All Rights Reserved.

spbm <1-100> lsdb-trap enable

Enable a trap when the Shortest Path Bridging MAC (SPBM) Link State Database (LSDB) changes.

Syntax

- `default spbm <1-100> lsdb-trap enable`
- `no spbm <1-100> lsdb-trap enable`
- `spbm <1-100> lsdb-trap enable`

Default

`The default is disabled.`

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description
`lsdb-trap enable`	Enables a trap when the Shortest Path Bridging MAC (SPBM) Link State Database (LSDB) changes.

©Avaya Inc. 2015 All Rights Reserved.

spbm <1-100> multicast enable

Enables SPBM multicast globally.

Syntax

- `default spbm <1-100> multicast enable`
- `no spbm <1-100> multicast enable`
- `spbm <1-100> multicast enable`

Default

`The default is disabled.`

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description
`<1-100>`	Specifies the Shortest Path Bridging MAC (SPBM) instance ID. Creates the SPBM instance. In this release only one SPBM instance is supported.

©Avaya Inc. 2015 All Rights Reserved.

spbm <1-100> multicast fwd-cache-timeout <10-86400>

Configures the timeout value for the Global Router.

Syntax

- `default spbm <1-100> multicast fwd-cache-timeout`
- `no spbm <1-100> multicast fwd-cache-timeout`
- `spbm <1-100> multicast fwd-cache-timeout <10-86400>`

Default

`The default is 210 seconds.`

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description
<10-86400>	Specifies the timeout value. The default is 210 seconds.
<1-100>	Specifies the Shortest Path Bridging MAC (SPBM) instance ID. Creates the SPBM instance. In this release only one SPBM instance is supported.

©Avaya Inc. 2015 All Rights Reserved.

spbm <1-100> nick-name

Configure a global nick-name for the Shortest Path Bridging MAC (SPBM) instance. The system uses the nick-name to calculate the multicast address for the node.

Syntax

- `default spbm <1-100> nick-name`
- `no spbm <1-100> nick-name`
- `spbm <1-100> nick-name x.xx.xx - 2.5 bytes`

Default

`By default, no nickname exists.`

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description
`<1-100>`	Specifies the SPBM instance ID.
`nick-name x.xx.xx - 2.5 bytes`	Specifies the system nick-name (2.5 bytes in the format <x.xx.xx>).

©Avaya Inc. 2015 All Rights Reserved.

spbm <1-100> smlt-peer-system-id

Configure the system ID of the interswitch trunk (IST) peer, so that if it goes down, the local peer can take over forwarding for the failed peer. You must configure this command to use Shortest Path Bridging MAC (SPBM) in a Split MultiLink Trunking (SMLT) environment. The device with the lower system ID is the primary device.

Syntax

- `spbm <1-100> smlt-peer-system-id xxxx.xxxx.xxxx - 6 bytes`

Default

None

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description
<1-100>	Specifies the SPBM instance ID. SMLT peer system ID is part of the required configuration. You must configure the SMLT peer system ID as the nodal MAC of the peer device. In the Intermediate-System-to-Intermediate-System (IS-IS) network, the nodal MAC of devices should be eight apart from each other.
xxxx.xxxx.xxxx - 6 bytes	Specifies the nodal MAC of the peer device as the system ID. Nodal MACs of devices in the Intermediate-System-to-Intermediate-System (IS-IS) network must be 8 apart from each other. Split MultiLink Trunking (SMLT) peer system ID is part of the required configuration. If SMLT virtual Backbone MAC (B-MAC) is not configured, it is derived from the configured SMLT peer system ID and the nodal MAC of the device (IS-IS system ID). SMLT split Backbone Edge Bridge (BEB) is also derived from the SMLT peer system ID and nodal MAC of the device. The device with the lower system ID is primary, the device with the higher system ID is secondary.

©Avaya Inc. 2015 All Rights Reserved.

spbm <1-100> smlt-virtual-bmac

Configure the virtual Backbone MAC (B-MAC) address, which is shared and advertised by both peers. Configuration of this command is optional.

Syntax

- `spbm <1-100> smlt-virtual-bmac 0x00:0x00:0x00:0x00:0x00:0x00`

Default

None

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description
<1-100>	Specifies the SPBM instance ID.
0x00:0x00:0x00:0x00:0x00:0x00	Specifies the virtual MAC address. SMLT virtual B-MAC is the optional configuration. If SMLT virtual B-MAC is not configured, the system derives SMLT virtual B-MAC from the configured SMLT peer system ID and the nodal MAC of the device (IS-IS system ID). The system compares the nodal MAC of the device with the SMLT peer system ID configured and takes the small one, plus 0x01, as the SMTL virtual B-MAC. The system also derives SMLT split BEB from the SMLT peer system ID and nodal MAC of the device. The device with the lower system ID is primary, the device with the higher system ID is secondary.

©Avaya Inc. 2015 All Rights Reserved.

spbm ethertype

Configure the ethertype for Shortest Path Bridging MAC (SPBM).

Syntax

- `default spbm ethertype`
- `spbm ethertype 0x8100`
- `spbm ethertype 0x88a8`

Default

`The default is 0x8100.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`0x8100`	Configures the ethertype to 0x8100.
`0x88a8`	Configures the ethertype to 0x88a8.

©Avaya Inc. 2015 All Rights Reserved.

speed

Configure the speed of the port on the Ethernet modules.

Syntax

- `default speed`
- `default speed port {slot/port[-slot/port][,...]}`
- `speed 10`
- `speed 100`
- `speed port {slot/port[-slot/port][,...]} 10`
- `speed port {slot/port[-slot/port][,...]} 100`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
<10|100>	Specifies the port speed. Not applicable to 1 Gigabit or 10 GigabitEthernet modules.
port	Specifies the slot and the port number.

©Avaya Inc. 2015 All Rights Reserved.

speed (for the management port)

Configure the speed for the Ethernet management (mgmt) port on the CP module.

Syntax

- `default speed [port {slot/port[-slot/port][,...]}]`
- `speed <10|100|port {slot/port[-slot/port][,...]}>`

Default

`The default is 10 Mb/s.`

Command mode

mgmtEthernet Interface Configuration

Command parameters

Parameter	Description
`<10|100>`	Configures the connection speed for ports to 10 Mb/s or 100 Mb/s.
`port{slot/port[-slot/port][,...]}`	Identifies the slot and port to configure the speed for the ethernet management port. Slots available are 1 and 2.

©Avaya Inc. 2015 All Rights Reserved.

spf-delay

Configure the delay, in milliseconds, to pace successive Shortest Path First (SPF) runs. The timer prevents more than two SPF runs from being scheduled back-to-back. The mechanism for pacing SPF allows two back-to-back SPF runs.

Syntax

- `default spf-delay`
- `no spf-delay`
- `spf-delay <0-5000>`

Default

`The default is 100 milliseconds.`

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description
`<0-5000>`	Configures the delay, in milliseconds.

©Avaya Inc. 2015 All Rights Reserved.

spoof-detect

Configure the spoof detection to prevent an IP spoofing.

Syntax

- `default spoof-detect`
- `default spoof-detect enable`
- `default spoof-detect port {slot/port[-slot/port][,...]}`
- `default spoof-detect port {slot/port[-slot/port][,...]} enable`
- `no spoof-detect`
- `no spoof-detect enable`
- `no spoof-detect port {slot/port[-slot/port][,...]}`
- `no spoof-detect port {slot/port[-slot/port][,...]} enable`
- `spoof-detect`
- `spoof-detect enable`
- `spoof-detect port {slot/port[-slot/port][,...]}`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables spoof detection on the port.
`port {slot/port [-slot/port][,...]}`	Specifies the port list.

©Avaya Inc. 2015 All Rights Reserved.

ssh (configuration)

Modify Secure Shell (SSH) configuration parameters to support public and private key encryption connections.

Syntax

- default ssh
- default ssh dsa-auth
- default ssh max-sessions
- default ssh pass-auth
- default ssh port
- default ssh rsa-auth
- default ssh secure
- default ssh timeout
- default ssh version
- no ssh
- no ssh dsa-auth
- no ssh dsa-host-key
- no ssh dsa-user-key WORD<1-15>
- no ssh pass-auth
- no ssh rsa-auth
- no ssh rsa-host-key
- no ssh secure
- ssh
- ssh dsa-auth
- ssh dsa-host-key
- ssh dsa-host-key <512-1024>
- ssh dsa-user-key WORD<1-15>
- ssh dsa-user-key WORD<1-15> size <512-4096>
- ssh max-sessions <0-8>
- ssh pass-auth
- ssh port <22, 1024..49151>

- `ssh rsa-auth`
- `ssh rsa-host-key`
- `ssh rsa-host-key <512-1024>`
- `ssh secure`
- `ssh timeout <1-120>`
- `ssh version <both|v2only>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`dsa-auth`	Enables or disables the DSA authentication.
`dsa-host-key <512-1024>`	Generates a new SSH DSA host key. The range of the host key size is 512 to 1024.
`dsa-user-key WORD<1-15> [size <512-4096>]`	Creates the DSA user key file. WORD<1-15> specifies the user access level. The valid user access levels for the Virtual Services Platform 9000 are: rwa - Specifies read-write-all. rw - Specifies read-write. ro - Specifies read-only rwl3 - Specifies read-write for Layer 3. rwl2 - Specifies read-write for Layer 2. rwl1 - Specifies read-write for Layer 1. size <512-4096> specifies the key size. The default is 1024 bits.
`max-sessions <0-8>`	Specifies the maximum number of SSH sessions allowed. A value from 0 to 8. Default is 4.
`pass-auth`	Enables password authentication.
`port <22, 1024..49151>`	Sets the Secure Shell (SSH) connection port. <22,1024..49151> is the TCP port number. The default is 22.
`rsa-auth`	Enable RSA authentication.
`rsa-host-key <512-1024>`	Generates new Secure Shell (SSH) RSA host key. The range of the SSH host key size is 512 to 1024.
`secure`	Enables Secure Shell (SSH) in secure mode and immediately disables the access services SNMP, FTP, TFTP, rlogin, and Telnet.
`timeout <1-120>`	The Secure Shell (SSH) connection authentication timeout in seconds. Default is 60 seconds.
`version <v2only|both>`	Sets the Secure Shell (SSH) version. Default is v2only. Avaya recommends setting the version to v2 only.

©Avaya Inc. 2015 All Rights Reserved.

ssh (connection)

Connect to a remote Secure Shell (SSH) host.

Syntax

- `ssh WORD<1-256> -l WORD<1-32>`
- `ssh WORD<1-256> -l WORD<1-32> -p <1-32768>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`-l WORD<1-32>`	Specifies the login name of the remote Secure Shell (SSH) server.
`-p <1-32768>`	Specifies the remote Secure Shell (SSH) server port number to which to connect. The default is 22.
`WORD<1-256>`	Specifies the IP address or host name.

©Avaya Inc. 2015 All Rights Reserved.

subnet-vlan

Enable subnet-based VLAN on the port.

Syntax

- `default subnet-vlan`
- `default subnet-vlan enable`
- `default subnet-vlan port {slot/port[-slot/port],[,…]} enable`
- `default subnet-vlan port {slot/port[-slot/port][,...]}`
- `no subnet-vlan`
- `no subnet-vlan enable`
- `no subnet-vlan port {slot/port[-slot/port],[,…]} enable`
- `no subnet-vlan port {slot/port[-slot/port][,...]}`
- `subnet-vlan`
- `subnet-vlan enable`
- `subnet-vlan port {slot/port[-slot/port],[,…]} enable`
- `subnet-vlan port {slot/port[-slot/port][,...]}`

Default

`The default is enabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables or disables subnet-based VLAN for the port.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

synchronization

Enable the router to accept routes from BGP peers without waiting for an update from the IGP.

Syntax

- `default synchronization`
- `no synchronization`
- `synchronization`

Default

`The default value is enable.`

Command mode

BGP Router Configuration

©Avaya Inc. 2015 All Rights Reserved.

sys action

Reset system functions to reset all statistics counters, the console port, and the operation of the switchover function.

Syntax

- `sys action <cpu-switch-over|reset {console|counters}>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`cpu-switch-over`	Resets the switch to change over to the backup CPU.
`reset {console|counters}`	Reinitializes the hardware universal asynchronous receiver transmitter (UART) drivers. Use this command only if the console connection stops responding. Resets all the statistics counters in the switch to zero. Resets the console port.

©Avaya Inc. 2015 All Rights Reserved.

sys action cpu-switch-over

Perform the switch over of the CPU while hot-swapping the master CP module in a dual CP module chassis.

Syntax

- `sys action cpu-switch-over`
- `sys action cpu-switch-over -coredump`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`-coredump`	Creates a coredump for the main process before the switch changes to the backup CPU. Caution: Only use the -coredump parameter if an issue causes you to switchover the switch, and you need to contact customer service for analysis of the problem.
`cpu-switch-over`	Switches over to the other CPU.

©Avaya Inc. 2015 All Rights Reserved.

sys clipId-topology-ip

Configure the circuitless IP (CLIP) ID as the topology IP.

Syntax

- `default sys clipId-topology-ip`
- `no sys clipId-topology-ip`
- `sys clipId-topology-ip <1-256>`

Default

`The default is 0.`

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-256>	Specifies the CLIP interface ID.

©Avaya Inc. 2015 All Rights Reserved.

sys data-path-fault-shutdown

Enables automatic shutdown of all ports on a lane where data path heartbeats have failed.

Syntax

- `default sys data-path-fault-shutdown`
- `no sys data-path-fault-shutdown`
- `sys data-path-fault-shutdown`

Default

`The default is enabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

sys force-msg

Use the force message control option to extend the message control feature functionality to the software and hardware log messages. To enable the message control feature, you must specify an action, control interval, and maximum message number. After you enable the feature, the log messages, which get repeated and cross the maximum message number in the control interval, trigger the force message feature. You can either suppress the message or send a trap notification, or both.

Syntax

- `no sys force-msg WORD<4-4>`
- `sys force-msg WORD<4-4>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
WORD<4-4>	Adds a forced message control pattern. WORD<4-4> is a string of 4 characters. You can add a four-byte pattern into the force-msg table. The software and the hardware log messages that use the first four bytes matching one of the patterns in the force-msg table undergo the configured message control action. You can specify up to 32 different patterns in the force-msg table, including a wildcard pattern (****). If you specify the wildcard pattern, all messages undergo message control.

©Avaya Inc. 2015 All Rights Reserved.

sys force-topology-ip-flag

Activate or disable the flag that Configure the CLIP ID as the topology IP.

Syntax

- `default sys force-topology-ip-flag [enable]`
- `no sys force-topology-ip-flag [enable]`
- `sys force-topology-ip-flag enable`

Default

`The default is disabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

syslog enable

The syslog commands control a facility in UNIX machines that logs SNMP messages and assigns each message a severity level based on importance.

Syntax

- `syslog enable`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
enable	Enables the sending of syslog messages on the switch.

©Avaya Inc. 2015 All Rights Reserved.

syslog host

The syslog commands control a facility in UNIX machines that logs SNMP messages and assigns each message a severity level based on importance.

Syntax

- `syslog host <1-10>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`address WORD<0-46>`	Configures a host location for the syslog host. WORD<0-46> is the IP address of the UNIX system syslog host.
`enable`	Enables the syslog host.
`facility {local0|local1|local2|local3|local4|local5|local6|local7}`	Specifies the UNIX facility used in messages to the syslog host. {local0|local1|local2|local3|local4|local5|local6|local7} is the UNIX system syslog host facility (LOCAL0 to LOCAL7).
`host`	Specifies host settings.
`maperror {emergency|alert|critical|error|warning|notice|info|debug}`	Specifies the syslog severity to use for Error messages.
`mapfatal {emergency|alert|critical|error|warning|notice|info|debug}`	Specifies the syslog severity to use for Fatal messages.
`mapinfo {emergency|alert|critical|error|warning|notice|info|debug}`	Specifies the syslog severity level to use for Information messages.
`mapwarning {emergency|alert|critical|error|warning|notice|info|debug}`	Specifies the syslog severity to use for Warning messages.
`severity <info|warning|error|fatal>`	Specifies the severity levels for which syslog messages should be sent for the specified modules.
`udp-port <514-530>`	Specifies the UDP port number on which to send syslog messages to the syslog host. This is the UNIX system syslog host port number (514 to 530).

©Avaya Inc. 2015 All Rights Reserved.

sys log ip-header-type

Specify the IP header in syslog packets.

Syntax

- `default syslog ip-header-type`
- `syslog ip-header-type circuitless-ip`
- `syslog ip-header-type default`
- `syslog ip-header-type management-virtual-ip`

Default

`The default is default.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`circuitless-ip`	For all syslog messages (in-band or out-of-band), the circuitless IP address is used in the IP header. If you configure multiple CLIPs, the first CLIP configured is used.
`default`	For syslog packets that are transmitted in-band via input/output (I/O) ports, the IP address of the VLAN is used. For syslog packets that are transmitted out-of-band through the management port, the physical IP address of the Master CPU is used in the IP header.
`management-virtual-ip`	For syslog packets that are transmitted out-of-band only through the management port, the virtual management IP address of the switch is used in the IP header.

©Avaya Inc. 2015 All Rights Reserved.

Home | Command modes | Alphabetical listing

syslog max-hosts <1-10>

Specify the maximum number of syslog hosts supported.

Syntax

- `default syslog max-hosts`
- `syslog max-hosts <1-10>`

Default

`The default is 5.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

sys mgmt-virtual-ip

Assign an IP address to a virtual management port to use it for out-of-band (OOB) management. Create a virtual management port in addition to the physical management ports on the switch management modules.

Syntax

- `default sys mgmt-virtual-ip`
- `no sys mgmt-virtual-ip`
- `sys mgmt-virtual-ip {A.B.C.D/X|A.B.C.D A.B.C.D}`

Default

`The default is no virtual IP address for the management port.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`{A.B.C.D/X|A.B.C.D A.B.C.D}`	Specifies the IP address and subnet mask in the format A.B.C.D/x or A.B.C.D/A.B.C.D. (For example, 10.127.231.15 255.255.255.0).Important You cannot assign an address of 0.0.0.0/0.

©Avaya Inc. 2015 All Rights Reserved.

sys msg-control

Configure system message control to suppress duplicate error messages on the console and to determine the action to take if they occur.

Syntax

- `default sys msg-control [action] [control-interval] [max-msg-num]`
- `no sys msg-control`
- `sys msg-control [action <both|send-trap|suppress-msg>][control-interval <1-30>] [max-msg-num <2-500>]`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`action <both|send-trap| suppress-msg>`	Configures the message control action. You can either suppress the message or send a trap notification, or both. The default is suppress-msg.
`control-interval <1-30>`	Configures the message control interval in minutes. The default control-interval is 5.
`max-msg-num <2-500>`	Configures the number of occurrences of a message after which the control action occurs. The default is 5 messages.

©Avaya Inc. 2015 All Rights Reserved.

sys mtu

Enable support for jumbo frames on Virtual Services Platform 9000.

Syntax

- `default sys mtu`
- `sys mtu <1522-9600>`

Default

`The default value is 1950.`

Command mode

Global Configuration

Command parameters

Parameter	Description
<1522-9600>	Activates Jumbo frame support for the data path. The value can be either 1522, 1950, or 9600 bytes. 1950 or 9600 bytes activate Jumbo frame support.

©Avaya Inc. 2015 All Rights Reserved.

sys name

Configure system identification to specify the name of the switch.

Syntax

- `default sys name`
- `sys name WORD<0-255>`

Default

`The default is VSP-9012.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`name WORD<0-255>`	Configures the system or root level prompt name for the switch. WORD<0-255> is an ASCII string from 1-255 characters (for example, LabSC7 or Closet4).

©Avaya Inc. 2015 All Rights Reserved.

sys-name

Configure the name for the system.

Syntax

- `default sys-name`
- `no sys-name`
- `sys-name WORD<0-255>`

Default

`By default, the system name is the host name at the system level.`

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description
`WORD<0-255>`	Specifies the system name.

©Avaya Inc. 2015 All Rights Reserved.

sys power

Enable power redundancy to create traps and events after power consumption exceeds redundancy capacity. Configure the slot priority to determine which slots shut down if insufficient power is available in the chassis. The slot with the lowest priority shuts down first. Slots with the same priority shut down in descending order (highest slot number first).

Syntax

- `default sys power`
- `default sys power fan-check`
- `default sys power slot {slot[-slot][,...]}`
- `default sys power slot-priority {<3-12>|SF2|SF3|SF5|SF6}`
- `no sys power fan-check`
- `no sys power slot {slot[-slot][,...]}`
- `sys power fan-check`
- `sys power slot {slot[-slot][,...]}`
- `sys power slot-priority {<3-12>|SF2|SF3|SF5|SF6} {critical|high|low}`

Default

`Power management is enabled by default.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`fan-check`	Enables fan check to check the power management on the port. The default is enable.
`slot {slot[-slot][,...]}`	Enables power for a specific slot. Identify the slot in one of the following formats: a single slot (3), a range of slots (3-6), or a series of slots (3,5,6). The valid slots are: 1-12 or SF1-SF6. The default is enabled.
`slot-priority {<3-12>|SF2|SF3|SF5|SF6} {critical|high|low}`	Designates the slot priority. You can configure priority for the interface module slots (3-12) or for Switch Fabric slots 2, 3, 5, and 6. The default is high.

©Avaya Inc. 2015 All Rights Reserved.

sys shutdown

Use this command to prepare the system for shutdown. This command properly shuts down the file system, and powers off all interface modules and Switch Fabric modules. The power supplies, cooling modules, and CP modules remain in the powered on state. After you use this command, you must physically turn off the chassis power. To restore power after you use this command, you must physically turn the chassis power on again.

Syntax

- `sys shutdown`

Default

None

Command mode

Privileged EXEC

©Avaya Inc. 2015 All Rights Reserved.

sys software auto-commit

Enable the auto-commit feature for software upgrades. If you enable the auto-commit option, the system automatically commits to the new software version after the commit timer expires. If you do not enable the auto-commit option, you must enter the software commit command before the commit timer expires to commit the new software version otherwise the system restarts automatically to the previous (committed) version.

Syntax

- `default sys software auto-commit enable`
- `no sys software auto-commit enable`
- `sys software auto-commit enable`

Default

`The default is enabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

sys software commit-time

Configure the commit feature for software upgrades to allows maximum time to ensure that the upgrade is successful. You must enter the software commit command before the commit timer expires to commit the new software version otherwise the system restarts automatically to the previous (committed) version.

Syntax

- `default sys software commit-time`
- `sys software commit-time <10-60>`

Default

The default is 10 minutes.

Command mode

Global Configuration

Command parameters

Parameter	Description
<10-60>	Specifies the commit timer in minutes.

©Avaya Inc. 2015 All Rights Reserved.

sys software patch

Configure the software patch.

Syntax

- `default sys software patch file-path`
- `sys software patch file-path WORD<1-255>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
WORD<1-255>	Specifies the location of the file to patch.

©Avaya Inc. 2015 All Rights Reserved.

system-id

Configure a system ID. You must configure a system ID before you enable IS-IS. You cannot delete the system ID but you can change it if you first disable IS-IS.

Syntax

- `default system-id`
- `no system-id`
- `system-id xxxx.xxxx.xxxx - 6 bytes`

Default

`The default system ID is the node Backbone MAC.`

Command mode

IS-IS Router Configuration

Command parameters

Parameter	Description
`xxxx.xxxx.xxxx - 6 bytes`	Specifies the system ID in 6 octets.

©Avaya Inc. 2015 All Rights Reserved.

tacacs accounting

Determines for which applications TACACS+ collects accounting information. Use TACACS+ accounting to track the services that users access and the amount of network resources that users consume.

Syntax

- `default tacacs accounting cli`
- `no tacacs accounting cli`
- `tacacs accounting disable`
- `tacacs accounting disable cli`
- `tacacs accounting enable cli`

Default

`None. If unassigned, TACACS+ does not perform the accounting function.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`cli`	Specifies the command line as the application.
`disable`	Disables the accounting function for the specified application.
`enable`	Enables the accounting function for the specified application.

©Avaya Inc. 2015 All Rights Reserved.

tacacs authentication

Determines which applications TACACS+ authenticates.

Syntax

- `default tacacs authentication all`
- `default tacacs authentication cli`
- `default tacacs authentication web`
- `no tacacs authentication all`
- `no tacacs authentication cli`
- `no tacacs authentication web`
- `tacacs authentication all`
- `tacacs authentication cli`
- `tacacs authentication web`

Default

`The default value is disabled.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`all`	TACACS+ authenticates all applications.
`cli`	TACACS+ authenticates command line connections.
`web`	TACACS+ authenticates web connections.

©Avaya Inc. 2015 All Rights Reserved.

tacacs authorization

Enables command authorization for a particular privilege level. Use this option to limit the use of certain commands to different users. To use TACACS+ authorization, you must also use TACACS+ authentication.

Syntax

- `default tacacs authorization`
- `no tacacs authorization enable`
- `no tacacs authorization level <1-6>`
- `tacacs authorization disable`
- `tacacs authorization enable`
- `tacacs authorization level <1-6>`
- `tacacs authorization level all`
- `tacacs authorization level none`

Default

`The default is disabled.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`disable`	Disables command authorization.
`enable`	Enables command authorization.
`level <1-6>`	Enables command authorization for a specific privilege level.
`level all`	Enables command authorization for all privilege levels.
`level none`	Disables command authorization for all privilege levels.

©Avaya Inc. 2015 All Rights Reserved.

tacacs protocol enable

Globally enables or disables TACACS+.

Syntax

- `default tacacs protocol enable`
- `no tacacs protocol enable`
- `tacacs protocol enable`

Default

`The default is disabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

tacacs server host

Configures the entry for the primary TACACS+ server.

Syntax

- `default tacacs server {A.B.C.D}`
- `default tacacs server {A.B.C.D} port`
- `default tacacs server {A.B.C.D} single-connection`
- `default tacacs server {A.B.C.D} single-connection source source-ip-interface enable`
- `default tacacs server {A.B.C.D} source source-ip-interface enable`
- `default tacacs server {A.B.C.D} timeout`
- `no tacacs server {A.B.C.D}`
- `no tacacs server {A.B.C.D} single-connection`
- `no tacacs server {A.B.C.D} source source-ip-interface enable`
- `tacacs server host {A.B.C.D}`
- `tacacs server host {A.B.C.D} key WORD<0-128>`
- `tacacs server host {A.B.C.D} port <1-65535>`
- `tacacs server host {A.B.C.D} port <1-65535> source {A.B.C.D} source-ip-interface enable`
- `tacacs server host {A.B.C.D} single-connection`
- `tacacs server host {A.B.C.D} source {A.B.C.D} source-ip-interface enable`
- `tacacs server host {A.B.C.D} timeout <10-30>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`{A.B.C.D}`	Specifies the IP address of the primary TACACS+ server.
`key WORD<0-128>`	Configures the secret key to share with this TACACS+ server. If the key length is zero, that indicates no encryption is used.
`port <1-65535>`	Configures the TCP port on which the client establishes a connection to the server. A value of 0 indicates that the system specified default value is used. The default is 49.

single-connection	Specifies if the TCP connection between the device and the TACACS+ server is a single connection. If you do not enable the single-connection parameter, the system uses the default connection type that opens and closes a connection for each communication session.
source {A.B.C.D}	Configures the IP address of the interface to use with this server. If you do not configure an address, the system uses 0.0.0.0 as the default.
source-ip-interface enable	Enables the source address. You must enable this parameter if you configure a valid source IP address. The default is disabled.
timeout <10-30>	Configures the maximum time, in seconds, to wait for this TACACS+ server to reply. The default is 10 seconds.

©Avaya Inc. 2015 All Rights Reserved.

tacacs server secondary-host

Configures the entry for the secondary TACACS+ server.

Syntax

- `default tacacs server {A.B.C.D}`
- `default tacacs server {A.B.C.D} port`
- `default tacacs server {A.B.C.D} single-connection`
- `default tacacs server {A.B.C.D} single-connection source source-ip-interface enable`
- `default tacacs server {A.B.C.D} source source-ip-interface enable`
- `default tacacs server {A.B.C.D} timeout`
- `no tacacs server {A.B.C.D}`
- `no tacacs server {A.B.C.D} single-connection`
- `no tacacs server {A.B.C.D} source source-ip-interface enable`
- `tacacs server secondary-host {A.B.C.D}`
- `tacacs server secondary-host {A.B.C.D} key WORD<0-128>`
- `tacacs server secondary-host {A.B.C.D} port <1-65535>`
- `tacacs server secondary-host {A.B.C.D} single-connection`
- `tacacs server secondary-host {A.B.C.D} source {A.B.C.D} source-ip-interface enable`
- `tacacs server secondary-host {A.B.C.D} timeout <10-30>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`{A.B.C.D}`	Specifies the IP address of the secondary TACACS+ server.
`key WORD<0-128>`	Configures the secret key to share with this TACACS+ server. If the key length is zero, that indicates no encryption is used.
`port <1-65535>`	Configures the TCP port on which the client establishes a connection to the server. A value of 0 indicates that the system specified default value is used. The default is 49.
	Specifies if the TCP connection between the device and the TACACS+ server is a single

single-connection	connection. If you do not enable the single-connection parameter, the system uses the default connection type that opens and closes a connection for each communication session.
source {A.B.C.D}	Configures the IP address of the interface to use with this server. If you do not configure an address, the system uses 0.0.0.0 as the default.
source-ip-interface enable	Enables the source address. You must enable this parameter if you configure a valid source IP address. The default is disabled.
timeout <10-30>	Configures the maximum time, in seconds, to wait for this TACACS+ server to reply. The default is 10 seconds.

©Avaya Inc. 2015 All Rights Reserved.

tacacs switch

Changes the privilege level to determine what commands a user can access through TACACS+ server authorization. You must configure separate profiles in the TACACS+ server configuration file for switch level.

Syntax

- `tacacs switch back`
- `tacacs switch level`
- `tacacs switch level <1-15>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`back`	Returns the privilege level to the original level.
`level <1-15>`	Selects a specific privilege level. VSP 9000 supports levels 1 through 6: read-only (1), Layer 1 read-write (2), Layer 2 read-write (3), Layer 3 read-write (4), read-write (5), and read-write-all (6), and level 15.

©Avaya Inc. 2015 All Rights Reserved.

tagged-frames-discard

Discards tagged frames on the port.

Syntax

- `default tagged-frames-discard`
- `default tagged-frames-discard enable`
- `default tagged-frames-discard port {slot/port[-slot/port][,...]}`
- `default tagged-frames-discard port {slot/port[-slot/port][,...]} enable`
- `no tagged-frames-discard`
- `no tagged-frames-discard enable`
- `no tagged-frames-discard port {slot/port[-slot/port][,...]}`
- `no tagged-frames-discard port {slot/port[-slot/port][,...]} enable`
- `tagged-frames-discard`
- `tagged-frames-discard enable`
- `tagged-frames-discard port {slot/port[-slot/port][,...]}`
- `tagged-frames-discard port {slot/port[-slot/port][,...]} enable`

Default

`The default is disabled.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Discards tagged frames on the port.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

telnet

Use this command to access another platform remotely.

Syntax

- `telnet [WORD<1-256>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
WORD <1-256>	Specifies the host name, IPv4 address or IPv6 address.

©Avaya Inc. 2015 All Rights Reserved.

telnet-access sessions

Configures the number of supported inbound Telnet sessions.

Syntax

- `default telnet-access sessions`
- `telnet-access sessions <0-8>`

Default

`The default is 8.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<0-8>`	Configures the allowable number of inbound Telnet sessions.

©Avaya Inc. 2015 All Rights Reserved.

terminal

Configures the ACLI display.

Syntax

- `terminal length <8-64>`
- `terminal length default`
- `terminal more <enable|disable>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`length <8-64>`	Configures the number of lines in the output display for the current session. The default is 23.
`length default`	Configures the number of lines in the output display for the current session to the default value.
`more <enable|disable>`	Configures scrolling for the output display. The default is enabled.

©Avaya Inc. 2015 All Rights Reserved.

timers basic holddown (for OSPF)

Configures the OSPF hold-down timer value, the length of time (in seconds) that OSPF continues to advertise a network after determining that it is unreachable.

Syntax

- `default timers basic`
- `default timers basic holddown`
- `timers basic holddown <3-60>`

Default

`The default is 120 seconds.`

Command mode

OSPF Router Configuration

Command parameters

Parameter	Description
`<3-60>`	Configures the holddown timer value.

©Avaya Inc. 2015 All Rights Reserved.

timers basic holddown (for RIP)

Configures the RIP hold-down timer value, the length of time (in seconds) that RIP continues to advertise a network after determining that it is unreachable.

Syntax

- `default timers basic holddown`
- `timers basic holddown <0-360>`

Default

`The default is 120 seconds.`

Command mode

RIP Router Configuration

Command parameters

Parameter	Description
`<0-360>`	Configures the holddown timer value.

©Avaya Inc. 2015 All Rights Reserved.

timers basic timeout

Configure the RIP timeout interval.

Syntax

- `default timers basic timeout`
- `timers basic timeout <15-259200>`

Default

`The default value is 180.`

Command mode

RIP Router Configuration

Command parameters

Parameter	Description
<15-259200>	Configures the value of default import metric to import a route into RIP domain.

©Avaya Inc. 2015 All Rights Reserved.

timers basic update

Configure the RIP update timer. The update time is the time interval between RIP updates.

Syntax

- `default timers basic update`
- `timers basic update <1-360>`

Default

`The default is 30 seconds.`

Command mode

RIP Router Configuration

Command parameters

Parameter	Description
`<1-360>`	Configures the update interval.

©Avaya Inc. 2015 All Rights Reserved.

trace cfm level <0-4>

Starts debug tracing for CFM. <0-4> specifies the trace level from 0 to 4, where 0 is disabled; 1 is very terse; 2 is terse; 3 is very verbose, 4 is verbose.

Syntax

- `trace cfm level <0-4>`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

trace filter file

Specifies the trace messages to filter.

Syntax

- `trace filter file WORD<0-128>`
- `trace filter file WORD<0-128> bt limit WORD<0-256>`
- `trace filter file WORD<0-128> clear`
- `trace filter file WORD<0-128> disable`
- `trace filter file WORD<0-128> lines`
- `trace filter file WORD<0-128> lines WORD<0-256>`
- `trace filter file WORD<0-128> range`
- `trace filter file WORD<0-128> range WORD<0-256> WORD<0-256>`
- `trace filter file WORD<0-128> supress`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`WORD<0-128>`	Specifies the filename.
`bt limit WORD<0-256>`	Performs backtrace filtering for a specific limit value.
`clear`	Clears trace filter information.
`disable`	Disables the trace filter.
`lines WORD<0-256>`	Specifies the lines to filter.
`range WORD<0-256> WORD<0-256>`	Specifies the range to filter.
`suppress`	Suppresses the trace filter.

©Avaya Inc. 2015 All Rights Reserved.

trace filter module

Specifies the trace messages to filter.

Syntax

- `trace filter module <0-136>`
- `trace filter module <0-136> clear`
- `trace filter module <0-136> disable`
- `trace filter module <0-136> info`
- `trace filter module <0-136> supress`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`<0-136>`	Specifies the module ID.
`clear`	Clears trace filter information.
`disable`	Disables the trace filter.
`info`	Shows the trace filter configuration for the module.
`suppress`	Suppresses the trace filter.

©Avaya Inc. 2015 All Rights Reserved.

trace flags isis

Enable or disable the Intermediate-System-to-Intermediate-System trace flags. After IS-IS trace is turned on, only trace information about the set flag appears.

Syntax

- `trace flags isis`
- `trace flags isis remove { none | tx-hello | rx-hello | tx-pkt | rx-pkt | adj | opt | tx-lsack | rx-lsack | tx-lsp | rx-lsp | pkt-err | nbr-mismatch | flood | spf-intra | spf-inter | spf-extern | prefix | nbr-change | intf-change | decide | fdb | dr | dd-masterslave | auth-fail | config | purge | policy | redist | tx-snp | rx-snp | timer | spbm-decide | global | perf | ha | ucast-fib | node | mcast-fib | isid | ip-shortcut | debug | ip-multicast }`
- `trace flags isis set { none | tx-hello | rx-hello | tx-pkt | rx-pkt | adj | opt | tx-lsack | rx-lsack | tx-lsp | rx-lsp | pkt-err | nbr-mismatch | flood | spf-intra | spf-inter | spf-extern | prefix | nbr-change | intf-change | decide | fdb | dr | dd-masterslave | auth-fail | config | purge | policy | redist | tx-snp | rx-snp | timer | spbm-decide | global | perf | ha | ucast-fib | node | mcast-fib | isid | ip-shortcut | debug | ip-multicast }`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
adj	Specifies the option of adjacencies.
auth-fail	Specifies the option of authorization failed.
config	Specifies the option of configuration.
dd-masterslave	The current release does not use this option.
debug	Specifies the option of debug.
decide	Specifies the option of shortest path first computation.
dr	Specifies the option of designated router.
fdb	Specifies the option of filtering database.
flood	Specifies the option of flood.
global	The current release does not use this option.
ha	Specifies the option of High Availability.
intf-change	Specifies the option of IS-IS circuit (interface) events.
ip-multicast	Specifies the option of IP multicast.
ip-shortcut	Specifies the option of IP Shortcut.
isid	Specifies the option of I-SID.
mcast-fib	Specifies the option of multicast forwarding information base.
nbr-change	Specifies the option of neighbor change.

nbr-mismatch	Specifies the option of neighbor mismatch.
node	Specifies the option of node.
none	Specifies the option of none.
opt	Specifies the option of IS-IS TLVs.
perf	Specifies the option of SPBM performance.
pkt-err	Specifies the option of packet error.
policy	The current release does not use this option.
prefix	Specifies the option of prefix.
purge	Specifies the option of Link State Packet purge.
redist	Specifies the option of redistribute.
remove	Removes the Intermediate-System-to-Intermediate-System (IS-IS) trace flags for the specified option.
rx-hello	Specifies the option of received IS-IS hello packets.
rx-lsack	Specifies the option of received LSP acknowledgement.
rx-lsp	Specifies the option of received Link State Packet.
rx-pkt	Specifies the option of received packets.
rx-snp	Specifies the option of received sequence number packet (CSNP and PSNP).
set	Configures the Intermediate-System-to-Intermediate-System (IS-IS) trace flags for the specified option.
spbm-decide	Specifies the option of shortest path first computation for SPBM.
spf-extern	Specifies the option of shortest path first external.
spf-inter	Specifies the option of shortest path first internal.
spf-intra	The current release does not use this option.
timer	Specifies the option of timer.
tx-hello	Specifies the option of transmitted IS-IS hello packets.
tx-lsack	Specifies the option of transmitted LSP acknowledgement.
tx-lsp	Specifies the option of transmitted Link State Packet.
tx-pkt	Specifies the option of transmitted packets.
tx-snp	Specifies the option of transmitted sequence number PDU (CSNP and PSNP).
ucast-fib	Specifies the option of unicast forwarding information base.

©Avaya Inc. 2015 All Rights Reserved.

trace flags ospf

Enable or disables OSPFv2 trace flags for debugging. The flags you set are used by the trace level.

Syntax

- `trace flags ospf remove <none|all|tx-hello|rx-hello|tx-ddp-pkt|rx-ddp-pkt|tx-lsu-pkt|rx-lsu-pkt|tx-lsack|rx-lsack|tx-lsr|rx-lsr|pkt-err|nbr-mismatch|flood|spf-intra|spf-inter|spf-extern|spf-tree|nbr-change|intf-change|abr-lsa-generate|asbr-lsa-generate|dr|dd-masterslave|auth-fail|config|lsa|policy>`
- `trace flags ospf set <none|all|tx-hello|rx-hello|tx-ddp-pkt|rx-ddp-pkt|tx-lsu-pkt|rx-lsu-pkt|tx-lsack|rx-lsack|tx-lsr|rx-lsr|pkt-err|nbr-mismatch|flood|spf-intra|spf-inter|spf-extern|spf-tree|nbr-change|intf-change|abr-lsa-generate|asbr-lsa-generate|dr|dd-masterslave|auth-fail|config|lsa|policy>`

Default

By default, all flags are turned off.

Command mode

User EXEC

Command parameters

Parameter	Description
`remove <none|all|tx-hello|rx-hello|tx-ddp-pkt|rx-ddp-pkt|tx-lsu-pkt|rx-lsu-pkt|tx-lsack|rx-lsack|tx-lsr|rx-lsr|pkt-err|nbr-mismatch|flood|spf-intra|spf-inter|spf-extern|spf-tree|nbr-change|intf-change|abr-lsa-generate|asbr-lsa-generate|dr|dd-masterslave|auth-fail|config|lsa|policy>`	Removes the OSPF trace flags for the specified option.
`set <none|all|tx-hello|rx-hello|tx-ddp-pkt|rx-ddp-pkt|tx-lsu-pkt|rx-lsu-pkt|tx-lsack|rx-lsack|tx-lsr|rx-lsr|pkt-err|nbr-mismatch|flood|spf-intra|spf-inter|spf-extern|spf-tree|nbr-change|intf-change|abr-lsa-generate|asbr-lsa-generate|dr|dd-masterslave|auth-fail|config|lsa|policy>`	Sets the OSPF trace flags for the specified option.

©Avaya Inc. 2015 All Rights Reserved.

trace grep

Search trace results for a specific string value, for example, the word error.

Syntax

- `trace grep`
- `trace grep WORD<0-128>`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
WORD<0-128>	Specifies the search keyword. You can use a specific MAC address or search for errors, using the command, trace grep error.

©Avaya Inc. 2015 All Rights Reserved.

trace ipv6 base

Configure trace parameters for the IPv6 base.

Syntax

- `trace ipv6 base disable <all|debug|error|icmp|info|ipclient|nbr|pkt|warn>`
- `trace ipv6 base enable <all|debug|error|icmp|info|ipclient|nbr|pkt|warn>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`<all|debug|error|icmp|info|ipclient|nbr|pkt|warn>`	Specifies the trace category.
`disable`	Disables the trace.
`enable`	Enables the trace.

©Avaya Inc. 2015 All Rights Reserved.

trace ipv6 forwarding

Configure trace parameters for IPv6 forwarding.

Syntax

- `trace ipv6 forwarding disable <all|debug|error|info|pkt|warn>`
- `trace ipv6 forwarding enable <all|debug|error|info|pkt|warn>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`<all|debug|error|info|pkt|warn>`	Specifies the trace category.
`disable`	Disables the trace.
`enable`	Enables the trace.

©Avaya Inc. 2015 All Rights Reserved.

trace ipv6 nd

Configure trace parameters for IPv6 neighbor discovery.

Syntax

- `trace ipv6 nd disable <all|debug|error|info|nbr|pkt|redirect|warn>`
- `trace ipv6 nd enable <all|debug|error|info|nbr|pkt|redirect|warn>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`<all|debug|error|info|nbr|pkt|redirect|warn>`	Specifies the trace category.
`disable`	Disables the trace.
`enable`	Enables the trace.

©Avaya Inc. 2015 All Rights Reserved.

trace ipv6 rtm

Configure trace parameters for the IPv6 routing table manager.

Syntax

- `trace ipv6 rtm disable <all|change-list|debug|error|fib|info|redist|update|warn>`
- `trace ipv6 rtm enable <all|change-list|debug|error|fib|info|redist|update|warn>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`<all|change-list|debug|error|fib|info|redist|update|warn>`	Specifies the trace category.
`disable`	Disables the trace.
`enable`	Enables the trace.

©Avaya Inc. 2015 All Rights Reserved.

trace ipv6 transport

Configure trace parameters for IPv6 transport.

Syntax

- `trace ipv6 transport disable <all|common|tcp|udp>`
- `trace ipv6 transport enable <all|common|tcp|udp>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
`<all|common|tcp|udp>`	Specifies the trace category.
`disable`	Disables the trace.
`enable`	Enables the trace.

©Avaya Inc. 2015 All Rights Reserved.

trace level

Use trace to observe the status of a software module at a given time.

Syntax

- `trace level [<0-192>] [<0-4>]`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`level [<0-192>] [<0-4>]`	Starts the trace by specifying the module ID and level.<0-192> specifies the module ID. <0-4> specifies the trace level from 0 to 4, where 0 is disabled; 1 is very terse; 2 is terse; 3 is very verbose, 4 is verbose.

©Avaya Inc. 2015 All Rights Reserved.

traceroute

Use traceroute to determine the route packets take through a network to a destination.

Syntax

- `traceroute WORD<0-256>`
- `traceroute WORD<0-256> <1-1176>`
- `traceroute WORD<0-256> -m <1-255>`
- `traceroute WORD<0-256> -p <1-65535>`
- `traceroute WORD<0-256> -q <1-255>`
- `traceroute WORD<0-256> source WORD<1-256>`
- `traceroute WORD<0-256> -v`
- `traceroute WORD<0-256> vrf WORD<1-16>`
- `traceroute WORD<0-256> -w <1-255>`

Default

None

Command mode

Privileged EXEC

Command parameters

Parameter	Description
<1-1176>	Specifies the size of the probe packet.
-m <1-255>	Specifies the is maximum time-to-live (TTL).
-p <1-65535>	Specifies the base UDP port number.
-q <1-255>	Specifies the number of probes per TTL.
source WORD<1-256>	Specifies the source IP address for use in traceroutes.
-v	Specifies verbose mode (detailed output).
vrf WORD<1-16>	Specifies the VRF instance by VRF name.
-w <1-255>	Specifies the wait time per probe.
WORD<0-256>	Specifies the hostname, IP address, or IPv6 address.

©Avaya Inc. 2015 All Rights Reserved.

trace route-map

Enable or disable trace for route-maps.

Syntax

- `trace route-map { off | on }`
- `trace route-map { off | on } address {A.B.C.D}`
- `trace route-map { off | on } iflist WORD<1-256>`
- `trace route-map { off | on } name WORD<1-64>`
- `trace route-map { off | on } protocol any`
- `trace route-map { off | on } protocol bgp`
- `trace route-map { off | on } protocol ospf`
- `trace route-map { off | on } protocol rip`
- `trace route-map { off | on } type accept`
- `trace route-map { off | on } type announce`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`{ off | on }`	Enables or disables tracing.
`address {A.B.C.D}`	Specifies the interface address.
`iflist WORD<1-256>`	Specifies the interface list name.
`name WORD<1-64>`	Specifies the name of a route-map.
`protocol`	Specifies a routing protocol.
`type`	Specifies a route-map type.

©Avaya Inc. 2015 All Rights Reserved.

trace screen

Configure if the system Display trace information on screen.

Syntax

- `trace screen disable`
- `trace screen enable`

Default

None

Command mode

User EXEC

Command parameters

Parameter	Description
`disable`	Prevents the trace messages from appearing on screen.
`enable`	Shows the trace messages on screen.

©Avaya Inc. 2015 All Rights Reserved.

trace shutdown

Disables trace.

Syntax

- `trace shutdown`

Default

None

Command mode

User EXEC

Avaya Virtual Services Platform 9000 Release 4.0
NN46250-104 ACLI Commands Reference for Avaya Virtual Services Platform 9000
Version 06.04 March 2015
©Avaya Inc. 2015 All Rights Reserved.
Avaya.com/support

trace spbm isis level <0-4>

Starts debug tracing for IS-IS. <0-4> specifies the trace level from 0 to 4, where 0 is disabled; 1 is very terse; 2 is terse; 3 is very verbose, 4 is verbose.

Syntax

- `trace spbm isis level <0-4>`

Default

None

Command mode

User EXEC

©Avaya Inc. 2015 All Rights Reserved.

trap

Enable OSPF traps.

Syntax

- `default trap`
- `default trap enable`
- `no trap`
- `no trap enable`
- `trap enable`

Default

`The default value is disable.`

Command mode

OSPF Router Configuration

Command parameters

Parameter	Description
`enable`	Enables OSPF traps.

©Avaya Inc. 2015 All Rights Reserved.

traps

Enable BGP traps.

Syntax

- `default traps`
- `default traps enable`
- `no traps`
- `no traps enable`
- `traps enable`

Default

`The default value is disable.`

Command mode

BGP Router Configuration

Command parameters

Parameter	Description
`enable`	Enables BGP traps.

©Avaya Inc. 2015 All Rights Reserved.

tx-flow-control

Enable TX flow control to allow TX to transmit the MAC control PAUSE frames to indicate congestion on the receive side of the port interface. Flow control can only be enabled on 1 Gbit/s and 10 Gbit/s ports. Flow control cannot be enabled for ports that run at less than 1 Gbit/s.

Syntax

- `default tx-flow-control`
- `default tx-flow-control enable`
- `default tx-flow-control port {slot/port[-slot/port][,...]}`
- `default tx-flow-control port {slot/port[-slot/port][,...]} enable`
- `no tx-flow-control`
- `no tx-flow-control enable`
- `no tx-flow-control port {slot/port[-slot/port][,...]}`
- `no tx-flow-control port {slot/port[-slot/port][,...]} enable`
- `tx-flow-control`
- `tx-flow-control enable`
- `tx-flow-control port {slot/port[-slot/port][,...]}`
- `tx-flow-control port {slot/port[-slot/port][,...]} enable`

Default

`The default is disable.`

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables the TX flow control on the module.
`port [portlist]`	Specifies the slot and the port number.

©Avaya Inc. 2015 All Rights Reserved.

udp checksum

Enable the User Datagram Protocol (UDP) checksum calculation on the Virtual Services Platform 9000.

Syntax

- `default udp checksum`
- `no udp checksum`
- `udp checksum`

Default

`The default is enabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

udpsrc-by-vip

Enable virtual IP as the UDP source on the Virtual Services Platform 9000.

Syntax

- `default udpsrc-by-vip`
- `no udpsrc-by-vip`
- `udpsrc-by-vip`

Default

`The default is enabled.`

Command mode

Global Configuration

©Avaya Inc. 2015 All Rights Reserved.

untagged-frames-discard

Configure a tagged port to discard all untagged packets so that the frame is not classified into the default VLAN for the port.

Syntax

- `default untagged-frames-discard`
- `default untagged-frames-discard port {slot/port[-slot/port][,...]}`
- `no untagged-frames-discard`
- `no untagged-frames-discard port {slot/port[-slot/port][,...]}`
- `untagged-frames-discard`
- `untagged-frames-discard port {slot/port[-slot/port][,...]}`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`port {slot/port [-slot/port [,...]}`	Specifies the slots and ports that are to be changed.

©Avaya Inc. 2015 All Rights Reserved.

untag-port-default-vlan

Untag the default VLAN on the port.

Syntax

- `default untag-port-default-vlan`
- `default untag-port-default-vlan enable`
- `default untag-port-default-vlan port {slot/port[-slot/port][,...]}`
- `no untag-port-default-vlan`
- `no untag-port-default-vlan enable`
- `no untag-port-default-vlan port {slot/port[-slot/port][,...]}`
- `untag-port-default-vlan`
- `untag-port-default-vlan enable`
- `untag-port-default-vlan port {slot/port[-slot/port][,...]}`

Default

The default is disabled.

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Untags the default VLAN for the port.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

©Avaya Inc. 2015 All Rights Reserved.

usb-stop

Stop the USB access and is done before removing the usb device.

Syntax

- `usb-stop`

Default

None

Command mode

Privileged EXEC

©Avaya Inc. 2015 All Rights Reserved.

vlacp

Configure Virtual Link Aggregation Control Protocol (VLACP) on a port to ensure there is end-to-end reachability.

Syntax

- `default vlacp`
- `default vlacp ethertype`
- `default vlacp fast-periodic-time`
- `default vlacp funcmac-addr`
- `default vlacp slow-periodic-time`
- `default vlacp timeout`
- `default vlacp timeout-scale`
- `no vlacp`
- `vlacp enable`
- `vlacp ethertype <1536-65535 | 0x600-0xffff>`
- `vlacp fast-periodic-time <100-20000>`
- `vlacp funcmac-addr 0x00:0x00:0x00:0x00:0x00:0x00`
- `vlacp slow-periodic-time <10000-30000>`
- `vlacp timeout long`
- `vlacp timeout short`
- `vlacp timeout-scale <2-10>`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`enable`	Enables VLACP for this port.
`ethertype <0X600-0Xffff>`	Sets the VLACP protocol identification for this port.
`fast-periodic-time <100-20000>`	Sets the fast periodic time (in milliseconds) for this port.
`funcmac-addr <0x00:0x00:0x00:0x00:0x00:0x00>`	Sets the multicast MAC address used for the VLACPDU. Specify a MAC address in the format

	0x00:0x00:0x00:0x00:0x00:0x00.
`slow-periodic-time <10000-30000>`	Sets the slow periodic time (in milliseconds) for a specific port type.
`timeout {long|short}`	Sets the port to use the long or short timeout: long sets the port to use the timeout-scale value multiplied by the slow-periodic-time. short sets the port to use the timeout-scale value multiplied by the fast-periodic-time. For example, if you specify a short timeout, set the timeout-scale value to 3, and the fast-periodic-time to 400 ms, the timer will expire within 1000 to 1200 ms. To set this option to the default value, use the default operator with the command.
`timeout-scale <2-10>`	Sets a timeout scale for this port used to calculate the timeout. The default value is 3. To set this option to the default value, use the default operator with the command.

©Avaya Inc. 2015 All Rights Reserved.

vlacp enable

Enable or disable the Virtual Link Aggregation Control Protocol (VLACP) globally to reset all port level settings on the chassis.

Syntax

- `default vlacp enable`
- `no vlacp enable`
- `vlacp enable`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`enable`	Enables the Virtual Link Aggregation Control Protocol (VLACP) globally.

©Avaya Inc. 2015 All Rights Reserved.

vlan action

Perform the general VLAN operations to set a Quality of Service (QoS) level for the VLAN add and to change the name of a VLAN.

Syntax

- `vlan action <1-4084> {none|flushMacFdb|flushArp|flushIp|flushDynMemb|triggerRipUpdate|all}`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`all`	Sets action to all.
`flushArp`	Sets action to flushMacFdb.
`flushDynMemb`	Sets action to flushDynMemb.
`flushIp`	Sets action to flushIp.
`none`	Sets action to none.
`triggerRipUpdate`	Sets action to triggerRipUpdate.

©Avaya Inc. 2015 All Rights Reserved.

vlan agetime

Configure the agetime for dynamic VLAN membership.

Syntax

- `default vlan agetime <2-2084>`
- `vlan agetime <2-2084> <0-1000000>`

Default

`The default is 600 seconds.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`<0-1000000>`	Specifies the agetime, in seconds.
`<2-2084>`	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

vlan create

Configure VLANs to discard tag or untagged frames for a port.

Syntax

- `vlan create <2-4084> [name <WORD 0-64>]type {ipsubnet-mstprstp <0-63> {A.B.C.D/X} [color <0-32>]|port-mstprstp <0-63> [color <0-32>]|protocol-mstprstp <0-63> WORD<0-64>|srcmacmstprstp< 0-63>}`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<2-4084>	Specifies the VLAN ID in the range of 2 to 4084.
name WORD<0-64>	Specifies the VLAN name in the range of 0-64. This parameter is optional. Note Do not use the name Mgmt when you specify a name for the VLAN that you create. The VSP 9000 creates a management VLAN at boot up with the assigned name Mgmt. The show command does not show the management VLAN.
type ipsubnet-mstprstp <0-63> <A.B.C.D/X> [color <0-32]	Creates a VLAN by IP subnet: <0-63> is the STP instance ID in the range of 0-63. A.B.C.D/X is the subnet address or mask {a.b.c.d/x | a.b.c.d/x.x.x.x}. color <0-32> is the color of the VLAN in the range of 0 to 32.
type port-mstprstp <0-63> [color <0-32>]	Creates a VLAN by port: 0-63 is the STP instance ID from 0 to 63. color <0-32> is the color of the VLAN in the range of 0 to 32.
type protocol-mstprstp <0-63> {appleTalk | decLat | decOther | ip | ipv6 | ipx802dot2 | ipx802dot3 | ipxEthernet2 | ipxsnap | netBios | PPPoE | rarp | sna802dot2 | snaEthernet2 | vines | xns} [color <0-32>]	Creates a VLAN by protocol:0-63 is the STP instance ID. appleTalk is the apple talk protocol. decLat is the declat protocol. decOther is the decother protocol. ip is the Ip version 4 protocol. ipv6 is the IP version 6 protocol. ipx802dot2 specifies the Novell Internetwork Packet Exchange (IPX) on IEEE 802.2 frames. ipx802dot3 specifies the Novell Internetwork Packet Exchange (IPX) on Ethernet 802.3 frames. ipxEthernet2 specifies the Novell IPX on Ethernet type 2 frames. ipxsnap specifies the Novell IPX on Ethernet Standard Network Access Protocol (SNAP) frames. netbios is the Netbios protocol. PPPoE is the Point-to-Point Protocol Over Ethernet. rarp is the Rarp protocol. sna802dot2 is the Sna802dot2 protocol. snaethernet2 is the Snaethernet2 protocol. vines is the Vines protocol. xns is the Xns protocol. color <0-32> is the color of the VLAN in the range of 0 to 32.
type protocol-mstprstp <0-63> userDefined {0x0000 | <decimal value>}	Creates a VLAN using a user defined protocol.<0-63> is the STP instance ID in the range of 0-63. {0x0000|<decimal value>} is the protocol ID in

[color] <0-32>] [encap {ethernet-ii | llc | snap}]	hexadecimal or decimal value. color <0-32> is the color of the VLAN in the range of 0 to 32. encap specifies the frame encapsulation header type.
type srcmac-mstprstp <0-63> [color<0-32>]	Creates a VLAN by source MAC address: 0-63 is the STP instance ID in the range of 0-63. color <0-32> is the color of the VLAN in the range of 0 to 32.

©Avaya Inc. 2015 All Rights Reserved.

vlan create <2-4084> type

Create a Shortest Path Bridging MAC (SPBM) backbone VLAN (B-VLAN). You can create a maximum of two B-VLANs.

Syntax

- `vlan create <2-4084> type spbm-bvlan`
- `vlan create <2-4084> type spbm-bvlan color <0-32>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<2-4084>	Specifies the VLAN ID.
color <0-32>	Specifies the color of the VLAN.
spbm-bvlan	Specifies the VLAN type as the backbone VLAN (B-VLAN) for Shortest Path Bridging MAC (SPBM).

©Avaya Inc. 2015 All Rights Reserved.

vlan delete

Delete a VLAN.

Syntax

- `no vlan <2-4084>`
- `vlan delete <2-4084>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<2-4084>	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

vlan i-sid

Map a customer VLAN (C-VLAN) to a service instance identifier to create a Layer 2 VSN. The C-VLAN cannot be a backbone VLAN (B-VLAN). Note: Different from the Ethernet Routing Switch 8800 SPBM implementation, on Virtual Services Platform 9000, when a Layer 2 VSN is in an NNI SMLT, customer VLANs (C-VLANs) that span the two Backbone Edge Bridges (BEBs) must include the interswitch trunking (IST) multilink trunk (MLT) port in their VLANs. An internal implementation difference on Virtual Services Platform 9000 makes this configuration difference visible.

Syntax

- `default vlan i-sid <1-4084>`
- `no vlan i-sid <1-4084>`
- `vlan i-sid <1-4084> <0-16777215>`

Default

`The default I-SID is 0.`

Command mode

Global Configuration

Command parameters

Parameter	Description
<0-16777215>	Specifies the service instance identifier (I-SID). You cannot use I-SID 0x00ffffff. The system reserves this I-SID to advertise the virtual BMAC in an SMLT dual-homing environment.
<1-4084>	Specifies the C-VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

vlan mac-address-entry

Configure the entries in the forwarding database (FDB) to configure or modify the VLAN entries in the FDB.

Syntax

- `vlan mac-address-entry <1-4084> [aging-time <10-1000000>|flush|sync]`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`<1-4084>`	Specifies the VLAN ID in the range of 1 to 4084.
`aging-time <10-1000000>`	Sets the FDB aging timer. seconds indicates the timeout period in seconds.
`flush`	Flushes the FDB.
`sync`	Synchronizes the switch forwarding database with the forwarding database of the other aggregation switch.

©Avaya Inc. 2015 All Rights Reserved.

vlan mac-address-static

Configure the static members of a VLAN to set the VLAN static member parameters.

Syntax

- `vlan mac-address-static <1-4084> <0x00:0x00:0x00:0x00:0x00:0x00> {slot/port[-slot/port][,...]}`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Specifies the slot and the port number.
`<0x00:0x00:0x00:0x00:0x00:0x00>`	Adds a static member to a VLAN bridge:
`<1-4084>`	Specifies the VLAN ID in the range of 1 to 4084.

©Avaya Inc. 2015 All Rights Reserved.

vlan members

Add or remove the ports in a VLAN to configure the ports in the VLAN.

Syntax

- `vlan members add <1-4084> {slot/port[-slot/port][,...]} [portmember|static|notallowed]`
- `vlan members remove <1-4084> {slot/port[-slot/port][,...]} [portmember|static|notallowed]`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`{slot/port [-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-4084>`	Specifies the VLAN ID.
`notallowed`	Selects the port type to not-allowed.
`portmember`	Select the port type to port member.
`static`	Selects the port type to static.

©Avaya Inc. 2015 All Rights Reserved.

vlan mlt

Add an MLT to a VLAN.

Syntax

- `vlan mlt <1-4084> <1-512>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-4084>	Specifies the VLAN ID.
<1-512>	Specifies the MLT ID.

©Avaya Inc. 2015 All Rights Reserved.

vlan nodal-mep

Add nodal Maintenance Endpoints (MEPs) to the VLAN. The Nodal B-VLAN MEPs created on the CP and function as if they are connected to the virtual interface of the given B-VLAN. Because of this they are supported for both port and MLT based B-VLANs. To support this behavior a MAC entry is added to the forwarding database (FDB) and a new CFM data path table containing the B-VLAN and MP level are added to direct CFM frames to the CP as required.

Syntax

- `no vlan nodal-mep <1-4084> WORD<0-22> WORD<0-22> <1-8191>`
- `vlan nodal-mep <1-4084> WORD<0-22> WORD<0-22> <1-8191>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-4084>	Specifies the VLAN ID.
<1-8191>	Specifies the nodal Maintenance Endpoints (MEPs) to add to the VLAN.
WORD<0-22> WORD<0-22>	The first parameter, specifies the Maintenance-Domain (MD) name. The second parameter, specifies the Maintenance-Association (MA) name.

©Avaya Inc. 2015 All Rights Reserved.

vlan nodal-mip-level

Add a nodal Maintenance Intermediate Point level to the VLAN. The Nodal MIP is associated with a B-VLAN. VLAN and level are sufficient to specify the Nodal MIP entity. The Nodal MIP MAC address is the SPBM system ID for the node on which it resides. If the fastpath sends a message to the CP, the MIP responds if it is not the target and the MEP responds if it is the target.

Syntax

- `no vlan nodal-mip-level <1-4084> WORD<0-15>`
- `vlan nodal-mip-level <1-4084> WORD<0-15>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<1-4084>	Specifies the VLAN ID.
WORD<0-15>	Adds the nodal Maintenance Intermediate Point (MIP) level.

©Avaya Inc. 2015 All Rights Reserved.

vlan ports ospf-passive

Specifies which ports in the VLAN are passive. Use this command to form neighbor adjacencies on some ports of a VLAN while other ports on the same VLAN remain passive. If you do not use this command to make a port within the VLAN an OSPF passive port, all ports on the VLAN can form a neighbor adjacency.

Syntax

- `default vlan ports ospf-passive <1–4084> {slot/port[-slot/port] [,...]}`
- `no vlan ports ospf-passive <1–4084> {slot/port[-slot/port] [,...]}`
- `vlan ports ospf-passive <1–4084> {slot/port[-slot/port] [,...]}`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`{slot/port[-slot/port] [,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1–4084>`	Specifies the VLAN ID.

©Avaya Inc. 2015 All Rights Reserved.

vlan srcmac

Add or remove a VLAN source MAC addresses to configure the source MAC address to a VLAN.

Syntax

- `default vlan srcmac <2-4084> <0x00:0x00:0x00:0x00:0x00:0x00>`
- `no vlan srcmac <2-4084> <0x00:0x00:0x00:0x00:0x00:0x00>`
- `vlan srcmac <2-4084> <0x00:0x00:0x00:0x00:0x00:0x00>`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
<0x00:0x00:0x00:0x00:0x00:0x00>	Specifies the source MAC address.
<2-4084>	Specifies the VLAN ID in the range of 2-4084.

©Avaya Inc. 2015 All Rights Reserved.

vlan static-mcastmac

Add VLAN static multicast MAC entries.

Syntax

- `default vlan static-mcastmac <1-4084> [0x00:0x00:0x00:0x00:0x00:0x00]`
- `default vlan static-mcastmac <1-4084> [mlt <1-256>]`
- `default vlan static-mcastmac <1-4084> ports{slot/port[-slot/port][,...]} [0x00:0x00:0x00:0x00:0x00:0x00]`
- `no vlan static-mcastmac <1-4084> 0x00:0x00:0x00:0x00:0x00:0x00`
- `no vlan static-mcastmac <1-4084> ports {slot/port[-slot/port][,...]} [0x00:0x00:0x00:0x00:0x00:0x00]`
- `vlan static-mcastmac <1-4084> ports {slot/port[-slot/port][,...]} [0x00:0x00:0x00:0x00:0x00:0x00]`
- `vlan static-mcastmac <1-4084>[0x00:0x00:0x00:0x00:0x00:0x00][mlt <1-256>]`

Default

None

Command mode

Global Configuration

Command parameters

Parameter	Description
`{slot/port[-slot/port][,...]}`	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`<1-256>`	Specifies the MLT ID.
`<1-4084>`	Specifies the VLAN ID.
`0x00:0x00:0x00:0x00:0x00:0x00`	Specifies the MAC address.

©Avaya Inc. 2015 All Rights Reserved.

vrf (for a port)

Associate a port to a Virtual Router Forwarding (VRF) so that the port becomes a member of the VRF instance.

Syntax

- `no vrf`
- `vrf WORD<1-16>`

Default

None

Command mode

GigabitEthernet Interface Configuration

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies the VRF name.

©Avaya Inc. 2015 All Rights Reserved.

vrf (for a VLAN)

Associate a VLAN to a Virtual Router Forwarding (VRF) so that the VLAN becomes a member of the VRF instance.

Syntax

- `no vrf`
- `vrf WORD<1-16>`

Default

None

Command mode

VLAN Interface Configuration

Command parameters

Parameter	Description
`vrf WORD<1-16>`	Specifies the VRF name.

©Avaya Inc. 2015 All Rights Reserved.

vsptalk

Create VSP Talk application.

Syntax

- `no vsptalk`
- `no vsptalk { gtalk | avaya }`
- `vsptalk`
- `vsptalk { gtalk | avaya }`

Default

`The default is disabled.`

Command mode

Application Configuration

Command parameters

Parameter	Description
`vsptalk { gtalk | avaya }`	Enables one of the instant messaging client types on Virtual Services Platform 9000. VSP 9000 supports the following: avaya - Avaya XMPP IM or gtalk - Google Talk. VSP Talk can use only one client type at a time. You cannot use more than one client type simultaneously.

©Avaya Inc. 2015 All Rights Reserved.

vsptalk { gtalk | avaya } client add-buddy

Add your contact email to become a contact to receive and send messages through Instant Messaging.

Syntax

- `no vsptalk { gtalk | avaya } client add-buddy`
- `no vsptalk { gtalk | avaya } client add-buddy WORD<0-1024>`
- `vsptalk { gtalk | avaya } client add-buddy WORD<0-1024>`

Default

None

Command mode

Application Configuration

Command parameters

Parameter	Description
`{ gtalk | avaya }`	Enables one of the instant messaging client types on Virtual Services Platform 9000. VSP 9000 supports the following: avaya - Avaya XMPP IM or gtalk - Google Talk. VSP Talk can use only one client type at a time. You cannot use more than one client type simultaneously.
`WORD<0-200>`	Adds your contact email to become a contact to receive and send messages through instant messaging. WORD<0-200> specifies your email address for the IM client. For instance, if you use Google Talk as the VSP Talk IM client your address is a gmail address: administrator1@gmail.com. The maximum number of contacts is 12.

©Avaya Inc. 2015 All Rights Reserved.

vsptalk { gtalk | avaya } client username

Define the VSP Talk instant messaging client username and password.

Syntax

- `no vsptalk { gtalk | avaya } client username`
- `vsptalk { gtalk | avaya } client username WORD<0-64>`
- `vsptalk { gtalk | avaya } client username WORD<0-64> password WORD<0-80>`

Default

None

Command mode

Application Configuration

Command parameters

Parameter	Description
`{ gtalk | avaya }`	Enables one of the instant messaging client types on Virtual Services Platform 9000. VSP 9000 supports the following: avaya - Avaya XMPP IM or gtalk - Google Talk. VSP Talk can use only one client type at a time. You cannot use more than one client type simultaneously.
`password WORD<0-80>`	Defines the VSP Talk instant messaging client password. WORD<0-80> specifies the password.
`username WORD<0-64>`	Defines the VSP Talk instant messaging client username. WORD<0-64> specifies the username. The username for Virtual Services Platform 9000 is the email used for Virtual Services Platform 9000 in the IM client.

©Avaya Inc. 2015 All Rights Reserved.

vsptalk { gtalk | avaya } enable

Enable the VSP Talk application.

Syntax

- `default vsptalk { gtalk | avaya } enable`
- `no vsptalk { gtalk | avaya } enable`
- `vsptalk { gtalk | avaya } enable`

Default

`The default is disabled.`

Command mode

Application Configuration

Command parameters

Parameter	Description
`{ gtalk | avaya }`	Enables one of the instant messaging client types on Virtual Services Platform 9000. VSP 9000 supports the following: avaya - Avaya XMPP IM or gtalk - Google Talk. VSP Talk can use only one client type at a time. You cannot use more than one client type simultaneously.

©Avaya Inc. 2015 All Rights Reserved.

vsptalk { gtalk | avaya } server address

Specify the instant messaging server address.

Syntax

- `no vsptalk { gtalk | avaya } server address`
- `vsptalk { gtalk | avaya } server address WORD<0-255>`

Default

None

Command mode

Application Configuration

Command parameters

Parameter	Description
`{ gtalk | avaya }`	Enables one of the instant messaging client types on Virtual Services Platform 9000. VSP 9000 supports the following: avaya - Avaya XMPP IM or gtalk - Google Talk. VSP Talk can use only one client type at a time. You cannot use more than one client type simultaneously.
`address <0-255>`	Specifies the instant messaging server address.

©Avaya Inc. 2015 All Rights Reserved.

vsptalk { gtalk | avaya } server encryption

Configure encryption on the server.

Syntax

- `default vsptalk { gtalk | avaya } server encryption`
- `vsptalk { gtalk | avaya } server encryption as-requested`
- `vsptalk { gtalk | avaya } server encryption required`

Default

`The default is required.`

Command mode

Application Configuration

Command parameters

Parameter	Description
`{ gtalk | avaya }`	Enables one of the instant messaging client types on Virtual Services Platform 9000. VSP 9000 supports the following: avaya - Avaya XMPP IM or gtalk - Google Talk. VSP Talk can use only one client type at a time. You cannot use more than one client type simultaneously.
`encryption <as-requested|required>`	Specifies the encryption option.

©Avaya Inc. 2015 All Rights Reserved.

vsptalk { gtalk | avaya } server port

Configure encryption on the server.

Syntax

- `default vsptalk { gtalk | avaya } server port`
- `vsptalk { gtalk | avaya } server port <0-49151>`

Default

`The default port for avaya and gtalk is 5222.`

Command mode

Application Configuration

Command parameters

Parameter	Description
`{ gtalk | avaya }`	Enables one of the instant messaging client types on Virtual Services Platform 9000. VSP 9000 supports the following: avaya - Avaya XMPP IM or gtalk - Google Talk. VSP Talk can use only one client type at a time. You cannot use more than one client type simultaneously.
`port <1-49151>`	Specifies the TCP port for instant messaging.

©Avaya Inc. 2015 All Rights Reserved.

vsptalk { gtalk | avaya } server proxy

Enable or disables the boundary-router on the router interface.

Syntax

- `no vsptalk { gtalk | avaya } server proxy`
- `vsptalk { gtalk | avaya } server proxy WORD<0-255>`

Default

`The default is disabled.`

Command mode

Application Configuration

Command parameters

Parameter	Description
`{ gtalk | avaya }`	Enables one of the instant messaging client types on Virtual Services Platform 9000. VSP 9000 supports the following: avaya - Avaya XMPP IM or gtalk - Google Talk. VSP Talk can use only one client type at a time. You cannot use more than one client type simultaneously.
`WORD<0-255>`	Configures a server proxy to access the Internet from the network. Note Currently only HTTP proxy is supported for the proxy operator. You cannot use HTTPS with the proxy operator.

©Avaya Inc. 2015 All Rights Reserved.

vsptalk { gtalk | avaya } server ssltype

Enable, restore to default, or disable the old-style Secure Sockets Layer (SSL) interface.

Syntax

- `default vsptalk { gtalk | avaya } server ssltype`
- `no vsptalk { gtalk | avaya } server ssltype old`
- `vsptalk { gtalk | avaya } server ssltype old`

Default

`The default is disabled.`

Command mode

Application Configuration

Command parameters

Parameter	Description
`{ gtalk | avaya }`	Enables one of the instant messaging client types on Virtual Services Platform 9000. VSP 9000 supports the following: avaya - Avaya XMPP IM or gtalk - Google Talk. VSP Talk can use only one client type at a time. You cannot use more than one client type simultaneously.
`old`	Enables the old-style Secure Socket Layer interface. SSL is a protocol used to encrypt and transmit private documents over the Internet. DEFAULT: disabled Note The system supports only HTTP proxy for the proxy operator. You cannot use HTTPS with the proxy operator.

©Avaya Inc. 2015 All Rights Reserved.

vsptalk endpoint-address

Assign a VSP Talk endpoint address.

Syntax

- `no vsptalk endpoint-address`
- `vsptalk endpoint-address {A.B.C.D}`
- `vsptalk endpoint-address {A.B.C.D} vrf WORD<1-16>`

Default

None

Command mode

Application Configuration

Command parameters

Parameter	Description
{A.B.C.D}	Assigns an address for the VSP Talk application to use for communication. Virtual Services Platform 9000 supports IPv4 addresses for the VSP Talk feature. To insulate mission critical applications, assign an address within your network that is separate from mission critical applications and other features.
vrf WORD<1-16>	Specifies the name of the virtual router for which the endpoint address belongs. This is an optional parameter. Note: If you configure the VSP Talk endpoint address under an IP address for a VLAN or brouter, you must first remove the VSP Talk endpoint address before you can remove the IP address for the VLAN or brouter.

©Avaya Inc. 2015 All Rights Reserved.

vsptalk event-notification enable

Configure the IPv6 address for the Ethernet management port.

Syntax

- `default vsptalk event-notification`
- `no vsptalk event-notification enable`
- `vsptalk event-notification enable`

Default

`The default is disabled.`

Command mode

Application Configuration

Command parameters

Parameter	Description
`event-notification enable`	Enables event notification to receive instant messages on status updates or to allow Virtual Services Platform 9000 to notify you about alarm conditions. Note: In IM chat, you must also use the command enable event-notification.

©Avaya Inc. 2015 All Rights Reserved.

web-server

Enable the web management interface to provide management access to the switch using a web browser. Configure the location of the Help files for the web interface.

Syntax

- `default web-server`
- `default web-server def-display-rows`
- `default web-server enable`
- `default web-server http-port`
- `default web-server https-port`
- `default web-server secure-only`
- `no web-server enable`
- `no web-server secure-only`
- `web-server def-display-rows <10-100>`
- `web-server enable`
- `web-server help-tftp WORD<0-256>`
- `web-server http-port <80-49151>`
- `web-server https-port <443-49151>`
- `web-server password ro WORD<1-20> WORD<1-20>`
- `web-server password rw WORD<1-20> WORD<1-20>`
- `web-server password rwa WORD<1-20> WORD<1-20>`
- `web-server secure-only`

Default

`The web server is disabled by default.`

Command mode

Global Configuration

Command parameters

Parameter	Description
`def-display-rows <10-100>`	Configures the web server default display row width. The default is 30.

`enable`	Enables the web interface. You must enable the web interface before you can connect to the system using Enterprise Device Manager (EDM).
`help-tftp WORD<0-256>`	Specifies the path to the location that stores the HTML Help files for the web server. WORD<0-256> is a string of 0-256 characters. You can store the HTML Help files on a TFTP server, internal flash, external flash, or USB device. Specify the file name in one of the following formats: a.b.c.d:/<directory>, /intflash/<directory>, /extflash/<directory>, or /usb/<directory> . For example, 47.17.82.25:/VSP9000_help or /extflash/help_files/vsp9000 are acceptable.
`http-port <80-49151>`	Configures the web server HTTP port. The default is 80. To select another port for HTTP, you can discover the ports that TCP already use. Use the show ip tcp connections command to list the ports already in use, and then select a port that does not appear in the command output.
`https-port <443-49151>`	Specifies the HTTPS port of the web server. You can select a value of 443 or 1024 to 49151. The default is 443. To select another port for HTTPS, you can discover the ports that TCP already use. Use the show ip tcp connections command to list the ports already in use, and then select a port that does not appear in the command output.
`password {ro|rw|rwa} WORD<1-20> WORD<1-20>`	Specifies the username and the password for the access level. The access level can be read-only, read-write access, or read-write-all.
`secure-only`	Enables secure-only access to the web server. The default value for the secure-only option is enabled. By default the web server is configured with the secure-only option, which requires you to use https to access EDM. To access EDM using http, you must disable the secure-only option, by using: no web-server secure-only. The default is enabled.

©Avaya Inc. 2015 All Rights Reserved.