|  |
| --- |
|  |
| HPE 5130EI-CMW710-R3507P10  Release Notes |
| Software Feature Changes |
|  |
|  |
| The information in this document is subject to change without notice.  © Copyright 2015, 2023 Hewlett Packard Enterprise Development LP |

Contents

[Release 3507P10 1](#_Toc129617206)

[Release 3507P09 2](#_Toc129617207)

[Release 3507P02 3](#_Toc129617208)

[Release 3507 4](#_Toc129617209)

[Modified feature: EAD assistant 4](#_Toc129617210)

[Feature change description 4](#_Toc129617211)

[Command changes 4](#_Toc129617212)

[Release 3506P10 5](#_Toc129617213)

[New feature: Configuring the 802.1p priority for control packets sent by a device 5](#_Toc129617214)

[Configuring the 802.1p priority for control packets sent by a device 5](#_Toc129617215)

[Command reference 5](#_Toc129617216)

[control-packet dot1p 5](#_Toc129617217)

[New feature: Packet spoofing logging and filtering entry logging for SAVI 6](#_Toc129617218)

[Enabling packet spoofing logging and filtering entry logging 6](#_Toc129617219)

[Command reference 7](#_Toc129617220)

[ipv6 savi log enable 7](#_Toc129617221)

[New feature: Configuring password control over weak passwords 8](#_Toc129617222)

[Configuring password control over weak passwords 8](#_Toc129617223)

[Command reference 8](#_Toc129617224)

[New command: password-control change-password weak-password enable 8](#_Toc129617225)

[Modified command: display password-control 9](#_Toc129617226)

[Modified command: password-control complexity 9](#_Toc129617227)

[Modified command: password-control composition 10](#_Toc129617228)

[Modified command: password-control super composition 11](#_Toc129617229)

[Modified command: set authentication password 11](#_Toc129617230)

[New feature: Enabling password change prompt logging 11](#_Toc129617231)

[Enabling password change prompt logging 11](#_Toc129617232)

[Command reference 12](#_Toc129617233)

[local-server log change-password-prompt 12](#_Toc129617234)

[Release 3506P08 14](#_Toc129617235)

[Release 3506P06 15](#_Toc129617236)

[New feature: Enabling recording untrusted DHCP servers on a DHCP snooping device 15](#_Toc129617237)

[Enabling recording untrusted DHCP servers on a DHCP snooping device 15](#_Toc129617238)

[Command reference 15](#_Toc129617239)

[dhcp snooping untrusted-server-record enable 15](#_Toc129617240)

[Modified feature: Factory defaults change for console login and password control settings 16](#_Toc129617241)

[Feature change description 16](#_Toc129617242)

[Command changes 17](#_Toc129617243)

[Release 3506P02 1](#_Toc129617244)

[Release 3506 1](#_Toc129617245)

[New feature: Enabling recording user IP address conflicts 2](#_Toc129617246)

[Enabling recording user IP address conflicts 2](#_Toc129617247)

[Command reference 2](#_Toc129617248)

[arp user-ip-conflict record enable 2](#_Toc129617249)

[display arp user-ip-conflict record 3](#_Toc129617250)

[New feature: LDRA on the DHCPv6 snooping device 5](#_Toc129617251)

[Enabling LDRA on the DHCPv6 snooping device 5](#_Toc129617252)

[About LDRA on the DHCPv6 snooping device 5](#_Toc129617253)

[Procedure 5](#_Toc129617254)

[Command reference 5](#_Toc129617255)

[ipv6 dhcp snooping relay-agent enable 5](#_Toc129617256)

[New feature: Enabling link flapping protection on an interface 6](#_Toc129617257)

[Enabling link flapping protection on an interface 6](#_Toc129617258)

[About link flapping protection 6](#_Toc129617259)

[Restrictions and guidelines 6](#_Toc129617260)

[Procedure 7](#_Toc129617261)

[Command reference 7](#_Toc129617262)

[display link-flap protection 7](#_Toc129617263)

[link-flap protect enable 8](#_Toc129617264)

[port link-flap protect enable 9](#_Toc129617265)

[New feature: Controlling the status of guest VLAN reauthentication in MAC authentication 10](#_Toc129617266)

[Enabling guest VLAN reauthentication in MAC authentication 10](#_Toc129617267)

[Overview 10](#_Toc129617268)

[Configuration procedure 10](#_Toc129617269)

[Command reference 11](#_Toc129617270)

[mac-authentication guest-vlan re-authenticate 11](#_Toc129617271)

[New feature: Specifying the Telnet service port number 12](#_Toc129617272)

[Specifying the Telnet service port number 12](#_Toc129617273)

[About specifying the Telnet service port number 12](#_Toc129617274)

[Procedure 12](#_Toc129617275)

[Command reference 12](#_Toc129617276)

[telnet server ipv6 port 12](#_Toc129617277)

[telnet server port 13](#_Toc129617278)

[New feature: Enabling the DHCPv6 relay agent to support Option 79 13](#_Toc129617279)

[Enabling the DHCPv6 relay agent to support Option 79 13](#_Toc129617280)

[Command reference 14](#_Toc129617281)

[ipv6 dhcp relay client-link-address enable 14](#_Toc129617282)

[New feature:Enable recording DHCPv6 snooping prefix entries 14](#_Toc129617283)

[Enable recording DHCPv6 snooping prefix entries 14](#_Toc129617284)

[Command reference 15](#_Toc129617285)

[ipv6 dhcp snooping pd binding record 15](#_Toc129617286)

[display ipv6 dhcp snooping pd binding 16](#_Toc129617287)

[reset ipv6 dhcp snooping pd binding 17](#_Toc129617288)

[New feature: Configuring resource monitoring 17](#_Toc129617289)

[Command reference 19](#_Toc129617290)

[resource-monitor minor resend enable 19](#_Toc129617291)

[resource-monitor output 19](#_Toc129617292)

[resource-monitor resource 20](#_Toc129617293)

[display resource-monitor 22](#_Toc129617294)

[New feature: Archiving configuration to a remote SCP server 23](#_Toc129617295)

[Configuring remote configuration archiving 23](#_Toc129617296)

[Command reference 24](#_Toc129617297)

[archive configuration server 24](#_Toc129617298)

[archive configuration server password 25](#_Toc129617299)

[archive configuration server user 26](#_Toc129617300)

[New feature: Setting the DSCP value for SNMP responses 27](#_Toc129617301)

[Setting the DSCP value for SNMP responses 27](#_Toc129617302)

[Command reference 27](#_Toc129617303)

[snmp-agent packet response dscp 27](#_Toc129617304)

[New feature: Specifying the NTP time-offset thresholds for log and trap outputs 28](#_Toc129617305)

[Specifying the NTP time-offset thresholds for log and trap outputs 28](#_Toc129617306)

[Command reference 28](#_Toc129617307)

[ntp-service time-offset-threshold 28](#_Toc129617308)

[New feature: Specifying the SNTP time-offset thresholds for log and trap outputs 29](#_Toc129617309)

[Specifying the SNTP time-offset thresholds for log and trap outputs 29](#_Toc129617310)

[Command reference 29](#_Toc129617311)

[sntp time-offset-threshold 29](#_Toc129617312)

[New feature: Configuring Link-up delay timer 30](#_Toc129617313)

[Configuring Link-up delay timer 30](#_Toc129617314)

[Command reference 31](#_Toc129617315)

[linkup-delay-timer 31](#_Toc129617316)

[New feature: Configuring an EAP profile 32](#_Toc129617317)

[Configuring an EAP profile 32](#_Toc129617318)

[Command reference 33](#_Toc129617319)

[eap-profile 33](#_Toc129617320)

[ca-file 33](#_Toc129617321)

[method 34](#_Toc129617322)

[New feature: Configuring 802.1X unauthenticated user aging 35](#_Toc129617323)

[Configuring 802.1X unauthenticated user aging 35](#_Toc129617324)

[Command reference 36](#_Toc129617325)

[dot1x unauthenticated-user aging enable 36](#_Toc129617326)

[dot1x timer user-aging 37](#_Toc129617327)

[New feature: Configuring MAC authentication unauthenticated user aging 38](#_Toc129617328)

[Configuring user aging for unauthenticated MAC authentication users 38](#_Toc129617329)

[Command reference 38](#_Toc129617330)

[mac-authentication unauthenticated-user aging enable 38](#_Toc129617331)

[mac-authentication timer user-aging 39](#_Toc129617332)

[New feature: VLAN check bypass for the port security MAC move feature 40](#_Toc129617333)

[Enabling VLAN check bypass for the port security MAC move feature 40](#_Toc129617334)

[Command reference 41](#_Toc129617335)

[port-security mac-move bypass-vlan-check 41](#_Toc129617336)

[New feature: Strict intrusion protection 42](#_Toc129617337)

[Configuring strict intrusion protection 42](#_Toc129617338)

[Command reference 42](#_Toc129617339)

[port-security strict-intrusion-protection enable 42](#_Toc129617340)

[New feature: Specifying the source IP address for outgoing SCP packets 43](#_Toc129617341)

[Specifying the source IP address for outgoing SCP packets 43](#_Toc129617342)

[Command reference 44](#_Toc129617343)

[scp client ipv6 source 44](#_Toc129617344)

[scp client source 44](#_Toc129617345)

[New feature: gRPC 45](#_Toc129617346)

[About gRPC 45](#_Toc129617347)

[gRPC protocol stack layers 45](#_Toc129617348)

[Network architecture 46](#_Toc129617349)

[Telemetry technology based on gRPC 46](#_Toc129617350)

[Telemetry modes 46](#_Toc129617351)

[Protocols 47](#_Toc129617352)

[FIPS compliance 47](#_Toc129617353)

[Configuring the gRPC dial-in mode 47](#_Toc129617354)

[gRPC dial-in mode configuration tasks at a glance 47](#_Toc129617355)

[Configuring the gRPC service 47](#_Toc129617356)

[Configuring a gRPC user 48](#_Toc129617357)

[Configuring the gRPC dial-out mode 48](#_Toc129617358)

[gRPC dial-out mode configuration tasks at a glance 48](#_Toc129617359)

[Enabling the gRPC service 48](#_Toc129617360)

[Configuring sensors 48](#_Toc129617361)

[Configuring collectors 49](#_Toc129617362)

[Configuring a subscription 50](#_Toc129617363)

[Display and maintenance commands for gRPC 50](#_Toc129617364)

[gRPC configuration examples 50](#_Toc129617365)

[Example: Configuring the gRPC dial-in mode 51](#_Toc129617366)

[Example: Configuring the gRPC dial-out mode 51](#_Toc129617367)

[gRPC dial-in mode commands 52](#_Toc129617368)

[display grpc 52](#_Toc129617369)

[grpc enable 53](#_Toc129617370)

[grpc idle-timeout 54](#_Toc129617371)

[grpc port 54](#_Toc129617372)

[gRPC dial-out mode commands 55](#_Toc129617373)

[destination-group (subscription view) 55](#_Toc129617374)

[destination-group (telemetry view) 56](#_Toc129617375)

[ipv4-address 57](#_Toc129617376)

[ipv6-address 57](#_Toc129617377)

[sensor path 58](#_Toc129617378)

[sensor-group (subscription view) 59](#_Toc129617379)

[sensor-group (telemetry view) 60](#_Toc129617380)

[source-address 60](#_Toc129617381)

[subscription 61](#_Toc129617382)

[telemetry 62](#_Toc129617383)

[Modified feature: Specifying the HTTPS redirect listening port number 62](#_Toc129617384)

[Feature change description 62](#_Toc129617385)

[Command changes 62](#_Toc129617386)

[Modified command: http-redirect https-port 62](#_Toc129617387)

[Modified feature: Specifying startup images 63](#_Toc129617388)

[Feature change description 63](#_Toc129617389)

[Command changes 63](#_Toc129617390)

[Modified command: boot-loader file 63](#_Toc129617391)

[Modified feature: Automatic configuration 63](#_Toc129617392)

[Feature change description 63](#_Toc129617393)

[Command changes 63](#_Toc129617394)

[Modified feature: Displaying ARP snooping entries 64](#_Toc129617395)

[Feature change description 64](#_Toc129617396)

[Command changes 64](#_Toc129617397)

[Modified command: display arp snooping 64](#_Toc129617398)

[Modified feature: Clearing ARP snooping entries 64](#_Toc129617399)

[Feature change description 64](#_Toc129617400)

[Command changes 64](#_Toc129617401)

[Modified command: reset arp snooping 64](#_Toc129617402)

[Modified feature: Setting the DHCP server response timeout time for DHCP server switchover 65](#_Toc129617403)

[Feature change description 65](#_Toc129617404)

[Command changes 65](#_Toc129617405)

[Modified command: dhcp relay dhcp-server timeout 65](#_Toc129617406)

[Modified command: dhcp-server timeout 65](#_Toc129617407)

[Modified feature: Automatic configuration 66](#_Toc129617408)

[Feature change description 66](#_Toc129617409)

[Command changes 66](#_Toc129617410)

[Modified feature: Physical type of a combo interface 66](#_Toc129617411)

[Feature change description 66](#_Toc129617412)

[Command changes 66](#_Toc129617413)

[Modified command: combo enable 66](#_Toc129617414)

[Modified feature: Physical state change suppression 67](#_Toc129617415)

[Feature change description 67](#_Toc129617416)

[Command changes 67](#_Toc129617417)

[Modified command: link-delay 67](#_Toc129617418)

[Modified feature: MAC-to-VLAN entries 68](#_Toc129617419)

[Feature change description 68](#_Toc129617420)

[Command changes 68](#_Toc129617421)

[Modified command: mac-vlan mac-address 68](#_Toc129617422)

[Modified command: display mac-vlan 69](#_Toc129617423)

[Modified feature: Displaying the loop detection configuration and status 69](#_Toc129617424)

[Feature change description 69](#_Toc129617425)

[Command changes 69](#_Toc129617426)

[Modified command: display loopback-detection 69](#_Toc129617427)

[Modified feature: Setting the 802.1p priority for IGMP messages 70](#_Toc129617428)

[Feature change description 70](#_Toc129617429)

[Command changes 70](#_Toc129617430)

[Modified command: dot1p-priority 70](#_Toc129617431)

[Modified command: igmp-snooping dot1p-priority 71](#_Toc129617432)

[Modified feature: Setting the 802.1p priority for MLD messages 71](#_Toc129617433)

[Feature change description 71](#_Toc129617434)

[Command changes 71](#_Toc129617435)

[Modified command: dot1p-priority 71](#_Toc129617436)

[Modified command: mld-snooping dot1p-priority 71](#_Toc129617437)

[Modified feature: Displaying IPv4SG bindings 72](#_Toc129617438)

[Feature change description 72](#_Toc129617439)

[Command changes 72](#_Toc129617440)

[Modified command: display ip source binding 72](#_Toc129617441)

[Modified feature: Displaying IPv6SG bindings 72](#_Toc129617442)

[Feature change description 72](#_Toc129617443)

[Command changes 72](#_Toc129617444)

[Modified command: display ipv6 source binding 72](#_Toc129617445)

[Modified feature: Displaying the MFF configuration for a VLAN 73](#_Toc129617446)

[Feature change description 73](#_Toc129617447)

[Command changes 73](#_Toc129617448)

[Modified command: display mac-forced-forwarding vlan 73](#_Toc129617449)

[Modified feature: Associating Track with application modules 74](#_Toc129617450)

[Feature change description 74](#_Toc129617451)

[Command changes 74](#_Toc129617452)

[Modified command: track bfd ctrl 74](#_Toc129617453)

[Modified command: track bfd echo 75](#_Toc129617454)

[Modified command: track cfd 75](#_Toc129617455)

[Modified command: track interface 75](#_Toc129617456)

[Modified command: track interface physical 76](#_Toc129617457)

[Modified command: track interface protocol 76](#_Toc129617458)

[Modified command: track ip route reachability 76](#_Toc129617459)

[Modified command: track lldp neighbor 77](#_Toc129617460)

[Modified command: track nqa 77](#_Toc129617461)

[Modified feature: Configuring binding attributes for local users 77](#_Toc129617462)

[Feature change description 77](#_Toc129617463)

[Command changes 78](#_Toc129617464)

[Modified command: bind-attribute 78](#_Toc129617465)

[Modified feature: Enabling password control 78](#_Toc129617466)

[Feature change description 78](#_Toc129617467)

[Command changes 78](#_Toc129617468)

[Modified command: password-control enable 78](#_Toc129617469)

[Modified feature: Password management after global password control is enabled 79](#_Toc129617470)

[Feature change description 79](#_Toc129617471)

[Managing local user passwords for device management users 79](#_Toc129617472)

[Managing super passwords 79](#_Toc129617473)

[Command changes 80](#_Toc129617474)

[Modified feature: Setting the quiet timer for RADIUS servers in a RADIUS scheme 80](#_Toc129617475)

[Feature change description 80](#_Toc129617476)

[Command changes 80](#_Toc129617477)

[Modified command: timer quiet (RADIUS scheme view) 80](#_Toc129617478)

[Modified feature: MAC-based MAC authentication user accounts for MAC authentication 80](#_Toc129617479)

[Feature change description 80](#_Toc129617480)

[Command changes 80](#_Toc129617481)

[Modified command: mac-authentication user-name-format 80](#_Toc129617482)

[Modified feature: MAC authentication VLAN mode 81](#_Toc129617483)

[Feature change description 81](#_Toc129617484)

[Modified feature: Web authentication 81](#_Toc129617485)

[Modified feature: Port security NTK feature 82](#_Toc129617486)

[Feature change description 82](#_Toc129617487)

[Command changes 82](#_Toc129617488)

[Modified command: port-security ntk-mode 82](#_Toc129617489)

[Modified feature: Port security MAC move 82](#_Toc129617490)

[Feature change description 82](#_Toc129617491)

[Modified feature: RSA key modulus length used for creating an RSA key pair 83](#_Toc129617492)

[Feature change description 83](#_Toc129617493)

[Command changes 83](#_Toc129617494)

[Modified command: public-key local create 83](#_Toc129617495)

[Modified feature: RSA key modulus length used for PKI certificate request 83](#_Toc129617496)

[Feature change description 83](#_Toc129617497)

[Command changes 84](#_Toc129617498)

[Modified command: public-key rsa 84](#_Toc129617499)

[Modified feature: SNMP notifications for IKE 84](#_Toc129617500)

[Feature change description 84](#_Toc129617501)

[Command changes 84](#_Toc129617502)

[Modified command: snmp-agent trap enable ike 84](#_Toc129617503)

[Modified feature: Configuring an SNMP notification target host 85](#_Toc129617504)

[Feature change description 85](#_Toc129617505)

[Command changes 85](#_Toc129617506)

[Modified command: snmp-agent target-host 85](#_Toc129617507)

[Modified feature: Displaying logs buffered over the last specified period of time 86](#_Toc129617508)

[Feature change description 86](#_Toc129617509)

[Command changes 86](#_Toc129617510)

[Modified command: display logbuffer 86](#_Toc129617511)

[Modified feature: Specifying a log host and its output parameters 87](#_Toc129617512)

[Feature change description 87](#_Toc129617513)

[Command changes 87](#_Toc129617514)

[Modified command: info-center loghost 87](#_Toc129617515)

[Modified command: info-center timestamp loghost 88](#_Toc129617516)

[Modified feature: Interface event 88](#_Toc129617517)

[Feature change description 88](#_Toc129617518)

[Command changes 88](#_Toc129617519)

[Modified command: event interface 88](#_Toc129617520)

[Modified feature: NTP 89](#_Toc129617521)

[Feature change description 89](#_Toc129617522)

[Command changes 89](#_Toc129617523)

[Modified command: display ntp-service status 89](#_Toc129617524)

[Modified command: ntp-service unicast-peer 89](#_Toc129617525)

[Modified command: ntp-service unicast-server 90](#_Toc129617526)

[Modified command: ntp-service ipv6 unicast-peer 90](#_Toc129617527)

[Modified command: ntp-service ipv6 unicast-server 90](#_Toc129617528)

[Modified feature: Specifying the source IP address for NTP messages 91](#_Toc129617529)

[Feature change description 91](#_Toc129617530)

[Command changes 91](#_Toc129617531)

[Modified command: ntp-service source 91](#_Toc129617532)

[Modified feature: sFlow counter sampling 91](#_Toc129617533)

[Feature change description 91](#_Toc129617534)

[Command changes 91](#_Toc129617535)

[Modified command: sflow counter collector 91](#_Toc129617536)

[Modified feature: sFlow flow sampling 92](#_Toc129617537)

[Feature change description 92](#_Toc129617538)

[Command changes 92](#_Toc129617539)

[Modified command: sflow counter collector 92](#_Toc129617540)

[Release 3208P16 93](#_Toc129617541)

[New feature: Setting the block timer for MAC addresses in the blocked MAC address list 93](#_Toc129617542)

[Setting the block timer for MAC addresses in the blocked MAC address list 93](#_Toc129617543)

[About setting the block timer for MAC addresses in the blocked MAC address list 93](#_Toc129617544)

[Procedure 93](#_Toc129617545)

[Command reference 93](#_Toc129617546)

[port-security timer blockmac 93](#_Toc129617547)

[New feature: Logging off 802.1X users 94](#_Toc129617548)

[Logging off 802.1X users 94](#_Toc129617549)

[Command reference 94](#_Toc129617550)

[reset dot1x access-user 94](#_Toc129617551)

[New feature: Logging off MAC authentication users 95](#_Toc129617552)

[Logging off MAC authentication users 95](#_Toc129617553)

[Command reference 95](#_Toc129617554)

[reset mac-authentication access-user 95](#_Toc129617555)

[Release 3208P15 97](#_Toc129617556)

[New feature: Configuring zero-to-two VLAN mapping 97](#_Toc129617557)

[Configuring zero-to-two VLAN mapping 97](#_Toc129617558)

[Command reference 98](#_Toc129617559)

[vlan mapping untagged 98](#_Toc129617560)

[New feature: Specifying DNS server information in RA messages 99](#_Toc129617561)

[Specifying DNS server information in RA messages 99](#_Toc129617562)

[About specifying DNS server information in RA messages 99](#_Toc129617563)

[Restrictions and guidelines 99](#_Toc129617564)

[Procedure 100](#_Toc129617565)

[Command reference 100](#_Toc129617566)

[ipv6 nd ra dns server 100](#_Toc129617567)

[New feature: Specifying DNS suffix information in RA messages 101](#_Toc129617568)

[Specifying DNS suffix information in RA messages 101](#_Toc129617569)

[About specifying DNS suffix information in RA messages 101](#_Toc129617570)

[Restrictions and guidelines 102](#_Toc129617571)

[Procedure 102](#_Toc129617572)

[Command reference 102](#_Toc129617573)

[ipv6 nd ra dns search-list 102](#_Toc129617574)

[New feature: Suppressing advertising DNS information in RA messages 103](#_Toc129617575)

[Suppressing advertising DNS information in RA messages 103](#_Toc129617576)

[About suppressing advertising DNS information in RA messages 103](#_Toc129617577)

[Procedure 104](#_Toc129617578)

[Command reference 104](#_Toc129617579)

[ipv6 nd ra dns search-list suppress 104](#_Toc129617580)

[ipv6 nd ra dns server suppress 105](#_Toc129617581)

[New feature: HTTP redirect 106](#_Toc129617582)

[About HTTP redirect 106](#_Toc129617583)

[HTTP redirect tasks at a glance 106](#_Toc129617584)

[Specifying the HTTPS redirect listening port number 107](#_Toc129617585)

[Associating an SSL server policy with the HTTPS redirect service 107](#_Toc129617586)

[Command reference 107](#_Toc129617587)

[http-redirect https-port 107](#_Toc129617588)

[http-redirect ssl-server-policy 108](#_Toc129617589)

[New feature: ERPS 109](#_Toc129617590)

[Configuring ERPS 109](#_Toc129617591)

[About ERPS 109](#_Toc129617592)

[Restrictions and guidelines: ERPS configuration 117](#_Toc129617593)

[ERPS tasks at a glance 117](#_Toc129617594)

[Prerequisites 118](#_Toc129617595)

[Enabling ERPS globally 118](#_Toc129617596)

[Configuring an ERPS ring 118](#_Toc129617597)

[Enabling ERPS for an instance 121](#_Toc129617598)

[Enabling R-APS packets to carry the ring ID in the destination MAC address 121](#_Toc129617599)

[Configuring R-APS packet levels 122](#_Toc129617600)

[Setting ERPS timers 122](#_Toc129617601)

[Setting the non-revertive mode 122](#_Toc129617602)

[Setting a switchover mode 123](#_Toc129617603)

[Associating a ring with a subring 123](#_Toc129617604)

[Enabling flush packet transparent transmission 124](#_Toc129617605)

[Associating an ERPS ring member port with a track entry 124](#_Toc129617606)

[Removing the MS mode and FS mode settings for an ERPS ring 124](#_Toc129617607)

[Displaying and maintaining ERPS 124](#_Toc129617608)

[ERPS configuration examples 125](#_Toc129617609)

[Troubleshooting ERPS 157](#_Toc129617610)

[Command reference 157](#_Toc129617611)

[control-vlan 157](#_Toc129617612)

[display erps 158](#_Toc129617613)

[display erps detail 159](#_Toc129617614)

[display erps statistics 162](#_Toc129617615)

[erps clear 163](#_Toc129617616)

[erps enable 164](#_Toc129617617)

[erps ring 164](#_Toc129617618)

[erps switch 165](#_Toc129617619)

[erps tcn-propagation 165](#_Toc129617620)

[instance 166](#_Toc129617621)

[instance enable 167](#_Toc129617622)

[node-role 167](#_Toc129617623)

[port erps track 168](#_Toc129617624)

[port0 169](#_Toc129617625)

[port1 169](#_Toc129617626)

[protected-vlan 170](#_Toc129617627)

[r-aps level 171](#_Toc129617628)

[r-aps ring-mac 171](#_Toc129617629)

[reset erps statistics 172](#_Toc129617630)

[revertive-operation 172](#_Toc129617631)

[ring-type sub-ring 173](#_Toc129617632)

[sub-ring connect 173](#_Toc129617633)

[timer guard 174](#_Toc129617634)

[timer hold-off 174](#_Toc129617635)

[timer wtr 175](#_Toc129617636)

[Modified feature: Physical type of a combo interface 176](#_Toc129617637)

[Feature change description 176](#_Toc129617638)

[Command changes 176](#_Toc129617639)

[combo enable 176](#_Toc129617640)

[Release 3208P12 178](#_Toc129617641)

[New feature: PD detection mode 178](#_Toc129617642)

[Configuring the PD detection mode 178](#_Toc129617643)

[Command reference 178](#_Toc129617644)

[poe detection-mode 178](#_Toc129617645)

[Modified feature: Setting the length of ICMP or ICMPv6 echo requests for the ping operation 179](#_Toc129617646)

[Feature change description 179](#_Toc129617647)

[Command changes 179](#_Toc129617648)

[Modified command: ping 179](#_Toc129617649)

[Modified command: ping ipv6 180](#_Toc129617650)

[Release 3208P10 181](#_Toc129617651)

[New feature: Automatic obtaining of the login username for temporary user role authorization 181](#_Toc129617652)

[Automatically obtaining the login username for temporary user role authorization 181](#_Toc129617653)

[About automatic obtaining of the login username for temporary user role authorization 181](#_Toc129617654)

[Restrictions and guidelines 181](#_Toc129617655)

[Procedure 181](#_Toc129617656)

[Command reference 182](#_Toc129617657)

[super use-login-username 182](#_Toc129617658)

[New feature: 802.1X EAP-TLS fragmentation for packets sent to the server 182](#_Toc129617659)

[Setting the maximum length of an EAP-TLS fragment sent to the server 182](#_Toc129617660)

[Command reference 183](#_Toc129617661)

[dot1x eap-tls-fragment to-server 183](#_Toc129617662)

[New feature: Enabling interface consistency check for ARP and MAC address entries 184](#_Toc129617663)

[Enabling interface consistency check for ARP and MAC address entries 184](#_Toc129617664)

[Command reference 185](#_Toc129617665)

[arp mac-interface-consistency check enable 185](#_Toc129617666)

[New feature: 802.1X offline detection 185](#_Toc129617667)

[Configuring 802.1X offline detection 185](#_Toc129617668)

[Command reference 186](#_Toc129617669)

[dot1x offline-detect enable 186](#_Toc129617670)

[dot1x timer offline-detect 187](#_Toc129617671)

[New feature: Enabling SAVI and setting the entry deletion delay by using commands 188](#_Toc129617672)

[About SAVI 188](#_Toc129617673)

[SAVI application scenarios 188](#_Toc129617674)

[SAVI tasks at a glance 188](#_Toc129617675)

[Enabling SAVI 188](#_Toc129617676)

[Configuring IPv6 source guard 189](#_Toc129617677)

[Configuring DHCPv6 snooping 189](#_Toc129617678)

[Configuring ND snooping and ND attack detection 189](#_Toc129617679)

[Setting the entry deletion delay 189](#_Toc129617680)

[SAVI configuration examples 190](#_Toc129617681)

[Example: Configuring DHCPv6-only SAVI 190](#_Toc129617682)

[Example: Configuring SLAAC-only SAVI 191](#_Toc129617683)

[Example: Configuring DHCPv6+SLAAC SAVI 192](#_Toc129617684)

[SAVI commands 194](#_Toc129617685)

[ipv6 savi down-delay 194](#_Toc129617686)

[ipv6 savi strict 194](#_Toc129617687)

[Modified feature: Configuring MAC-based MAC authentication user accounts 195](#_Toc129617688)

[Feature change description 195](#_Toc129617689)

[Command changes 195](#_Toc129617690)

[Modified command: mac-authentication user-name-format 195](#_Toc129617691)

[Modified feature: Port security NTK feature 195](#_Toc129617692)

[Feature change description 195](#_Toc129617693)

[Command changes 196](#_Toc129617694)

[Modified command: port-security ntk-mode 196](#_Toc129617695)

[Release 3208P08 197](#_Toc129617696)

[New feature: Shutting down an interface by OpenFlow 197](#_Toc129617697)

[Shut down an interface by OpenFlow. 197](#_Toc129617698)

[Command reference 197](#_Toc129617699)

[openflow shutdown 197](#_Toc129617700)

[Release 3208P03 199](#_Toc129617701)

[New feature: VRRP 199](#_Toc129617702)

[About VRRP 199](#_Toc129617703)

[VRRP standard mode 200](#_Toc129617704)

[VRRP networking 200](#_Toc129617705)

[Virtual IP address and IP address owner 200](#_Toc129617706)

[Router priority in a VRRP group 200](#_Toc129617707)

[Preemption 200](#_Toc129617708)

[Authentication method 201](#_Toc129617709)

[VRRP timers 201](#_Toc129617710)

[Master election 202](#_Toc129617711)

[VRRP tracking 202](#_Toc129617712)

[VRRP application 202](#_Toc129617713)

[VRRP load balancing mode 204](#_Toc129617714)

[Virtual MAC address assignment 204](#_Toc129617715)

[Virtual forwarder 206](#_Toc129617716)

[Protocols and standards 208](#_Toc129617717)

[Configuring IPv4 VRRP 208](#_Toc129617718)

[Restrictions and guidelines: IPv4 VRRP configuration 208](#_Toc129617719)

[IPv4 VRRP tasks at a glance 208](#_Toc129617720)

[Specifying an IPv4 VRRP operating mode 208](#_Toc129617721)

[Specifying the IPv4 VRRP version 209](#_Toc129617722)

[Configuring an IPv4 VRRP group 209](#_Toc129617723)

[Configuring IPv4 VRRP packet attributes 211](#_Toc129617724)

[Configuring VF tracking 212](#_Toc129617725)

[Setting the packet sending mode for IPv4 VRRPv3 212](#_Toc129617726)

[Enabling periodic sending of gratuitous ARP packets for IPv4 VRRP 213](#_Toc129617727)

[Configuring a subordinate IPv4 VRRP group to follow a master IPv4 VRRP group 214](#_Toc129617728)

[Enabling SNMP notifications for VRRP 215](#_Toc129617729)

[Display and maintenance commands for IPv4 VRRP 215](#_Toc129617730)

[Configuring IPv6 VRRP 215](#_Toc129617731)

[Restrictions and guidelines: IPv6 VRRP configuration 215](#_Toc129617732)

[IPv6 VRRP tasks at a glance 215](#_Toc129617733)

[Specifying an IPv6 VRRP operating mode 216](#_Toc129617734)

[Configuring an IPv6 VRRP group 216](#_Toc129617735)

[Configuring VF tracking 218](#_Toc129617736)

[Configuring IPv6 VRRP packet attributes 218](#_Toc129617737)

[Enabling periodic sending of ND packets for IPv6 VRRP 219](#_Toc129617738)

[Configuring a subordinate IPv6 VRRP group to follow a master IPv6 VRRP group 220](#_Toc129617739)

[Display and maintenance commands for IPv6 VRRP 221](#_Toc129617740)

[IPv4 VRRP configuration examples 221](#_Toc129617741)

[Example: Configuring a single VRRP group 221](#_Toc129617742)

[Example: Configuring multiple VRRP groups 224](#_Toc129617743)

[Example: Configuring VRRP load balancing 226](#_Toc129617744)

[IPv6 VRRP configuration examples 234](#_Toc129617745)

[Example: Configuring a single VRRP group 234](#_Toc129617746)

[Example: Configuring multiple VRRP groups 237](#_Toc129617747)

[Example: Configuring VRRP load balancing 241](#_Toc129617748)

[Troubleshooting VRRP 249](#_Toc129617749)

[An error prompt is displayed 249](#_Toc129617750)

[Multiple masters appear in a VRRP group 249](#_Toc129617751)

[Fast VRRP state flapping 250](#_Toc129617752)

[IPv4 VRRP commands 250](#_Toc129617753)

[display vrrp 250](#_Toc129617754)

[display vrrp binding 258](#_Toc129617755)

[display vrrp statistics 260](#_Toc129617756)

[reset vrrp statistics 263](#_Toc129617757)

[snmp-agent trap enable vrrp 264](#_Toc129617758)

[vrrp check-ttl enable 264](#_Toc129617759)

[vrrp dscp 265](#_Toc129617760)

[vrrp mode 266](#_Toc129617761)

[vrrp send-gratuitous-arp 266](#_Toc129617762)

[vrrp version 267](#_Toc129617763)

[vrrp vrid 268](#_Toc129617764)

[vrrp vrid authentication-mode 269](#_Toc129617765)

[vrrp vrid follow 270](#_Toc129617766)

[vrrp vrid name 271](#_Toc129617767)

[vrrp vrid preempt-mode 272](#_Toc129617768)

[vrrp vrid priority 273](#_Toc129617769)

[vrrp vrid shutdown 274](#_Toc129617770)

[vrrp vrid source-interface 274](#_Toc129617771)

[vrrp vrid timer advertise 275](#_Toc129617772)

[vrrp vrid track 276](#_Toc129617773)

[vrrp vrid vrrpv3-send-packet 278](#_Toc129617774)

[IPv6 VRRP commands 279](#_Toc129617775)

[display vrrp ipv6 279](#_Toc129617776)

[display vrrp ipv6 binding 286](#_Toc129617777)

[display vrrp ipv6 statistics 288](#_Toc129617778)

[reset vrrp ipv6 statistics 291](#_Toc129617779)

[vrrp ipv6 dscp 292](#_Toc129617780)

[vrrp ipv6 mode 292](#_Toc129617781)

[vrrp ipv6 send-nd 293](#_Toc129617782)

[vrrp ipv6 vrid 294](#_Toc129617783)

[vrrp ipv6 vrid follow 295](#_Toc129617784)

[vrrp ipv6 vrid name 296](#_Toc129617785)

[vrrp ipv6 vrid preempt-mode 297](#_Toc129617786)

[vrrp ipv6 vrid priority 298](#_Toc129617787)

[vrrp ipv6 vrid shutdown 298](#_Toc129617788)

[vrrp ipv6 vrid timer advertise 299](#_Toc129617789)

[vrrp ipv6 vrid track 300](#_Toc129617790)

[Release 3208 303](#_Toc129617791)

[New feature: MAC address information display for 802.1X users in 802.1X VLANs of a specific type 303](#_Toc129617792)

[Displaying MAC address information of 802.1X users in 802.1X VLANs of a specific type 303](#_Toc129617793)

[Command reference 303](#_Toc129617794)

[display dot1x mac-address 303](#_Toc129617795)

[New feature: Authorization CAR action for an ISP domain 305](#_Toc129617796)

[Configuring an authorization CAR action for an ISP domain 305](#_Toc129617797)

[Command reference 305](#_Toc129617798)

[authorization-attribute car 305](#_Toc129617799)

[New feature: 802.1X client 306](#_Toc129617800)

[Configuring 802.1X client 306](#_Toc129617801)

[802.1X client configuration task list 306](#_Toc129617802)

[Enabling the 802.1X client feature 307](#_Toc129617803)

[Configuring an 802.1X client username and password 307](#_Toc129617804)

[Configuring an 802.1X client MAC address 307](#_Toc129617805)

[Specifying an 802.1X client EAP authentication method 308](#_Toc129617806)

[Configuring an 802.1X client anonymous identifier 308](#_Toc129617807)

[Specifying an SSL client policy 309](#_Toc129617808)

[Displaying and maintaining 802.1X client 309](#_Toc129617809)

[802.1X client commands 310](#_Toc129617810)

[display dot1x supplicant 310](#_Toc129617811)

[dot1x supplicant anonymous identify 311](#_Toc129617812)

[dot1x supplicant eap-method 312](#_Toc129617813)

[dot1x supplicant enable 313](#_Toc129617814)

[dot1x supplicant mac-address 313](#_Toc129617815)

[dot1x supplicant password 314](#_Toc129617816)

[dot1x supplicant ssl-client-policy 315](#_Toc129617817)

[dot1x supplicant username 316](#_Toc129617818)

[New feature: MAC address information display for MAC authentication users in MAC authentication VLANs of a specific type 317](#_Toc129617819)

[Displaying MAC address information of MAC authentication users in MAC authentication VLANs of a specific type 317](#_Toc129617820)

[Command reference 317](#_Toc129617821)

[display mac-authentication mac-address 317](#_Toc129617822)

[Modified feature: Configuring the hash seed for global link aggregation load sharing 318](#_Toc129617823)

[Feature change description 318](#_Toc129617824)

[Command changes 318](#_Toc129617825)

[Modified command: link-aggregation global load-sharing seed 318](#_Toc129617826)

[Modified feature: Specifying a RADIUS or HWTACACS server 319](#_Toc129617827)

[Feature change description 319](#_Toc129617828)

[Command changes 319](#_Toc129617829)

[Modified commands in RADIUS scheme view: primary accounting, primary authentication, secondary accounting, secondary authentication, state secondary 319](#_Toc129617830)

[Modified commands in HWTACACS scheme view: primary accounting, primary authentication, primary authorization, secondary accounting, secondary authentication, secondary authorization 320](#_Toc129617831)

[Release 3207 321](#_Toc129617832)

[New features: Fundamentals features 322](#_Toc129617833)

[New features: IRF features 324](#_Toc129617834)

[New features: Layer 2—LAN switching features 324](#_Toc129617835)

[New features: Layer 3—IP services features 325](#_Toc129617836)

[New features: Layer 3—IP routing features 330](#_Toc129617837)

[New features: IP multicast features 331](#_Toc129617838)

[New features: ACL and QoS features 331](#_Toc129617839)

[New features: Security features 332](#_Toc129617840)

[New features: High availability features 337](#_Toc129617841)

[New features: Network management and monitoring features 338](#_Toc129617842)

[New features: OpenFlow features 340](#_Toc129617843)

[Modified feature: Configuring a command alias 340](#_Toc129617844)

[Feature change description 340](#_Toc129617845)

[Command changes 340](#_Toc129617846)

[Modified command: command-alias mapping 340](#_Toc129617847)

[Modified feature: Displaying command aliases 341](#_Toc129617848)

[Feature change description 341](#_Toc129617849)

[Command changes 341](#_Toc129617850)

[Modified command: display command-alias 341](#_Toc129617851)

[Modified feature: Configuring a hotkey 341](#_Toc129617852)

[Feature change description 341](#_Toc129617853)

[Command changes 341](#_Toc129617854)

[Modified command: hotkey 341](#_Toc129617855)

[Modified feature: Maximum length for a configuration file name 342](#_Toc129617856)

[Feature change description 342](#_Toc129617857)

[Command changes 342](#_Toc129617858)

[Modified command: configuration replace file 342](#_Toc129617859)

[Modified command: restore startup-configuration 342](#_Toc129617860)

[Modified command: save 342](#_Toc129617861)

[Modified command: startup saved-configuration 343](#_Toc129617862)

[Modified feature: BFD MAD collision handling process 343](#_Toc129617863)

[Feature change description 343](#_Toc129617864)

[Command changes 343](#_Toc129617865)

[Modified feature: Support for commands on IRF physical interfaces 343](#_Toc129617866)

[Feature change description 343](#_Toc129617867)

[Command changes 344](#_Toc129617868)

[Modified feature: Excluding a service interface from the IRF MAD shutdown action by the system 344](#_Toc129617869)

[Feature change description 344](#_Toc129617870)

[Command changes 345](#_Toc129617871)

[Modified feature: Displaying information about packets dropped on an interface 345](#_Toc129617872)

[Feature change description 345](#_Toc129617873)

[Command changes 345](#_Toc129617874)

[Modified command: display packet-drop 345](#_Toc129617875)

[Modified feature: Displaying MAC address move records 345](#_Toc129617876)

[Feature change description 345](#_Toc129617877)

[Command changes 345](#_Toc129617878)

[Modified feature: MAC address move notifications 345](#_Toc129617879)

[Feature change description 345](#_Toc129617880)

[Command changes 346](#_Toc129617881)

[Modified feature: Setting the voice VLAN aging timer 346](#_Toc129617882)

[Feature change description 346](#_Toc129617883)

[Command changes 346](#_Toc129617884)

[Modified command: voice-vlan aging 346](#_Toc129617885)

[Modified feature: Creating a VLAN 346](#_Toc129617886)

[Feature change description 346](#_Toc129617887)

[Command changes 347](#_Toc129617888)

[Modified command: vlan 347](#_Toc129617889)

[Modified feature: Displaying history about ports that are blocked by spanning tree protection features 347](#_Toc129617890)

[Feature change description 347](#_Toc129617891)

[Command changes 347](#_Toc129617892)

[Modified command: display stp abnormal-port 347](#_Toc129617893)

[Modified feature: Setting the LLDP frame transmission interval 348](#_Toc129617894)

[Feature change description 348](#_Toc129617895)

[Command changes 348](#_Toc129617896)

[Modified command: lldp timer tx-interval 348](#_Toc129617897)

[Modified feature: Displaying ARP entries 348](#_Toc129617898)

[Feature change description 348](#_Toc129617899)

[Command changes 349](#_Toc129617900)

[Modified command: display arp 349](#_Toc129617901)

[Modified feature: Displaying the aging time of dynamic ARP entries 350](#_Toc129617902)

[Feature change description 350](#_Toc129617903)

[Command changes 350](#_Toc129617904)

[Modified command: display arp timer aging 350](#_Toc129617905)

[Modified feature: Default source IP address in packets relayed to the DHCP server 351](#_Toc129617906)

[Feature change description 351](#_Toc129617907)

[Command changes 351](#_Toc129617908)

[Modified feature: Specifying gateways on the DHCP server for DHCP clients 351](#_Toc129617909)

[Feature change description 351](#_Toc129617910)

[Command changes 351](#_Toc129617911)

[Modified command: gateway-list 351](#_Toc129617912)

[Modified feature: Displaying information for DHCP snooping trusted ports 352](#_Toc129617913)

[Feature change description 352](#_Toc129617914)

[Command changes 352](#_Toc129617915)

[Modified command: display dhcp snooping trust 352](#_Toc129617916)

[Modified feature: Setting the MTU of IPv4 packets sent over an interface 353](#_Toc129617917)

[Feature change description 353](#_Toc129617918)

[Command changes 353](#_Toc129617919)

[Modified command: ip mtu 353](#_Toc129617920)

[Modified feature: Setting the TCP buffer size 353](#_Toc129617921)

[Feature change description 353](#_Toc129617922)

[Command changes 353](#_Toc129617923)

[Modified command: tcp window 353](#_Toc129617924)

[Modified feature: Configuring prefix to be advertised in RA messages 354](#_Toc129617925)

[Feature change description 354](#_Toc129617926)

[Command changes 354](#_Toc129617927)

[Modified command: ipv6 nd ra prefix 354](#_Toc129617928)

[Modified feature: Setting the MTU of IPv6 packets sent over an interface 354](#_Toc129617929)

[Feature change description 354](#_Toc129617930)

[Command changes 355](#_Toc129617931)

[Modified feature: Displaying PBR configuration 355](#_Toc129617932)

[Feature change description 355](#_Toc129617933)

[Command changes 355](#_Toc129617934)

[Modified command: display ip policy-based-route setup 355](#_Toc129617935)

[Modified feature: Displaying IPv6 PBR configuration 356](#_Toc129617936)

[Feature change description 356](#_Toc129617937)

[Command changes 356](#_Toc129617938)

[Modified command: display ipv6 policy-based-route setup 356](#_Toc129617939)

[Modified feature: Creating an ACL 356](#_Toc129617940)

[Feature change description 356](#_Toc129617941)

[Command changes 357](#_Toc129617942)

[Modified command: acl 357](#_Toc129617943)

[Modified feature: Copying an ACL to create a new ACL 357](#_Toc129617944)

[Feature change description 357](#_Toc129617945)

[Command changes 357](#_Toc129617946)

[Modified command: acl copy 357](#_Toc129617947)

[Modified feature: Displaying ACL configuration and match statistics 358](#_Toc129617948)

[Feature change description 358](#_Toc129617949)

[Command changes 358](#_Toc129617950)

[Modified command: display acl 358](#_Toc129617951)

[Modified feature: Displaying packet filtering statistics 358](#_Toc129617952)

[Feature change description 358](#_Toc129617953)

[Command changes 358](#_Toc129617954)

[Modified command: display packet-filter statistics 358](#_Toc129617955)

[Modified feature: Displaying accumulated packet filtering statistics for an ACL 359](#_Toc129617956)

[Feature change description 359](#_Toc129617957)

[Command changes 359](#_Toc129617958)

[Modified command: display packet-filter statistics sum 359](#_Toc129617959)

[Modified feature: Displaying ACL application details for packet filtering 359](#_Toc129617960)

[Feature change description 359](#_Toc129617961)

[Command changes 359](#_Toc129617962)

[Modified command: display packet-filter verbose 359](#_Toc129617963)

[Modified feature: Applying an ACL to an interface for packet filtering 360](#_Toc129617964)

[Feature change description 360](#_Toc129617965)

[Command changes 360](#_Toc129617966)

[Modified command: packet-filter 360](#_Toc129617967)

[Modified feature: Specify the applicable scope of packet filtering on a VLAN interface 360](#_Toc129617968)

[Feature change description 360](#_Toc129617969)

[Command changes 361](#_Toc129617970)

[Modified command: packet-filter filter 361](#_Toc129617971)

[Modified feature: Clearing statistics for ACLs 361](#_Toc129617972)

[Feature change description 361](#_Toc129617973)

[Command changes 361](#_Toc129617974)

[Modified command: reset acl counter 361](#_Toc129617975)

[Modified feature: Clearing the packet filtering statistics and accumulated statistics for an ACL 361](#_Toc129617976)

[Feature change description 361](#_Toc129617977)

[Command changes 362](#_Toc129617978)

[Modified command: reset packet-filter statistics 362](#_Toc129617979)

[Modified feature: Specifying an ACL match criterion 362](#_Toc129617980)

[Feature change description 362](#_Toc129617981)

[Command changes 362](#_Toc129617982)

[Modified command: if-match acl 362](#_Toc129617983)

[Modified feature: Displaying predefined control plane QoS policies of cards 362](#_Toc129617984)

[Feature change description 362](#_Toc129617985)

[Command changes 363](#_Toc129617986)

[Modified command: display qos policy control-plane pre-defined 363](#_Toc129617987)

[Modified feature: Length range for an ISP domain 364](#_Toc129617988)

[Feature change description 364](#_Toc129617989)

[Command changes 364](#_Toc129617990)

[Modified commands: display domain, domain, domain default enable, domain if-unknown 364](#_Toc129617991)

[Modified feature: Displaying local user configuration 365](#_Toc129617992)

[Feature change description 365](#_Toc129617993)

[Command changes 365](#_Toc129617994)

[Modified command: display local-user 365](#_Toc129617995)

[Modified feature: Displaying user group configuration 365](#_Toc129617996)

[Feature change description 365](#_Toc129617997)

[Command changes 366](#_Toc129617998)

[Modified command: display user-group 366](#_Toc129617999)

[Modified feature: Enabling the RADIUS server load sharing feature 366](#_Toc129618000)

[Feature change description 366](#_Toc129618001)

[Command changes 366](#_Toc129618002)

[Modified command: server-load-sharing enable 366](#_Toc129618003)

[Modified feature: Setting the real-time accounting interval 367](#_Toc129618004)

[Feature change description 367](#_Toc129618005)

[Command changes 367](#_Toc129618006)

[Modified command: timer realtime-accounting 367](#_Toc129618007)

[Modified feature: Displaying 802.1X information 367](#_Toc129618008)

[Feature change description 367](#_Toc129618009)

[Command changes 367](#_Toc129618010)

[Modified command: display dot1x 367](#_Toc129618011)

[Modified feature: Port-specific mandatory 802.1X authentication domain 368](#_Toc129618012)

[Feature change description 368](#_Toc129618013)

[Command changes 368](#_Toc129618014)

[Modified command: dot1x mandatory-domain 368](#_Toc129618015)

[Modified feature: Removing users from the MAC authentication critical VLAN on a port 368](#_Toc129618016)

[Feature change description 368](#_Toc129618017)

[Command changes 368](#_Toc129618018)

[Modified command: reset mac-authentication critical vlan 368](#_Toc129618019)

[Modified feature: Port security's limit on the number of secure MAC addresses on a port 369](#_Toc129618020)

[Feature change description 369](#_Toc129618021)

[Command changes 369](#_Toc129618022)

[Modified command: port-security max-mac-count 369](#_Toc129618023)

[Modified feature: Enabling the SSH server to support SSH1 clients 369](#_Toc129618024)

[Feature change description 369](#_Toc129618025)

[Command changes 369](#_Toc129618026)

[Modified command: ssh server compatible-ssh1x 369](#_Toc129618027)

[Modified feature: Creating an SSH user and specifying the service type and authentication method 370](#_Toc129618028)

[Feature change description 370](#_Toc129618029)

[Command changes 370](#_Toc129618030)

[Modified command: ssh user 370](#_Toc129618031)

[Modified feature: Predefined user roles for SSH and FTP client commands 371](#_Toc129618032)

[Feature change description 371](#_Toc129618033)

[Command changes 371](#_Toc129618034)

[Modified command: bye 371](#_Toc129618035)

[Modified command: exit 371](#_Toc129618036)

[Modified command: help 371](#_Toc129618037)

[Modified command: quit 372](#_Toc129618038)

[Modified feature: Setting the number of ARP blackhole route probes for each unresolved IP address 372](#_Toc129618039)

[Feature change description 372](#_Toc129618040)

[Command changes 372](#_Toc129618041)

[Modified command: arp resolving-route probe-count 372](#_Toc129618042)

[Modified feature: Displaying information about SNMPv1 or SNMPv2c communities 373](#_Toc129618043)

[Feature change description 373](#_Toc129618044)

[Command changes 373](#_Toc129618045)

[Modified command: display snmp-agent community 373](#_Toc129618046)

[Modified feature: Displaying information about SNMP groups 374](#_Toc129618047)

[Feature change description 374](#_Toc129618048)

[Command changes 374](#_Toc129618049)

[Modified command: display snmp-agent group 374](#_Toc129618050)

[Modified feature: Displaying SNMPv3 user information 374](#_Toc129618051)

[Feature change description 374](#_Toc129618052)

[Command changes 375](#_Toc129618053)

[Modified command: display snmp-agent usm-user 375](#_Toc129618054)

[Modified feature: Configuring an SNMPv1 or SNMPv2c community 375](#_Toc129618055)

[Feature change description 375](#_Toc129618056)

[Command changes 376](#_Toc129618057)

[Modified command: snmp-agent community 376](#_Toc129618058)

[Modified feature: Creating an SNMP group 376](#_Toc129618059)

[Feature change description 376](#_Toc129618060)

[Command changes 376](#_Toc129618061)

[Modified command: snmp-agent group 376](#_Toc129618062)

[Modified feature: Creating an SNMPv1 or SNMPv2c user 377](#_Toc129618063)

[Feature change description 377](#_Toc129618064)

[Command changes 377](#_Toc129618065)

[Modified command: snmp-agent usm-user { v1 | v2c } 377](#_Toc129618066)

[Modified feature: Creating an SNMPv3 user 378](#_Toc129618067)

[Feature change description 378](#_Toc129618068)

[Command changes 378](#_Toc129618069)

[Modified command: snmp-agent usm-user v3 378](#_Toc129618070)

[Modified feature: Configuration locking BY NETCONF 380](#_Toc129618071)

[Feature change description 380](#_Toc129618072)

[Command changes 380](#_Toc129618073)

[Modified feature: Value range for the interval for an OpenFlow instance to reconnect to a controller 380](#_Toc129618074)

[Feature change description 380](#_Toc129618075)

[Command changes 380](#_Toc129618076)

[Modified command: controller connect interval 380](#_Toc129618077)

[Removed features 380](#_Toc129618078)

[Related documentation 382](#_Toc129618079)

1. Release 3507P10

This release has no feature changes.

1. Release 3507P09

This release has no feature changes.

1. Release 3507P02

This release has no feature changes.

Release 3507

This release has the following changes:

* Modified feature: EAD assistant

# Modified feature: EAD assistant

## Feature change description

As from this version, you can use both EAD assistant and MAC authentication on the device.

Before modification: EAD assistant is mutually exclusive with MAC authentication and port security.

* You cannot enable EAD assistant when MAC authentication or port security is enabled globally.
* You cannot enable MAC authentication or port security globally when EAD assistant is enabled.

After modification: EAD assistant is still mutually exclusive with the port security feature, but you can use both EAD assistant and MAC authentication on the device. When you use both EAD assistant and MAC authentication on the device, follow these restrictions and guidelines:

* If both EAD assistant and MAC authentication are configured on the device, the MAC address of a user that fails MAC authentication is not marked as a silent MAC address. If the user has never passed MAC authentication, packets from the user can trigger MAC authentication again only after the user's EAD entry ages out.
* As a best practice, do not configure MAC authentication guest VLANs or critical VALNs. The VLANs might fail to work correctly when both EAD assistant and MAC authentication are configured on the device.
* As a best practice, do not configure the Web authentication or IP source guard feature. The feature might fail to work correctly when both EAD assistant and MAC authentication are configured on the device.
* If the MAC address of a user has been marked as a silent MAC address before EAD assistant is enabled, packets from the user can trigger 802.1X or MAC authentication only after the quiet timer expires.

## Command changes

None.

1. Release 3506P10

This release has the following changes:

* New feature: Configuring the 802.1p priority for control packets sent by a device
* New feature: Packet spoofing logging and filtering entry logging for SAVI
* New feature: Configuring password control over weak passwords
* New feature: Enabling password change prompt logging

# New feature: Configuring the 802.1p priority for control packets sent by a device

## Configuring the 802.1p priority for control packets sent by a device

#### About this task

By default, the 802.1p priority is 6 for control packets sent by a device. However, some devices will drop or not process packets with 802.1p priority 6, which affects the operation of protocols in the network. To resolve this problem, configure the 802.1p priority for control packets sent by a device.

#### Restrictions and guidelines

This feature configures the 802.1p priority for packets of the following protocols: ARP, DNS, NTP, OSPF, ICMP, SSH, Telnet, RADIUS, SYSLOG, and SNMP.

#### Procedure

Enter system view.

system-view

Configure the 802.1p priority for control packets sent by the device

control-packet dot1p priority

By default, the 802.1p priority is 6 for control packets sent by a device.

## Command reference

### control-packet dot1p

Use control-packet dot1p to configure the 802.1p priority for control packets sent by a device.

Use undo control-packet dot1p to restore the default.

Syntax

control-packet dot1p priority

undo control-packet dot1p

Default

The 802.1p priority is 6 for control packets sent by a device.

Views

System view

Predefined user roles

network-admin

network-operator

Parameters

priority: Specifies an 802.1p priority value in the range of 0 to 7. 0 indicates the lowest priority, and 7 indicates the highest priority.

Usage guidelines

By default, the 802.1p priority is 6 for control packets sent by a device. However, some devices will drop or not process packets with 802.1p priority 6, which affects the operation of protocols in the network. To resolve this problem, configure the 802.1p priority for control packets sent by a device.

This command configures the 802.1p priority for packets of the following protocols: ARP, DNS, NTP, OSPF, ICMP, SSH, Telnet, RADIUS, SYSLOG, and SNMP. As a best practice, make sure you have known the impact on the network before executing this command.

Examples

# Configure the 802.1p priority as 7 for control packets sent by the device.

<Sysname> system-view

[Sysname] control-packet dot1p 7

# New feature: Packet spoofing logging and filtering entry logging for SAVI

## Enabling packet spoofing logging and filtering entry logging

#### About this task

Packet spoofing logging enables the device to generate log messages for the spoofed packets detected by SAVI.

Filtering entries are effective bindings used for filtering IPv6 packets by the source IPv6 address. Filtering entry logging enables the device to generate log messages for filtering entries. A log message contains the IPv6 address, MAC address, VLAN, and interface of a filtering entry.

The device sends packet spoofing and filtering entry log messages to the information center. With the information center, you can set log message filtering and output rules, including output destinations. For more information about using the information center, see Network Management and Monitoring Configuration Guide.

#### Procedure

Enter system view.

system-view

Enable packet spoofing logging.

ipv6 savi log enable spoofing-packet [ interval interval | total-number number ] \*

By default, packet spoofing logging is disabled.

Enable filtering entry logging.

ipv6 savi log enable filter-entry

By default, filtering entry logging is disabled.

## Command reference

### ipv6 savi log enable

Use ipv6 savi log enable to enable packet spoofing logging or filtering entry logging.

undo ipv6 savi log enable to disable packet spoofing logging or filtering entry logging.

Syntax

ipv6 savi log enable { spoofing-packet [ interval interval | total-number number ] \* | filter-entry }

undo ipv6 savi log enable { spoofing-packet | filter-entry }

Default

Packet spoofing logging and filtering entry logging are disabled.

Views

System view

Predefined user roles

network-admin

Parameters

spoofing-packet [ interval interval | total-number number ]: Enables packet spoofing logging.

* interval interval: Sets the log output interval in seconds. The value of the interval argument can be 0 or in the range of 5 to 3600. The default value is 60 seconds. If you set this parameter to 0, the device outputs a log message immediately after it is generated.
* total-number number: Sets the maximum number of log messages that can be output per interval. The value range for the number argument is 1 to 128, and the default value is 128.

filter-entry: Enables filtering entry logging.

Usage guidelines

Packet spoofing logging enables the device to generate log messages for the spoofed packets detected by SAVI.

Filtering entries are effective bindings used for filtering IPv6 packets by the source IPv6 address. Filtering entry logging enables the device to generate log messages for filtering entries. A log message contains the IPv6 address, MAC address, VLAN, and interface of a filtering entry.

The device sends packet spoofing and filtering entry log messages to the information center. With the information center, you can set log message filtering and output rules, including output destinations. For more information about using the information center, see Network Management and Monitoring Configuration Guide.

The device can output a maximum of 128 packet spoofing log messages. If this limit is crossed, the device drops excess log messages. To ensure device performance, set the log output interval and maximum number of log messages output per interval appropriately.

Examples

# Enable packet spoofing logging.

<Sysname> system-view

[Sysname] ipv6 savi log enable spoofing-packet

# New feature: Configuring password control over weak passwords

## Configuring password control over weak passwords

#### About this task

The system checks for weak passwords for Telnet, SSH, HTTP, or HTTPS device management users. A password is weak if it does not meet the following requirements:

* Password composition restriction.
* Minimum password length restriction.
* Cannot contain the username or the reverse letters of the username.

By default, the system displays a message about a weak password but does not force the user to change it. To improve the device security, you can enable the mandatory weak password change feature, which forces the users to change the identified weak passwords. The users can log in to the device only after their passwords meet the password requirements.

#### Procedure

Enter system view.

system-view

Enable mandatory weak password change.

password-control change-password weak-password enable

By default, the mandatory weak password change feature is disabled.

## Command reference

### New command: password-control change-password weak-password enable

Use password-control change-password weak-password enable to enable mandatory weak password change.

Use undo password-control change-password weak-password enable to disable mandatory weak password change.

Syntax

password-control change-password weak-password enable

undo password-control change-password weak-password enable

Default

The mandatory weak password change feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The system checks for weak login passwords for Telnet, SSH, HTTP, or HTTPS device management users. A password is weak if it does not meet the following requirements:

* Password composition restriction.
* Minimum password length restriction.
* Cannot contain the username or the reverse letters of the username.

By default, the system displays a message about a weak password but does not force the user to change it. To improve the device security, you can enable the mandatory weak password change feature, which forces the users to change the identified weak passwords. The users can log in to the device only after their passwords meet the password requirements.

By default, the global composition policy and global minimum password length are as follows:

* A password must contain a minimum of two character types and a minimum of one character for each type.
* A password must contain a minimum of 10 characters.

By default, the password composition policy for a user group equals the global setting. The password composition policy for a local user equals that of the user group to which the local user belongs.

To change the password composition restriction and minimum password length, use the password-control composition and password-control length commands, respectively.

Examples

# Enable the mandatory weak password change feature.

<Sysname> system-view

[Sysname] password-control change-password weak-password enable

Related commands

password-control { aging | composition | history | length } enable

password-control complexity

password-control composition

password-control length

password-control enable

### Modified command: display password-control

Use display password-control to display password control configuration.

Syntax

display password-control [ super ]

Views

Any view

Predefined user roles

network-admin

Change description

Before modification: The Password change field does not contain the enabling state of the mandatory weak password change feature.

After modification: The Password change field displays the enabling state of the mandatory weak password change feature, including Enabled (mandatory weak password change) and Disabled (mandatory weak password change).

### Modified command: password-control complexity

Use password-control complexity to configure the password complexity checking policy.

Use undo password-control complexity to remove a password complexity checking item.

Syntax

password-control complexity { same-character | user-name } check

undo password-control complexity { same-character | user-name } check

Views

System view

User group view

Local user view

Change description

Before modification: By default, the global password complexity checking policy is that both username checking and repeated character checking are disabled. The password complexity checking policy for a user group equals the global setting. The password complexity checking policy for a local user equals that of the user group to which the local user belongs.

After modification: By default, the global password complexity checking policy is as follows:

* In non-FIPS mode:

The global password complexity checking policy is that username checking is enabled and repeated character checking is disabled. The password complexity checking policy for a user group equals the global setting. The password complexity checking policy for a local user equals that of the user group to which the local user belongs.

* In FIPS mode:

The global password complexity checking policy is that both username checking and repeated character checking are disabled. The password complexity checking policy for a user group equals the global setting. The password complexity checking policy for a local user equals that of the user group to which the local user belongs.

### Modified command: password-control composition

Use password-control composition to configure the password composition policy.

Use undo password-control composition to restore the default.

Syntax

password-control composition type-number type-number [ type-length type-length ]

undo password-control composition

Views

System view

User group view

Local user view

Change description

Before modification: By default, the global composition policy requires that a password must contain a minimum of one character type and a minimum of one character for each type.

After modification: By default, the global composition policy requires that a password must contain a minimum of two character types and a minimum of one character for each type.

### Modified command: password-control super composition

Use password-control super composition to configure the composition policy for super passwords.

Use undo password-control super composition to restore the default.

Syntax

password-control super composition type-number type-number [ type-length type-length ]

undo password-control super composition

Views

System view

Change description

Before modification: By default, a super password must contain a minimum of one character type and a minimum of one character for each type.

After modification: By default, a super password must contain a minimum of two character types and a minimum of one character for each type.

### Modified command: set authentication password

Use set authentication password to set the password for local password authentication.

Use undo set authentication password to restore the default.

Syntax

set authentication password { hash | simple } string

undo set authentication password

Default

No password is set for local password authentication.

Views

User line view

User line class view

Change description

Before modification: The password in plaintext form is a string of 1 to 16 characters.

After modification: The password in plaintext form is a string of 4 to 16 characters, and must contain a minimum of two character types and a minimum of one character for each type.

# New feature: Enabling password change prompt logging

## Enabling password change prompt logging

#### About this task

Use this feature to enhance the protection of passwords for Telnet, SSH, HTTP, HTTPS, NETCONF over SSH, and NETCONF over SOAP users and improve the system security.

This feature enables the device to generate logs to prompt users to change their weak passwords at an interval of 24 hours and at the users' login.

A password is a weak password if it does not meet the following requirements:

* Password composition restriction configured by using the password-control composition command.
* Minimum password length restriction set by using the password-control length command.
* It cannot contain the username or the reverse letters of the username.

For a NETCONF over SSH or NETCONF over SOAP user, the device also generates a password change prompt log if any of the following conditions exists:

* The current password of the user is the default password or has expired.
* The user logs in to the device for the first time or uses a new password to log in after global password control is enabled.

The device will no longer generate password change prompt logs for a user when one of the following conditions exists:

* The password change prompt logging feature is disabled.
* The user has changed the password and the new password meets the password control requirements.
* The enabling status of a related password control feature has changed so the current password of the user meets the password control requirements.
* The password composition policy or the minimum password length has changed.

#### Restrictions and guidelines

You can use the display password-control command to display password control configuration. For more information about password control commands, see password control commands in Security Command Reference.

#### Procedure

Enter system view.

system-view

Enable password change prompt logging.

local-server log change-password-prompt

By default, password change prompt logging is enabled.

## Command reference

### local-server log change-password-prompt

Use local-server log change-password-prompt to enable password change prompt logging.

Use undo local-server log change-password-prompt to disable password change prompt logging.

Syntax

local-server log change-password-prompt

undo local-server log change-password-prompt

Default

Password change prompt logging is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Use this feature to enhance the protection of passwords for Telnet, SSH, HTTP, HTTPS, NETCONF over SSH, and NETCONF over SOAP users and improve the system security.

This feature enables the device to generate logs to prompt users to change their weak passwords at an interval of 24 hours and at the users' login.

A password is a weak password if it does not meet the following requirements:

* Password composition restriction configured by using the password-control composition command.
* Minimum password length restriction set by using the password-control length command.
* It cannot contain the username or the reverse letters of the username.

For a NETCONF over SSH or NETCONF over SOAP user, the device also generates a password change prompt log if any of the following conditions exists:

* The current password of the user is the default password or has expired.
* The user logs in to the device for the first time or uses a new password to log in after global password control is enabled.

The device will no longer generate password change prompt logs for a user when one of the following conditions exists:

* The password change prompt logging feature is disabled.
* The user has changed the password and the new password meets the password control requirements.
* The enabling status of a related password control feature has changed so the current password of the user meets the password control requirements.
* The password composition policy or the minimum password length has changed.

You can use the display password-control command to display password control configuration. For more information about password control commands, see password control commands in Security Command Reference.

Examples

# Enable password change prompt logging.

<Sysname> system-view

[Sysname] local-server log change-password-prompt

Related commands

display password-control

password-control composition

password-control length

1. Release 3506P08

This release has no feature changes.

1. Release 3506P06

This release has the following changes:

* New feature: Enabling recording untrusted DHCP servers on a DHCP snooping device
* Modified feature: Factory defaults change for console login and password control settings

# New feature: Enabling recording untrusted DHCP servers on a DHCP snooping device

## Enabling recording untrusted DHCP servers on a DHCP snooping device

#### About this task

Typically, a DHCP snooping device identifies the DHCP servers that are connected to the untrusted ports as untrusted. The snooping device drops incoming DHCP replies through these ports. With feature enabled, the snooping device will record the DHCP servers for dropped DHCP replies, and generate and send log messages to the information center. With the information center, you can set log message filtering and output rules, including output destinations.

This command takes effect after DHCP snooping is enabled in a VLAN. If DHCP snooping is enabled globally or in a VXLAN, this command does not take effect.

If a log message is generated for an untrusted DHCP server, no more log messages will be generated for this server within 10 minutes. When the 10-minute interval expires, the DHCP snooping device will generate a log message for this server upon receiving a reply from this server.

#### Procedure

Enter system view.

system-view

Enable recording untrusted DHCP servers.

dhcp snooping untrusted-server-record enable

By default, the device does not record untrusted DHCP servers.

## Command reference

### dhcp snooping untrusted-server-record enable

Use dhcp snooping untrusted-server-record enable to enable recording untrusted DHCP servers.

Use undo dhcp snooping untrusted-server-record enable to disable recording untrusted DHCP servers.

Syntax

dhcp snooping untrusted-server-record enable

undo dhcp snooping untrusted-server-record enable

Default

Recording untrusted DHCP servers is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Typically, a DHCP snooping device identifies the DHCP servers that are connected to the untrusted ports as untrusted. The snooping device drops incoming DHCP replies through these ports. With feature enabled, the snooping device will record the DHCP servers for dropped DHCP replies, and generate and send log messages to the information center. With the information center, you can set log message filtering and output rules, including output destinations.

This command takes effect after DHCP snooping is enabled in a VLAN. If DHCP snooping is enabled globally or in a VXLAN, this command does not take effect.

If a log message is generated for an untrusted DHCP server, no more log messages will be generated for this server within 10 minutes. When the 10-minute interval expires, the DHCP snooping device will generate a log message for this server upon receiving a reply from this server.

Examples

# Enable the DHCP snooping device to record untrusted DHCP servers

<Sysname> system-view

[Sysname] dhcp snooping untrusted-server-record enable

# Modified feature: Factory defaults change for console login and password control settings

## Feature change description

Factory defaults are custom basic settings that came with the device. You can use the display default-configuration command to display factory defaults.

The device starts up with the factory defaults if no next-startup configuration files are available.

In this version, the following factory default settings are added:

#

password-control enable

#

local-user admin class manage

service-type terminal

authorization-attribute user-role network-admin

#

line class aux

authentication-mode scheme

#

undo password-control aging enable

#

undo password-control composition enable

#

undo password-control history enable

#

undo password-control length enable

#

password-control login idle-time 0

#

password-control login-attempt 3 exceed unlock

#

password-control update-interval 0

#

The output shows that the factory defaults for console login and password control settings change:

* The device performs local AAA authentication for console users. A console user must use the username admin without any password to log in to the device for the first time. The user role network-admin is assigned to the login console user.
* By default, the global password control and password change at first login are both enabled. Users must change the password at first login before they can access the system. The new password must contain a minimum of four different characters.
* The default maximum account idle time is 0 days. The system has no restriction for the account idle time.
* The default minimum password update interval is 0 hours. The system has no requirement for the password update interval.
* The default maximum number of consecutive login failures is 3. When console user fails the maximum number of login attempts, the console user can continue using this user account to make login attempts.
* After a console user modifies the password after first login, if you want to delete the default user account admin, make sure either of the following conditions are met before deleting the user account admin:
  + Another user account with the highest permissions exists.
  + The authentication-mode none command has been configured for AUX user lines.
* If you add or modify security configurations, make sure they do not conflict with the factory defaults or will not lead login failures. For more information about factory defaults, see configuration file management in Fundamentals Configuration Guide for the product. For more information about AAA authentication and password control, see Security Configuration Guide.
* After the global password control is enabled, the device generates an lauth.dat file to save the authentication and login information for local users.
  + If you execute the restore factory-default command in user view to restore the factory defaults, the lauth.dat file will be deleted. After the device reboots, you can use the username admin without any password to log in to the device, and you are required to change the password.
  + If you restore the factory defaults through Restore to factory default configuration on the boot menu, the lauth.dat file will not be deleted. After the device reboots, you must use the latest password to log in to the device.

## Command changes

None.

1. Release 3506P02

This release has no feature changes.

1. Release 3506

This release has the following changes:

* New feature: Enabling recording user IP address conflicts
* New feature: LDRA on the DHCPv6 snooping device
* New feature: Enabling link flapping protection on an interface
* New feature: Controlling the status of guest VLAN reauthentication in MAC authentication
* New feature: Specifying the Telnet service port number
* New feature: Enabling the DHCPv6 relay agent to support Option 79
* New feature: Configuring resource monitoring
* New feature: Archiving configuration to a remote SCP server
* New feature: Setting the DSCP value for SNMP responses
* New feature: Specifying the NTP time-offset thresholds for log and trap outputs
* New feature: Specifying the SNTP time-offset thresholds for log and trap outputs
* New feature: Configuring Link-up delay timer
* New feature: Configuring an EAP profile
* New feature: Configuring 802.1X unauthenticated user aging
* New feature: Configuring MAC authentication unauthenticated user aging
* New feature: VLAN check bypass for the port security MAC move feature
* New feature: Strict intrusion protection
* New feature: Specifying the source IP address for outgoing SCP packets
* New feature: gRPC
* Modified feature: Specifying the HTTPS redirect listening port number
* Modified feature: Specifying startup images
* Modified feature: Automatic configuration
* Modified feature: Displaying ARP snooping entries
* Modified feature: Clearing ARP snooping entries
* Modified feature: Setting the DHCP server response timeout time for DHCP server switchover
* Modified feature: Automatic configuration
* Modified feature: Physical type of a combo interface
* Modified feature: Physical state change suppression
* Modified feature: MAC-to-VLAN entries
* Modified feature: Displaying the loop detection configuration and status
* Modified feature: Setting the 802.1p priority for IGMP messages
* Modified feature: Setting the 802.1p priority for MLD messages
* Modified feature: Displaying IPv4SG bindings
* Modified feature: Displaying IPv6SG bindings
* Modified feature: Displaying the MFF configuration for a VLAN
* Modified feature: Associating Track with application modules
* Modified feature: Configuring binding attributes for local users
* Modified feature: Enabling password control
* Modified feature: Password management after global password control is enabled
* Modified feature: Setting the quiet timer for RADIUS servers in a RADIUS scheme
* Modified feature: MAC-based MAC authentication user accounts for MAC authentication
* Modified feature: MAC authentication VLAN mode
* Modified feature: Web authentication
* Modified feature: Port security NTK feature
* Modified feature: Port security MAC move
* Modified feature: RSA key modulus length used for creating an RSA key pair
* Modified feature: RSA key modulus length used for PKI certificate request
* Modified feature: SNMP notifications for IKE
* Modified feature: Configuring an SNMP notification target host
* Modified feature: Displaying logs buffered over the last specified period of time
* Modified feature: Specifying a log host and its output parameters
* Modified feature: Interface event
* Modified feature: NTP
* Modified feature: Specifying the source IP address for NTP messages
* Modified feature: sFlow counter sampling
* Modified feature: sFlow flow sampling

# New feature: Enabling recording user IP address conflicts

## Enabling recording user IP address conflicts

#### About this task

This feature enables the device to detect and record user IP address conflicts. The device determines that a conflict occurs if an incoming non-gratuitous ARP packet has the same sender IP address as an existing ARP entry but a different sender MAC address. The device generates a user IP address conflict record, logs the conflict, and sends the log to the information center. For information about the log destination and output rule configuration in the information center, see the information center in Network Management and Monitoring Configuration Guide.

#### Procedure

Enter system view.

system-view

Enable recording user IP address conflicts.

arp user-ip-conflict record enable

## Command reference

### arp user-ip-conflict record enable

Use arp user-ip-conflict record enable to enable recording user IP address conflicts.

Use undo arp user-ip-conflict record enable to disable recording user IP address conflicts.

Syntax

arp user-ip-conflict record enable

undo arp user-ip-conflict record enable

Default

Recording user IP address conflicts is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This feature enables the device to detect and record user IP address conflicts. The device determines that a conflict occurs if an incoming non-gratuitous ARP packet has the same sender IP address as an existing ARP entry but a different sender MAC address. The device generates a user IP address conflict record, logs the conflict, and sends the log to the information center. For information about the log destination and output rule configuration, see the information center in Network Management and Monitoring Configuration Guide.

An IRF member device can generate a maximum of 10 user IP address conflict logs per second.

To display user IP address conflict records, use the display arp user-ip-conflict record command.

Examples

# Enable recording user IP address conflicts.

<Sysname> system-view

[Sysname] arp user-ip-conflict record enable

Related commands

display arp user-ip-conflict record

### display arp user-ip-conflict record

Use display arp user-ip-conflict record to display user IP address conflict records.

Syntax

display arp user-ip-conflict record [ slot slot-number ]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot slot-number: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays user IP address conflict records for the master device.

Usage guidelines

Each IRF member device can save a maximum of 200 user IP address conflict records.

If the maximum number is reached, a new record will override the earliest record.

Examples

# Display all user IP address conflict records.

<Sysname> display arp user-ip-conflict record

IP address: 10.1.1.1

System time: 2018-02-02 11:22:29

Conflict count: 1

Log suppress count: 0

Old interface: GigabitEthernet1/0/1

New interface: GigabitEthernet1/0/2

Old SVLAN/CVLAN: 100/2

New SVLAN/CVLAN: 100/2

Old MAC: 00e0-ca63-8141

New MAC: 00e0-ca63-8142

IP address: 10.1.1.2

System time: 2018-02-02 10:20:30

Conflict count: 1

Log suppress count: 0

Old interface: GigabitEthernet1/0/1

New interface: GigabitEthernet1/0/2

Old SVLAN/CVLAN: 100/--

New SVLAN/CVLAN: 100/--

Old MAC: 00e0-ca63-8141

New MAC: 00e0-ca63-8142

Command output

| Field | Description |
| --- | --- |
| IP address | IP address of a user. |
| System time | Time when the user IP address conflict occurred. |
| Conflict count | Number of times that conflicts for the IP address. |
| Log suppress count | Number of times that user IP address conflict logs are suppressed. |
| Old interface | Output interface in the old ARP entry. |
| New interface | Output interface in the new ARP entry. |
| Old SVLAN/CVLAN | ID of the outer VLAN or inner VLAN in the old ARP entry. This field displays hyphens (--) if the ARP entry does not belong to any outer VLAN or inner VLAN. |
| New SVLAN/CVLAN | ID of the outer VLAN or inner VLAN in the new ARP entry. This field displays hyphens (--) if the ARP entry does not belong to any outer VLAN or inner VLAN. |
| Old MAC | MAC address in the old ARP entry. |
| New MAC | MAC address in the new ARP entry. |

‌

Related commands

arp user-ip-conflict record enable

# New feature: LDRA on the DHCPv6 snooping device

## Enabling LDRA on the DHCPv6 snooping device

### About LDRA on the DHCPv6 snooping device

Some DHCPv6 servers assign IPv6 addresses or prefixes to DHCPv6 clients only based on the Interface ID option in a Relay-Forward packet. If no DHCPv6 relay agent exists between DHCPv6 clients and such a DHCP server, the IPv6 address or prefix assignment based on the Interface ID option will fail.

To solve this problem, you can enable the lightweight DHCPv6 relay agent (LDRA) on the interface that receives DHCPv6 requests. The feature allows the interface to generate a Relay-Forward packet for a received DHCPv6 request and to insert the Interface ID option in the packet. After receiving the Relay-Forward packet, the DHCPv6 server can assign an IPv6 address or prefix based on the Interface ID option.

### Procedure

Enter system view.

system-view

Enter interface view.

interface interface-type interface-number

Enable LDRA on the interface.

ipv6 dhcp snooping relay-agent enable

By default, LDRA is disabled on the interface.

## Command reference

### ipv6 dhcp snooping relay-agent enable

Use ipv6 dhcp snooping relay-agent enable to enable LDRA on an interface.

Use undo ipv6 dhcp snooping relay-agent enable to disable LDRA on an interface.

Syntax

ipv6 dhcp snooping relay-agent enable [ trust ]

undo ipv6 dhcp snooping relay-agent enable [ trust ]

Default

By default, LDRA is disabled on the interface.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

trust: Specifies the interface as a trusted interface. The device trusts the Relay-Forward packets received on the interface and forwards these packets to the DHCPv6 server. If you do not specify this keyword, the device drops the Relay-Forward packets received on this interface.

Usage guidelines

A network might have multiple cascaded lightweight DHCPv6 relay agents. As a best practice, do not specify the trust keyword if illegal Relay-Forward packets exist in the network.

Before you enable this feature, execute the ipv6 dhcp snooping enable command to enable DHCPv6 snooping. Otherwise, this feature does not take effect.

If this command and the ipv6 dhcp snooping option interface-id enable command are both executed, this command does not take effect.

Examples

# Enable LDRA on .

<Sysname> system-view

[Sysname] interface

[Sysname-] ipv6 dhcp snooping relay-agent enable

# New feature: Enabling link flapping protection on an interface

## Enabling link flapping protection on an interface

### About link flapping protection

Link flapping on an interface changes network topology and increases the system overhead. For example, in an active/standby link scenario, when interface status on the active link changes between UP and DOWN, traffic switches between active and standby links. To solve this problem, configure this feature on the interface.

With this feature enabled on an interface, when the interface goes down, the system enables link flapping detection. During the link flapping detection interval, if the number of detected flaps reaches or exceeds the link flapping detection threshold, the system shuts down the interface.

### Restrictions and guidelines

This feature takes effect only if it is configured in both the system view and interface view.

The link-delay and port link-flap protect enable commands are mutually exclusive on an Ethernet interface.

To bring up an interface that has been shut down by link flapping protection, execute the undo shutdown command.

In the display interface command output, the Link-Flap DOWN value of the Current state field indicates that the interface has been shut down by link flapping protection.

IRF physical interfaces also support this feature. However, this feature on IRF physical interfaces works differently from this feature on common Ethernet interfaces as follows:

* To avoid IRF physical link flapping, which will affect the IRF system stability, this feature is enabled by default on IRF physical interfaces and is not affected by the status of global link flapping protection.
* If the number of detected flaps on an IRF physical interface reaches or exceeds the link flapping detection threshold during the link flapping detection interval, the system displays prompt messages rather than shuts down the interface.

### Procedure

Enter system view.

system-view

Enable link flapping protection globally.

link-flap protect enable

By default, link flapping protection is disabled globally.

Enter Ethernet interface view.

interface interface-type interface-number

Enable link flapping protection on the Ethernet interface.

port link-flap protect enable [ interval interval | threshold threshold ] \*

By default, link flapping protection is disabled on an Ethernet interface.

## Command reference

### display link-flap protection

Use display link-flap protection to display information about link flapping protection on an interface.

Syntax

display link-flap protection [ interface interface-type [ interface-number ] ]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type: Specifies an interface type. If you do not specify an interface type, the command displays information about link flapping protection on all interfaces.

interface-number: Specifies an interface number. If you do not specify an interface number, the command displays information about link flapping protection on all interfaces of the specified type.

Examples

# Display information about link flapping protection on all interfaces.

<Sysname> display link-flap protection

Link-flap protection: Enabled

Interface Link-flap Status Interval Threshold

GE1/0/1 Enabled Down 10 5

GE1/0/2 Disabled N/A -- --

Command output

| Field | Description |
| --- | --- |
| Link-flap protection | Status of global link flapping protection:   * + - * Enabled—Link flapping protection is enabled globally.       * Disabled—Link flapping protection is disabled globally. |
| Link-flap | Status of link flapping protection on an interface:   * + - * Enabled—Link flapping protection is enabled on an interface.       * Disabled—Link flapping protection is disabled on an interface. |
| Status | Status of an interface:   * + - * Down—The interface has been shut down by the link flapping protection feature.       * N/A—The interface status is not affected by the link flapping protection feature. |
| Interval | Link flapping detection interval for an interface. |
| Threshold | Link flapping detection threshold for an interface. |

‌

Related commands

link-flap protect enable

port link-flap protect enable

### link-flap protect enable

Use link-flap protect enable to enable link flapping protection globally.

Use undo link-flap protect enable to disable link flapping protection globally.

Syntax

link-flap protect enable

undo link-flap protect enable

Default

Link flapping protection is disabled globally.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Link flapping on any interface changes network topology and increases the system overhead. For example, in an active/standby link scenario, when the interface status on the active link changes between UP and DOWN, traffic switches between active and standby links. To solve this problem, execute this command.

With link flapping protection enabled on an interface, when the interface goes down, the system enables link flapping detection on the interface. During the link flapping detection interval, if the number of detected flaps reaches or exceeds the link flapping detection threshold, the system shuts down the interface.

Link flapping protection takes effect only when it is enabled in both system view and interface view.

Examples

# Enable link flapping protection globally.

<Sysname> system-view

[Sysname] link-flap protect enable

Related commands

port link-flap protect enable

### port link-flap protect enable

Use port link-flap protect enable to enable link flapping protection on an interface.

Use undo port link-flap protect enable to disable link flapping protection on an interface.

Syntax

port link-flap protect enable [ interval interval | threshold threshold ] \*

undo port link-flap protect enable [ interval | threshold ]

Default

Link flapping protection is disabled on an interface.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

interval: Specifies the link flapping detection interval in seconds. The value range for this argument is 10 to 60. The default value for this argument is 10.

threshold: Specifies the link flapping detection threshold in the range of 5 to 10. The default value for this argument is 5.

Usage guidelines

Link flapping protection takes effect only when it is enabled in both system view and interface view.

If you do not specify the interval interval or threshold threshold option when you execute the port link-flap protect enable command, the command uses the default settings.

If you specify the interval or threshold keyword when you execute the undo port link-flap protect enable command, the command restores the default setting for the keyword.

With link flapping protection enabled on an interface, when the interface goes down, the system enables link flapping detection on the interface. During the link flapping detection interval, if the number of detected flaps reaches or exceeds the link flapping detection threshold, the system shuts down the interface.

To bring up an interface that has been shut down by link flapping protection, execute the undo shutdown command.

This command and the link-delay command are mutually exclusive on an Ethernet interface.

IRF physical interfaces also support this feature. However, this feature on IRF physical interfaces works differently from this feature on common Ethernet interfaces as follows:

* To avoid IRF physical link flapping, which will affect the IRF system stability, this feature is enabled by default on IRF physical interfaces and is not affected by the status of global link flapping protection.
* If the number of detected flaps on an IRF physical interface reaches or exceeds the link flapping detection threshold during the link flapping detection interval, the system displays prompt messages rather than shuts down the interface.

Examples

# Enable link flapping protection on an interface. Set the link flapping detection interval to 10 seconds, and set the link flapping detection threshold to 5.

<Sysname> system-view

[Sysname] interface

[Sysname-] port link-flap protect enable interval 10 threshold 5

Related commands

link-delay

link-flap protect enable

# New feature: Controlling the status of guest VLAN reauthentication in MAC authentication

## Enabling guest VLAN reauthentication in MAC authentication

### Overview

The guest VLAN reauthentication feature of MAC authentication enables the device to reauthenticate users in the MAC authentication guest VLAN on a port at reauthentication intervals.

In software versions earlier than R3503, guest VLAN reauthentication is enabled by default and cannot be disabled from the CLI.

As from version R3503, you can enable guest VLAN reauthentication by using the mac-authentication guest-vlan re-authenticate command or disable the feature by using the undo form of the command.

Typically, you disable this feature to suppress excessive authentication failure log messages, which might occur when a network issue results in a large number of reauthentication failures.

If guest VLAN reauthentication is disabled on a port, the device does not reauthenticate users in the MAC authentication guest VLAN on the port. The guest VLAN users will stay in the guest VLAN until they age out. To configure the aging timer, use the mac-authentication timer user-aging guest-vlan aging-time-value command.

As a best practice, set the reauthentication interval to a value greater than 30 seconds if the number of concurrent MAC authentication users on a port is likely to exceed 300.

### Configuration procedure

To enable the guest VLAN reauthentication feature of MAC authentication on a port:

Enter system view.

system-view

Enter interface view.

interface interface-type interface-number

Enable the guest VLAN reauthentication feature of MAC authentication on the port.

mac-authentication guest-vlan re-authenticate

By default, the guest VLAN reauthentication feature of MAC authentication is enabled on a port.

## Command reference

### mac-authentication guest-vlan re-authenticate

Use mac-authentication guest-vlan re-authenticate to enable the guest VLAN reauthentication feature of MAC authentication on a port.

Use undo mac-authentication guest-vlan re-authenticate to disable the guest VLAN reauthentication feature of MAC authentication on a port.

Syntax

mac-authentication guest-vlan re-authenticate

undo mac-authentication guest-vlan re-authenticate

Default

The guest VLAN reauthentication feature of MAC authentication is enabled on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

The guest VLAN reauthentication feature of MAC authentication enables the device to reauthenticate users in the MAC authentication guest VLAN on a port at reauthentication intervals.

Typically, you disable this feature to suppress excessive authentication failure log messages, which might occur when a network issue results in a large number of reauthentication failures.

If guest VLAN reauthentication is disabled on a port, the device does not reauthenticate users in the MAC authentication guest VLAN on the port. The guest VLAN users will stay in the guest VLAN until they age out. To configure the aging timer, use the mac-authentication timer user-aging guest-vlan aging-time-value command.

Examples

# Enable the guest VLAN reauthentication feature of MAC authentication on GigabitEthernet 1/0/1.

<Sysname> system-view

[Sysname] interface GigabitEthernet 1/0/1

[Sysname-GigabitEthernet1/0/1] mac-authentication guest-vlan re-authenticate

Related commands

display mac-authentication

mac-authentication guest-vlan

mac-authentication guest-vlan auth-period

mac-authentication timer

# New feature: Specifying the Telnet service port number

## Specifying the Telnet service port number

### About specifying the Telnet service port number

You can specify the Telnet service port number. By default, the Telnet service port number is 23.

### Procedure

Enter system view.

system-view

Specify the Telnet service port number.

IPv4:

telnet server port port-number

IPv6:

telnet server ipv6 port port-number

## Command reference

### telnet server ipv6 port

Use telnet server ipv6 port to specify the IPv6 Telnet service port number.

Use undo telnet server ipv6 port to restore the default.

Syntax

telnet server ipv6 port port-number

undo telnet server ipv6 port

Default

The IPv6 Telnet service port number is 23.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies a port number. The value can be 23 or in the range of 1025 to 65535.

Usage guidelines

This command terminates all existing Telnet connections to the IPv6 Telnet server. To use the Telnet service, users must reestablish Telnet connections.

Examples

# Set the IPv6 Telnet service port number to 1026.

<Sysname> system-view

[Sysname] telnet server ipv6 port 1026

### telnet server port

Use telnet server port to specify the IPv4 Telnet service port number.

Use undo telnet server port to restore the default.

Syntax

telnet server port port-number

undo telnet server port

Default

The IPv4 Telnet service port number is 23.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies a port number. The value can be 23 or in the range of 1025 to 65535.

Usage guidelines

This command terminates all existing Telnet connections to the IPv4 Telnet server. To use the Telnet service, users must reestablish Telnet connections.

Examples

# Set the IPv4 Telnet service port number to 1025.

<Sysname> system-view

[Sysname] telnet server port 1025

# New feature: Enabling the DHCPv6 relay agent to support Option 79

## Enabling the DHCPv6 relay agent to support Option 79

#### About enabling the DHCPv6 relay agent to support Option 79

If DHCPv6 relay agents exist in the network, the DHCPv6 server needs the MAC address of the DHCPv6 client for authentication or for IPv6 address or prefix assignment. To meet the requirement, enable the DHCPv6 relay agent that the client first passes to support Option 79. This feature allows the DHCPv6 relay agent to learn the MAC address in the client request. When the relay agent generates a Relay-Forward packet for the request, it fills the MAC address of the client in Option 79. The Relay-Forward packet is then forwarded to the DHCPv6 server.

#### Procedure

Enter system view.

system-view

Enter interface view.

interface interface-type interface-number

Enable the DHCPv6 relay agent to support Option 79.

ipv6 dhcp relay client-link-address enable

By default, the DHCPv6 relay agent does not support Option 79.

## Command reference

### ipv6 dhcp relay client-link-address enable

Use ipv6 dhcp relay client-link-address enable to enable the DHCPv6 relay agent to support Option 79.

Use undo ipv6 dhcp relay client-link-address enable to disable Option 79 support.

Syntax

ipv6 dhcp relay client-link-address enable

undo ipv6 dhcp relay client-link-address enable

Default

The DHCPv6 relay agent does not support Option 79.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

If DHCPv6 relay agents exist in the network, the DHCPv6 server needs the MAC address of the DHCPv6 client for authentication or for IPv6 address or prefix assignment. To meet the requirement, enable the DHCPv6 relay agent that the client first passes to support Option 79. This feature allows the DHCPv6 relay agent to learn the MAC address in the client request. When the relay agent generates a Relay-Forward packet for the request, it fills the MAC address of the client in Option 79. The Relay-Forward packet is then forwarded to the DHCPv6 server.

Examples

# Enable Option 79 support on the relay agent.

<Sysname> system-view

[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] ipv6 dhcp relay client-link-address enable

## New feature:Enable recording DHCPv6 snooping prefix entries

### Enable recording DHCPv6 snooping prefix entries

#### Restrictions and guidelines

If the basic DHCPv6 snooping features are configured globally, you can only use the undo form of the global configuration commands to disable the settings globally. The VLAN-specific configuration commands cannot disable the settings.

If the basic DHCPv6 snooping features are configured in a VLAN, you can only use the undo form of the VLAN-specific configuration commands to disable the settings in the VLAN. The global configuration command cannot disable the settings.

#### Procedure

#### Enter system view.

system-view

Enable DHCPv6 snooping globally.

ipv6 dhcp snooping enable

By default, DHCPv6 snooping is disabled globally.

Enter interface view.

interface interface-type interface-number

This interface must connect to the DHCPv6 server.

Specify the port as a trusted port.

ipv6 dhcp snooping trust

By default, all ports are untrusted ports after DHCPv6 snooping is enabled.

Enable recording DHCPv6 snooping entries.

Return to system view.

quit

Enter interface view.

interface interface-type interface-number

This interface must connect to the DHCPv6 client.

Enable recording DHCPv6 snooping prefix entries.

ipv6 dhcp snooping pd binding record

By default, recording of DHCPv6 snooping prefix entries is disabled.

## Command reference

### ipv6 dhcp snooping pd binding record

Use ipv6 dhcp snooping pd binding record to enable recording DHCPv6 snooping prefix entries.

Use undo ipv6 dhcp snooping pd binding record to disable recording DHCPv6 snooping prefix entries.

Syntax

ipv6 dhcp snooping pd binding record

undo ipv6 dhcp snooping pd binding record

Default

Recording of DHCPv6 snooping prefix entries is disabled.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

VLAN view

Predefined user roles

network-admin

Usage guidelines

This command enables DHCPv6 snooping to record IPv6 prefix-to-port information of the DHCPv6 clients (called DHCPv6 snooping prefix entries). When IP source guard (IPSG) is configured on the DHCP snooping device, IPSG can generate dynamic bindings based on the DHCP snooping prefix entries to filter out illegitimate packets.

Examples

# Enable DHCPv6 snooping prefix entries on .

<Sysname> system-view

[Sysname]interface

[Sysname-] ipv6 dhcp snooping pd binding record

Related commands

display ipv6 dhcp snooping pd binding

### display ipv6 dhcp snooping pd binding

Use display ipv6 dhcp snooping pd binding to display DHCPv6 snooping prefix entries.

Syntax

display ipv6 dhcp snooping pd binding [ prefix prefix/prefix-length [ vlan vlan-id ] ]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

prefix prefix/prefix-length: Specifies an IPv6 prefix with its length. The value range for the prefix-length argument is 1 to 128.

vlan vlan-id: Specifies the ID of the VLAN where the IPv6 prefix resides. The value range for the vlan-id argument is 1 to 4094.

Usage guidelines

This command takes effect only after you execute the ipv6 dhcp snooping pd binding record command on the port directly connecting to the clients.

If you do not specify any parameters, this command displays all DHCPv6 snooping prefix entries.

Examples

# Display all DHCPv6 snooping prefix entries.

<Sysname> display ipv6 dhcp snooping pd binding

1 DHCPv6 snooping PD entries found.

IPv6 prefix Lease VLAN SVLAN Interface

================ =========== ==== ===== ========================

1:2::/64 54 2 N/A

Command output

| Field | Description |
| --- | --- |
| n DHCPv6 snooping PD entries found. | Total number of DHCPv6 snooping prefix entries. |
| IPv6 prefix | IPv6 prefix assigned to the DHCPv6 client. |
| Lease | Remaining lease duration in seconds. |
| VLAN | When both DHCPv6 snooping and QinQ are enabled or the DHCPv6 packet contains two VLAN tags, this field identifies the outer VLAN tag. Otherwise, it identifies the VLAN where the port connecting the DHCPv6 client resides. |
| SVLAN | When both DHCPv6 snooping and QinQ are enabled or the DHCPv6 packet contains two VLAN tags, this field identifies the inner VLAN tag. Otherwise, it displays N/A. |
| Interface | Port connecting to the DHCPv6 client. |

Related commands

ipv6 dhcp snooping pd binding record

reset ipv6 dhcp snooping pd binding

### reset ipv6 dhcp snooping pd binding

Use reset ipv6 dhcp snooping pd binding to clear DHCPv6 snooping prefix entries.

Syntax

reset ipv6 dhcp snooping pd binding { all | prefix prefix/prefix-length [ vlan vlan-id ] }

Views

User view

Predefined user roles

network-admin

Parameters

all: Clears all DHCPv6 snooping prefix entries.

prefix prefix/prefix-length: Clears DHCPv6 snooping entries for the specified IPv6 prefix. The value range for the prefix-length argument is 1 to 128.

vlan vlan-id: Clears DHCPv6 snooping prefix entries for the specified VLAN. The value range for the vlan-id argument is 1 to 4094.

Usage guidelines

If you do not specify any parameters, this command clears all DHCPv6 snooping prefix entries.

Examples

# Clear DHCPv6 snooping prefix entries for 1:2::/64.

<Sysname> reset ipv6 dhcp snooping pd binding prefix 1:2::/64

Related commands

display ipv6 dhcp snooping pd binding

# New feature: Configuring resource monitoring

#### About resource monitoring

The resource monitoring feature enables the device to monitor the available amounts of types of resources, for example, the space for ARP entries. The device samples the available amounts periodically and compares the samples with resource depletion thresholds to identify the resource depletion status.

The device supports a minor resource depletion threshold and a severe resource depletion threshold for each supported resource type.

* If the available amount is equal to or less than the minor resource depletion threshold but greater than the severe resource depletion threshold, the resource type is in minor alarm state.
* If the available amount is equal to or less than the severe resource depletion threshold, the resource type is in severe alarm state.
* If the available amount increases above the minor resource depletion threshold, the resource type is in recovered state.

When a resource type enters severe alarm state, the device issues a severe alarm. If the resource type stays in severe alarm state, the device resends severe alarms periodically.

When a resource type enters minor alarm state, the device issues a minor alarm. If the resource type stays in minor alarm state or changes from severe alarm state to minor alarm state, the device identifies whether resending of minor resource depletion alarms is enabled. If the feature is disabled, the device does not issue additional minor alarms. If the feature is enabled, the device resends minor alarms periodically.

Resource depletion alarms can be sent to NETCONF, SNMP, and the information center to be encapsulated as NETCONF events, SNMP traps and informs, and log messages. For more information, see NETCONF, SNMP, and information center in Network Management and Monitoring Configuration Guide.

Resource depletion alarms and alarm-removed notifications



‌

#### Procedure

Enter system view.

system-view

Set resource depletion thresholds.

resource-monitor resource resource-name slot slot-number cpu cpu-number { by-absolute | by-percent } minor-threshold minor-threshold severe-threshold severe-threshold

The default settings vary by resource type. Use the display resource-monitor command to display the resource depletion thresholds.

Specify destinations for resource depletion alarms.

resource-monitor output { netconf-event | snmp-notification | syslog } \*

By default, resource depletion alarms are sent to NETCONF, SNMP, and the information center.

Enable resending of minor resource depletion alarms.

resource-monitor minor resend enable

By default, resending of minor resource depletion alarms is enabled.

## Command reference

### resource-monitor minor resend enable

Use resource-monitor minor resend enable to enable resending of minor resource depletion alarms.

Use undo resource-monitor minor resend enable to disable resending of minor resource depletion alarms.

Syntax

resource-monitor minor resend enable

undo resource-monitor minor resend enable

Default

Resending of minor resource depletion alarms is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When a resource type enters minor alarm state, the device issues a minor alarm. If the resource type stays in minor alarm state or changes from severe alarm state to minor alarm state, the device identifies whether resending of minor resource depletion alarms is enabled. If the feature is disabled, the device does not issue additional minor alarms. If the feature is enabled, the device resends minor alarms periodically.

The resending period is fixed at 24 hours for a severe alarm and is fixed at 7 \* 24 hours for a minor alarm.

Examples

# Enable resending of minor resource depletion alarms.

<Sysname> system-view

[Sysname] resource-monitor minor resend enable

Related commands

display resource-monitor

resource-monitor output

resource-monitor resource

### resource-monitor output

Use resource-monitor output to specify destinations for resource depletion alarms.

Use undo resource-monitor output to remove destinations for resource depletion alarms.

Syntax

resource-monitor output { netconf-event | snmp-notification | syslog } \*

undo resource-monitor output [ netconf-event | snmp-notification | syslog ] \*

Default

Resource depletion alarms are sent to NETCONF, SNMP, and the information center.

Views

System view

Predefined user roles

network-admin

Parameters

netconf-event: Sends resource depletion alarms to the NETCONF feature to encapsulate the alarms in NETCONF events. For more information, see NETCONF in Network Management and Monitoring Configuration Guide.

snmp-notification: Sends resource depletion alarms to the SNMP feature to encapsulate the alarms in SNMP traps and informs. For more information, see SNMP in Network Management and Monitoring Configuration Guide.

syslog: Sends resource depletion alarms to the information center to encapsulate the alarms in log messages. For more information, see information center in Network Management and Monitoring Configuration Guide.

Usage guidelines

If you do not specify any keywords for the undo resource-monitor output command, the command disables resource depletion alarm output.

Examples

# Specify the information center module as the output destination for resource depletion alarms.

<Sysname> system-view

[Sysname] resource-monitor output syslog

Related commands

resource-monitor minor resend enable

resource-monitor resource

### resource-monitor resource

Use resource-monitor resource to set resource depletion thresholds.

Use undo resource-monitor resource to disable resource depletion thresholds.

Syntax

resource-monitor resource resource-name slot slot-number cpu cpu-number { by-absolute | by-percent } minor-threshold minor-threshold severe-threshold severe-threshold

undo resource-monitor resource resource-name slot slot-number cpu cpu-number

Default

The default settings vary by resource type. Use the display resource-monitor command to display the resource depletion thresholds.

Views

System view

Predefined user roles

network-admin

Parameters

resource-name: Specifies a resource type by its name. The values for this argument are case insensitive and cannot be abbreviated. Table 4 shows the resource types that can be monitored.

Resource types that can be monitored

| Resource type | Description |
| --- | --- |
| agg\_group | Aggregation group hardware resources. |
| mac | MAC address table hardware resources. |
| mqcin | Inbound MQC resources. |
| mqcout | Outbound MQC resources. |
| mqcvlan | VFP MQC resources. |
| pfilterin | Inbound packet filter resources. |
| pfilterout | Outbound packet filter resources. |

‌

slot slot-number: Specifies an IRF member device by its member ID.

cpu cpu-number: Specifies a CPU by its number.

by-absolute: Specifies resource depletion thresholds by using absolute values.

by-percent: Specifies resource depletion thresholds in percentage.

minor-threshold minor-threshold: Specifies the minor resource depletion threshold. To view the value range, enter a question mark (?) in the place of the minor-threshold argument.

severe-threshold severe-threshold: Specifies the severe resource depletion threshold. To view the value range, enter a question mark (?) in the place of the severe-threshold argument.

Usage guidelines

After you execute this command for a resource type, the device monitors the available amount of the type of resources. The device samples the available amount at intervals, compares the sample with the resource depletion thresholds to identify the resource depletion status, and sends alarms as configured.

Examples

# Set the minor resource depletion threshold to 30% and the severe resource depletion threshold to 10% for ARP entry resources on slot 1.

<Sysname> system-view

[Sysname] resource-monitor resource arp slot 1 cpu 0 by-percent minor-threshold 30 severe-threshold 10

Related commands

display resource-monitor

resource-monitor minor resend enable

resource-monitor output

### display resource-monitor

Use display resource-monitor to display resource monitoring information.

Syntax

display resource-monitor [ resource resource-name ] [ slot slot-number [ cpu cpu-number ] ]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

resource resource-name: Specifies a resource type by its name. For information about available resource types, see Table 4.

slot slot-number: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays resource monitoring information for all member devices.

cpu cpu-number: Specifies a CPU by its number.

Examples

# Display ARP resource monitoring information.

<Sysname> display resource-monitor resource arp

Minor alarms resending: Enabled

Slot 1:

Resource Minor Severe Free/Total

(%) (%) (absolute)

arp 50 20 90095/90098

Command output

| Field | Description |
| --- | --- |
| Minor alarms resending | Status of the minor resource depletion alarm resending feature, Enabled or Disabled. |
| Resource | Monitored resource type. |
| Minor  (%) | Minor resource depletion threshold, in percentage. |
| Severe  (%) | Severe resource depletion threshold, in percentage. |
| Free/Total  (absolute) | Numbers of available resources and total resources, in absolute values. |

‌

Related commands

resource-monitor minor resend enable

resource-monitor resource

# New feature: Archiving configuration to a remote SCP server

## Configuring remote configuration archiving

#### About remote configuration archiving

As from this version, the device supports archiving the running configuration to a remote SCP server.

Before archiving the running configuration, you must set a file directory and file name prefix for configuration archives. The archive directory is located on a remote SCP server.

Configuration archives are named in the format of prefix\_YYYYMMDD\_HHMMSS.cfg, for example, archive\_20170526\_203430.cfg.

If you change the file directory or file name prefix on the remote SCP server, the display archive configuration command no longer displays the old configuration archives saved before the change.

#### Restrictions and guidelines

Remote archiving (the archive configuration server command) and local archiving (the archive configuration location command) are mutually exclusive. You cannot use the two features at the same time.

| IMPORTANT | IMPORTANT:  In FIPS mode, the device does not support archiving the running configuration to a remote SCP server. |
| --- | --- |

‌

The maximum number of configuration archives on a remote SCP server depends on the SCP server setting and is not restricted by the archive configuration max command.

The undo archive configuration server command removes the remote configuration archive directory and file name prefix settings, but it does not delete the configuration archives on the server. The command also performs the following operations:

* Disables both the manual and automatic configuration archiving features.
* Restores the default setting for the archive configuration interval command.
* Clears the configuration archive information displayed by using the display archive configuration command.

#### Procedure

Enter system view.

system-view

Set the directory and file name prefix for archiving the running configuration on a remote SCP server.

archive configuration server scp { ipv4-address | ipv6 ipv6-address } [ port port-number ] [ directory directory ] filename-prefix filename-prefix

By default, no path or file name prefix is set for archiving the running configuration to a remote SCP server.

Configure the username and password for accessing the remote SCP server:

Configure the username.

archive configuration server user user-name

By default, no username is configured for accessing the SCP server.

Configure the password.

archive configuration server password { cipher | simple } string

By default, no password is configured for accessing the SCP server.

Make sure the username and password are the same as the SCP account settings on the SCP server.

## Command reference

### archive configuration server

Use archive configuration server to configure the parameters for archiving the running configuration to a remote SCP server.

Use undo archive configuration server to restore the default.

Syntax

archive configuration server scp { ipv4-address | ipv6 ipv6-address } [ port port-number ] [ directory directory ] filename-prefix filename-prefix

undo archive configuration server

Default

No parameters are set for archiving the running configuration to a remote SCP server.

Views

System view

Predefined user roles

network-admin

Parameters

scp: Specifies a remote SCP server.

ipv4-address: Specifies the SCP server by its IPv4 address.

ipv6 ipv6-address: Specifies the SCP server by its IPv6 address.

port port-number: Specifies the TCP port number of the SCP server.

directory directory: Specifies the archive directory, a case-insensitive string. If you do not specify this option, the archive directory is the root directory of the SCP server.

filename-prefix filename-prefix: Specifies a file name prefix for configuration archives, a case-insensitive string of 1 to 30 characters. Valid characters are letters, digits, underscores (\_), and hyphens (-).

Usage guidelines

|  |  |
| --- | --- |
| IMPORTANT | IMPORTANT:  In FIPS mode, the device does not support archiving the running configuration to a remote SCP server. |

‌

Before archiving the running configuration to a remote SCP server, you must perform the following tasks:

* Use this command to specify a configuration archive directory and a name prefix on the remote SCP server.
* Use the archive configuration server user and archive configuration server password commands to configure a username and password for accessing the server.

To manually archive the running configuration, use the archive configuration command. To periodically archive the running configuration, use the archive configuration interval command.

On the specified remote SCP server, configuration archives are named in the format of filename-prefix\_YYYYMMDD\_HHMMSS.cfg, for example, archive\_20170526\_203430.cfg.

Local archiving (the archive configuration location command) and remote archiving (the archive configuration server command) are mutually exclusive. You cannot use the two features at the same time.

The maximum number of configuration archives on a remote SCP server depends on the SCP server setting and is not restricted by the archive configuration max command.

The undo archive configuration server command removes the configuration archive directory and file name prefix settings, but it does not delete the configuration archives saved on the server. The command also performs the following operations:

* Disables the configuration archive feature (both manual and automatic methods).
* Restores the default setting for the archive configuration interval command.
* Clears the configuration archive information displayed by using the display archive configuration command.

Examples

# Set the configuration archive directory as archive/ on the SCP server at 192.168.1.1 and set the archive file name prefix as my\_archive.

<Sysname> system-view

[Sysname] archive configuration server scp 192.168.1.1 port 22 directory /archive/ filename-prefix my\_archive

Related commands

archive configuration

archive configuration interval

archive configuration location

archive configuration server password

archive configuration server user

display archive configuration

### archive configuration server password

Use archive configuration server password to configure the password for accessing the SCP server that saves configuration archives.

Use undo archive configuration server password to restore the default.

Syntax

archive configuration server password { cipher | simple } string

undo archive configuration server password

Default

No password is configured for accessing the SCP server that saves configuration archives.

Views

System view

Predefined user roles

network-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 33 to 117 characters.

Examples

# Set the password to admin in plaintext form for accessing the SCP server that saves configuration archives.

<Sysname> system-view

[Sysname] archive configuration server password simple admin

Related commands

archive configuration server

archive configuration server user

display archive configuration

### archive configuration server user

Use archive configuration server user to configure the username for accessing the SCP server that saves configuration archives.

Use undo archive configuration server user to restore the default.

Syntax

archive configuration server user user-name

undo archive configuration server user

Default

No username is configured for accessing the SCP server that saves configuration archives.

Views

System view

Predefined user roles

network-admin

Parameters

user-name: Specifies the username, a case-sensitive string of 1 to 63 characters.

Examples

# Set the username to admin for accessing the SCP server that saves configuration archives.

<Sysname> system-view

[Sysname] archive configuration server user admin

Related commands

archive configuration server

archive configuration server password

display archive configuration

# New feature: Setting the DSCP value for SNMP responses

## Setting the DSCP value for SNMP responses

Enter system view.

system-view

Set the DSCP value for SNMP responses.

snmp-agent packet response dscp dscp-value

By default, the DSCP value for SNMP responses is 0.

## Command reference

### snmp-agent packet response dscp

Use snmp-agent packet response dscp to set the DSCP value for SNMP responses.

Use undo snmp-agent packet response dscp to restore the default.

Syntax

snmp-agent packet response dscp dscp-value

undo snmp-agent packet response dscp

Default

The DSCP value for SNMP responses is 0.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Sets the DSCP value for SNMP responses, in the range of 0 to 63. A greater DSCP value represents a higher priority.

Usage guidelines

The DSCP value is encapsulated in the ToS field of an IP packet. It specifies the priority level of the packet and affects the transmission priority of the packet.

Examples

# # Set the DSCP value to 40 for SNMP responses.

<Sysname> system-view

[Sysname] snmp-agent packet response dscp 40

# New feature: Specifying the NTP time-offset thresholds for log and trap outputs

## Specifying the NTP time-offset thresholds for log and trap outputs

#### About the NTP time-offset thresholds for log and trap outputs

By default, the system synchronizes the NTP client's time to the server and outputs a log and a trap when the time offset exceeds 128 ms for multiple times.

After you set the NTP time-offset thresholds for log and trap outputs, the system synchronizes the client's time to the server when the time offset exceeds 128 ms for multiple times, but outputs logs and traps only when the time offset exceeds the specified thresholds, respectively.

#### Procedure

Enter system view.

system-view

Specify the NTP time-offset thresholds for log and trap outputs.

ntp-service time-offset-threshold { log log-threshold | trap trap-threshold } \*

By default, no NTP time-offset thresholds are set for log and trap outputs.

## Command reference

### ntp-service time-offset-threshold

Use ntp-service time-offset-threshold to set the NTP time-offset thresholds for log and trap outputs.

Use undo ntp-service time-offset-threshold to restore the default.

Syntax

ntp-service time-offset-threshold { log log-threshold | trap trap-threshold } \*

undo ntp-service time-offset-threshold

Default

No NTP time-offset thresholds are set for log and trap outputs.

Views

System view

Predefined user roles

network-admin

mdc-admin

Parameters

log log-threshold: Specifies the NTP time-offset threshold for log output. The value range for the log-threshold argument is 128 to 60000, in milliseconds.

trap trap-threshold: Specifies the NTP time-offset threshold for trap output. The value range for the trap-threshold argument is 128 to 60000, in milliseconds.

Usage guidelines

By default, the system synchronizes the NTP client's time to the server and outputs a log and a trap when the time offset exceeds 128 ms for multiple times.

After you set the thresholds, the system synchronizes the client's time to the server when the time offset exceeds 128 ms for multiple times, but outputs logs and traps only when the time offset exceeds the specified thresholds, respectively.

Examples

# Set the NTP time-offset thresholds for log and trap outputs to 500 ms and 600 ms, respectively.

<Sysname> system-view

[Sysname] ntp-service time-offset-threshold log 500 trap 600

# New feature: Specifying the SNTP time-offset thresholds for log and trap outputs

## Specifying the SNTP time-offset thresholds for log and trap outputs

#### About SNTP time-offset thresholds for log and trap outputs

By default, the system synchronizes the SNTP client's time to the server and outputs a log and a trap when the time offset exceeds 128 ms for multiple times.

After you set the SNTP time-offset thresholds for log and trap outputs, the system synchronizes the client's time to the server when the time offset exceeds 128 ms for multiple times, but outputs logs and traps only when the time offset exceeds the specified thresholds, respectively.

#### Procedure

Enter system view.

system-view

Specify the SNTP time-offset thresholds for log and trap outputs.

sntp time-offset-threshold { log log-threshold | trap trap-threshold } \*

By default, no SNTP time-offset thresholds are set for log and trap outputs

## Command reference

### sntp time-offset-threshold

Use sntp time-offset-threshold to specify the SNTP time-offset thresholds for log and trap outputs.

Use undo sntp time-offset-threshold to restore the default.

Syntax

sntp time-offset-threshold { log log-threshold | trap trap-threshold } \*

undo sntp time-offset-threshold

Default

No SNTP time-offset thresholds are set for log and trap outputs.

Views

System view

Predefined user roles

network-admin

mdc-admin

Parameters

log log-threshold: Specifies the SNTP time-offset threshold for log output. The value range for the log-threshold argument is 128 to 60000, in milliseconds.

trap trap-threshold: Specifies the SNTP time-offset threshold for trap output. The value range for the trap-threshold argument is 128 to 60000, in milliseconds.

Usage guidelines

By default, the system synchronizes the SNTP client's time to the server and outputs a log and a trap when the time offset exceeds 128 ms for multiple times.

After you set the thresholds, the system synchronizes the client's time to the server when the time offset exceeds 128 ms for multiple times, but outputs logs and traps only when the time offset exceeds the specified thresholds, respectively.

Examples

# Set the SNTP time-offset thresholds for log and trap outputs to 500 ms and 600 ms, respectively.

<Sysname> system-view

[Sysname] sntp time-offset-threshold log 500 trap 600

# New feature: Configuring Link-up delay timer

## Configuring Link-up delay timer

#### About 802.1X unauthenticated user aging

This feature prevents frequent switchover of RRPP traffic forwarding paths caused by unstable RRPP port states. This feature behaves differently depending on whether you specify the distribute keyword in the linkup-delay-timer command.

* If you do not specify the distribute keyword, the master node starts the link-up delay timer when a faulty port comes up and the master node receives Hello packets from the secondary port.
  + If the master node can still receive Hello packets from the secondary port after the link-up delay timer expires, the master node performs the following operations:
    - Changes the RRPP ring state from Disconnect to Health.
    - Switches the traffic from the secondary port to the primary port.
  + If the master node cannot receive Hello packets from the secondary port after the Fail timer expires and before the link-up delay timer expires, the master node performs the following operations:
    - Stops the link-up delay timer.
    - Keeps the RRPP ring in Disconnect state.
* If you specify the distribute keyword, all nodes in the RRPP domain can learn the value of the link-up delay timer through Hello packets. When the faulty port comes up, the master node performs the following operations:
  + The hosting RRPP node blocks the faulty port (the faulty port cannot send or receive any packets).
  + Starts the link-up delay timer.

If the port does not become faulty after the link-up delay timer expires, the hosting RRPP node sets the port state to up. The master node can receive Hello packets from its secondary port again. Then, the master node changes the RRPP ring state from Disconnect to Health and switches the traffic from the secondary port to the primary port.

If the port becomes faulty again before the link-up delay timer expires, the hosting RRPP node blocks the port and stops the link-up delay timer.

#### Restrictions and guidelines

If the distribute keyword is not specified, the link-up delay timer value cannot be greater than the Fail timer value minus twice the Hello timer value.

If you specify the distribute keyword in an RRPP network implementing load balancing, you must configure the link-up delay timer for each RRPP domain for the timer to take effect. If you set different timer values for different RRPP domains, the smallest timer value takes effect.

#### Procedure

Enter system view.

system-view

Enter RRPP domain view.

rrpp domain domain-id

Set the link-up delay timer for the RRPP domain.

linkup-delay-timer delay-time [ distribute ]

By default, the link-up delay timer value is 0 seconds, and the distribute keyword is not specified.

## Command reference

### linkup-delay-timer

Use linkup-delay-timer to set the link-up delay timer.

Use undo linkup-delay-timer to restore the default.

Syntax

linkup-delay-timer delay-time [ distribute ]

undo linkup-delay-timer

Default

The link-up delay timer is 0 seconds, and the distribute keyword is not specified.

Views

RRPP domain view

Predefined user roles

network-admin

Parameters

delay-time: Specifies the link-up delay timer in the range of 0 to 30 seconds.

distribute: Enables all nodes in the RRPP domain to learn the link-up delay timer value.

Usage guidelines

The link-up delay timer prevents frequent switchover of RRPP traffic forwarding paths caused by unstable RRPP port states.

You can configure this command on any node in an RRPP domain, but this command can take effect only on the master node.

If you specify the distribute keyword in an RRPP network implementing loading balancing, you must configure the link-up delay timer for each RRPP domain for the timer to take effect. If you set different timer values for different RRPP domains, the smallest timer value takes effect.

If the distribute keyword is not specified, the link-up delay timer value cannot be greater than the Fail timer value minus twice the Hello timer value.

Examples

# Set the link-up delay timer to 10 seconds for RRPP domain 1.

<Sysname> system-view

[Sysname] rrpp domain 1

[Sysname-rrpp-domain1] linkup-delay-timer 10

Related commands

timer

# New feature: Configuring an EAP profile

## Configuring an EAP profile

#### About EAP profiles

An EAP profile is a collection of EAP authentication settings, including the EAP authentication method and the CA certificate file to be used for some EAP authentication methods.

#### Restrictions and guidelines

You can specify an EAP profile in multiple test profiles.

You can configure a maximum of 16 EAP profiles.

#### Prerequisites

Before you specify a CA certificate file, use FTP or TFTP to transfer the CA certificate file to the root directory of the default storage medium on the device.

In an IRF fabric, make sure a CA certificate file already exists in the root directory of the default storage medium on the master device before you specify the file.

#### Procedure

Enter system view.

system-view

Create an EAP profile and enter EAP profile view.

eap-profile eap-profile-name

Specify the EAP authentication method.

method { md5 | peap-gtc | peap-mschapv2 | ttls-gtc | ttls-mschapv2 }

By default, the EAP authentication method is MD5-challenge.

Specify a CA certificate file for EAP authentication.

ca-file file-name

By default, no CA certificate file is specified for EAP authentication.

You must specify a CA certificate file to verify the RADIUS server certificate if the EAP authentication method is PEAP-GTC, PEAP-MSCHAPv2, TTLS-GTC, or TTLS-MSCHAPv2.

## Command reference

### eap-profile

Use eap-profile to create an EAP profile and enter its view, or enter the view of an existing EAP profile.

Use undo eap-profile to delete an EAP profile.

Syntax

eap-profile eap-profile-name

undo eap-profile eap-profile-name

Default

No EAP profiles exist.

Views

System view

Predefined user roles

network-admin

Parameters

eap-profile-name: Specifies the EAP profile name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

An EAP profile is a collection of EAP authentication settings, including the EAP authentication method and the CA certificate file to be used for some EAP authentication methods. You can use an EAP profile in a test profile for RADIUS server status detection.

You can specify an EAP profile in multiple test profiles.

You can configure a maximum of 16 EAP profiles.

Examples

# Create an EAP profile named eap1 and enter its view.

<Sysname> system-view

[Sysname] eap-profile eap1

[Sysname-eap-profile-eap1]

Related commands

radius-server test-profile

### ca-file

Use ca-file to specify a CA certificate file for EAP authentication.

Use undo ca-file to restore the default.

Syntax

ca-file file-name

undo ca-file

Default

No CA certificate file is specified for EAP authentication. The device does not verify the RADIUS server certificate during EAP authentication.

Views

EAP profile view

Predefined user roles

network-admin

Parameters

file-name: Specifies a CA certificate file by its name, a case-sensitive string of 1 to 91 characters.

Usage guidelines

You must specify a CA certificate file to verify the RADIUS server certificate if the EAP authentication method is PEAP-GTC, PEAP-MSCHAPv2, TTLS-GTC, or TTLS-MSCHAPv2.

Before you specify a CA certificate file, you must use FTP or TFTP to transfer the CA certificate file to the root directory of the default storage medium on the device.

In an IRF fabric, make sure a CA certificate file already exists in the root directory of the default storage medium on the master device before you specify the file.

You can specify only one CA certificate file in an EAP profile. If you execute this command multiple times, the most recent configuration takes effect.

If you change the CA certificate file, the new CA certificate file takes effect at the next server status detection.

Examples

# In EAP profile eap1, specify CA certificate file CA.der for EAP authentication.

<Sysname> system-view

[Sysname] eap-profile eap1

[Sysname-eap-profile-eap1] ca-file CA.der

### method

Use method to specify the EAP authentication method.

Use undo method to restore the default.

Syntax

method { md5 | peap-gtc | peap-mschapv2 | ttls-gtc | ttls-mschapv2 }

undo method

Default

MD5-challenge authentication is used.

Views

EAP profile view

Predefined user roles

network-admin

Parameters

md5: Specifies the MD5-challenge method.

peap-gtc: Specifies the PEAP-GTC method.

peap-mschapv2: Specifies the PEAP-MSCHAPv2 method.

ttls-gtc: Specifies the TTLS-GTC method.

ttls-mschapv2: Specifies the TTLS-MSCHAPv2 method.

Usage guidelines

You must specify an EAP authentication method that is supported by the RADIUS server to be detected.

You can specify only one EAP authentication method in an EAP profile. If you execute this command multiple times, the most recent configuration takes effect.

If you change the EAP authentication method, the new method takes effect in the next server status detection.

Examples

# In EAP profile eap1, specify PEAP-GTC as the EAP authentication method.

<Sysname> system-view

[Sysname] eap-profile eap1

[Sysname-eap-profile-eap1] method peap-gtc

# New feature: Configuring 802.1X unauthenticated user aging

## Configuring 802.1X unauthenticated user aging

#### About 802.1X unauthenticated user aging

802.1X unauthenticated user aging applies to users added to an 802.1X guest, critical, or Auth-Fail VLAN because they have not been authenticated or have failed authentication.

When a user in one of those VLANs ages out, the device removes the user from the VLAN and deletes the MAC address entry for the user from the access port.

For users in one of those VLANs on one port to be authenticated successfully and come online on another port, enable this feature. In any other scenarios, disable this feature as a best practice.

The 802.1X user aging mechanism on a port depends on its access control mode.

* If the port uses port-based access control, a user aging timer starts when the port is assigned to the critical or Auth-Fail VLAN. When the aging timer expires, the port is removed from the VLAN and all MAC address entries for users in the VLAN are also removed.
* If the port uses MAC-based access control, a user aging timer starts for each 802.1X user when they are assigned to the Auth-Fail, critical, or guest VLAN. When the aging timer for a user expires, the device removes that user from the VLAN.

The removed users will be unable to access any network resources until after another authentication is triggered.

#### Restrictions and guidelines

As a best practice, use this feature on a port only if you want to have its unauthenticated users to be authenticated and come online on a different port.

#### Procedure

Enter system view.

system-view

Set the user aging timer for a type of 802.1X VLAN.

dot1x timer user-aging { auth-fail-vlan | critical-vlan | guest-vlan } aging-time-value

By default, the user aging timers for all applicable types of 802.1X VLANs are 1000 seconds.

Enter interface view.

interface interface-type interface-number

Enable 802.1X unauthenticated user aging.

dot1x unauthenticated-user aging enable

By default, 802.1X unauthenticated user aging is enabled.

## Command reference

### dot1x unauthenticated-user aging enable

Use dot1x unauthenticated-user aging enable to 802.1X unauthenticated user aging.

Use undo dot1x unauthenticated-user aging enable to disable 802.1X unauthenticated user aging.

Syntax

dot1x unauthenticated-user aging enable

undo dot1x unauthenticated-user aging enable

Default

User aging is enabled for 802.1X users that have not been authenticated or have not passed authentication.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

802.1X unauthenticated user aging applies to users added to 802.1X guest, critical, or Auth-Fail VLANs because they have not been authenticated or have failed authentication.

When a user in one of those VLANs ages out, the device removes the user from the VLAN and deletes the MAC address entry for the user from the access port.

The 802.1X user aging mechanism on a port depends on its access control mode.

* If the port uses port-based access control, a user aging timer starts when the port is assigned to the critical or Auth-Fail VLAN. When the aging timer expires, the port is removed from the VLAN and all MAC address entries for users in the VLAN are also removed.
* If the port uses MAC-based access control, a user aging timer starts for each 802.1X user when they are assigned to the Auth-Fail, critical, or guest VLAN. When the aging timer for a user expires, the device removes that user from the VLAN.

For users in one of those VLANs on one port to be authenticated successfully and come online on another port, enable this feature. In any other scenarios, disable this feature as a best practice.

The removed users will be unable to access any network resources until after another authentication is triggered.

Examples

# Disable 802.1X user aging on .

<Sysname> system-view

[Sysname] interface

[Sysname-] undo dot1x unauthenticated-user aging enable

Related commands

dot1x timer

### dot1x timer user-aging

Use dot1x timer user-aging to set the user aging timer for a type of 802.1X VLAN.

Use undo dot1x timer user-aging to restore the default user aging timer setting for a type of 802.1X VLAN.

Syntax

dot1x timer user-aging { auth-fail-vlan | critical-vlan | guest-vlan } aging-time-value

undo dot1x timer user-aging { auth-fail-vlan | critical-vlan | guest-vlan }

Default

By default, the user aging timers for all applicable types of 802.1X VLANs are 1000 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

user-aging: Sets the user aging timer for a type of 802.1X VLAN.

auth-fail-vlan: Specifies 802.1X Auth-Fail VLANs.

critical-vlan: Specifies 802.1X critical VLANs.

guest-vlan: Specifies 802.1X guest VLANs.

aging-time-value: Sets the user aging timer. The value range is 60 to 2147483647 seconds.

Usage guidelines

If you enable 802.1X unauthenticated user aging, you can set a user aging timer for Auth-Fail, critical, or guest VLANs. The user aging timer for a type of 802.1X VLAN determines how long a user can stay in that type of VLAN.

For more information about how user aging operates, see the usage guidelines on the dot1x unauthenticated-user aging enable command.

For a user aging timer to take effect, do not set it to a multiple of the username request timeout timer (the dot1x timer tx-period command).

A user aging timer change takes effect immediately.

Examples

# Set the user aging timer to 150 seconds for 802.1X critical VLANs.

<Sysname> system-view

[Sysname] dot1x timer user-aging critical-vlan 150

Related commands

display dot1x

dot1x unauthenticated-user aging enable

# New feature: Configuring MAC authentication unauthenticated user aging

## Configuring user aging for unauthenticated MAC authentication users

#### About user aging for unauthenticated MAC authentication users

User aging for unauthenticated MAC authentication users applies to users added to a MAC authentication guest or critical VLAN because they have not been authenticated or have failed authentication.

When a user in one of those VLANs ages out, the device removes the user from the VLAN and deletes the MAC address entry for the user from the access port.

For users in one of those VLANs on one port to be authenticated successfully and come online on another port, enable this feature. In any other scenarios, disable this feature as a best practice.

#### Restrictions and guidelines

As a best practice, use this feature on a port only if you want to have its unauthenticated users to be authenticated and come online on a different port.

#### Procedure

Enter system view.

system-view

Set the user aging timer for a type of MAC authentication VLAN.

mac-authentication timer user-aging { critical-vlan | guest-vlan } aging-time-value

By default, the user aging timer is 1000 seconds for all applicable types of MAC authentication VLANs.

Enter interface view.

interface interface-type interface-number

Enable user aging for unauthenticated MAC authentication users.

mac-authentication unauthenticated-user aging enable

By default, user aging is enabled for unauthenticated MAC authentication users.

## Command reference

### mac-authentication unauthenticated-user aging enable

Use mac-authentication unauthenticated-user aging enable to enable user aging for unauthenticated MAC authentication users.

Use undo mac-authentication unauthenticated-user aging enable to disable user aging for unauthenticated MAC authentication users.

Syntax

mac-authentication unauthenticated-user aging enable

undo mac-authentication unauthenticated-user aging enable

Default

User aging is enabled for unauthenticated MAC authentication users.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

User aging for unauthenticated MAC authentication users applies to users added to a MAC authentication guest or critical VLAN because they have not been authenticated or have failed authentication.

When a user in one of those VLANs ages out, the device removes the user from the VLAN and deletes the MAC address entry for the user from the access port.

For users in one of those VLANs on one port to be authenticated successfully and come online on another port, enable this feature. In any other scenarios, disable this feature as a best practice.

Examples

# Disable user aging for unauthenticated MAC authentication users on .

<Sysname> system-view

[Sysname] interface

[Sysname-] undo mac-authentication unauthenticated-user aging enable

Related commands

mac-authentication timer

### mac-authentication timer user-aging

Use mac-authentication timer user-aging to set the user aging timer for a type of MAC authentication VLAN.

Use undo mac-authentication timer user-aging to restore the default setting of the user aging timer for a type of MAC authentication VLAN.

Syntax

mac-authentication timer user-aging { critical-vlan | guest-vlan } aging-time-value

undo mac-authentication timer user-aging { critical-vlan | guest-vlan }

Default

The user aging timer is 1000 seconds for all applicable types of MAC authentication VLANs.

Views

System view

Predefined user roles

network-admin

Parameters

user-aging: Sets the user aging timer for a type of MAC authentication VLAN.

critical-vlan: Specifies MAC authentication critical VLANs.

guest-vlan: Specifies MAC authentication guest VLANs.

aging-time-value: Sets the user aging timer. The value range is 60 to 2147483647 seconds.

Usage guidelines

If you enable user aging for unthenticated MAC authentication user, you can set a user aging timer for MAC authentication critical or guest VLANs. The user aging timer for a type of MAC authentication VLAN determines how long a user can stay in that type of VLAN.

For more information about how user aging operates, see the usage guidelines for the mac-authentication unauthenticated-user aging enable command.

Do not set the user aging timer for users in MAC authentication guest VLANs to a multiple of the authentication interval for them. If you do so, the aging timer will not take effect. The authentication interval for MAC authentication users in a guest VLAN is configurable with the mac-authentication guest-vlan auth-period command.

A user aging timer change takes effect immediately.

Examples

# Set the user aging timer to 150 seconds for MAC authentication critical VLANs.

<Sysname> system-view

[Sysname] mac-authentication timer user-aging critical-vlan 150

Related commands

display mac-authentication

mac-authentication unauthenticated-user aging enable

# New feature: VLAN check bypass for the port security MAC move feature

## Enabling VLAN check bypass for the port security MAC move feature

#### About VLAN check bypass

VLAN check bypass enables a port to ignore the VLAN information in the packets that trigger 802.1X or MAC reauthentication for MAC move users.

The port from which the user moves is called the source port and the port to which the user moves is called the destination port.

On the destination port, an 802.1X or MAC authentication user will be reauthenticated in the VLAN authorized on the source port if the source port is enabled with MAC-based VLAN. If that VLAN is not permitted to pass through on the destination port, reauthentication will fail. To avoid this situation, enable VLAN check bypass on the destination port.

#### Restrictions and guidelines

When you configure VLAN check bypass for users moving between ports, follow these guidelines:

* To ensure a successful reauthentication, enable VLAN check bypass on a destination port if the source port is enabled with MAC-based VLAN.
* If the destination port is an 802.1X-enabled trunk port, you must configure it to send 802.1X protocol packets without VLAN tags. For more information, see 802.1X configuration in Security Configuration Guide.

#### Prerequisites

For VLAN check bypass to take effect, you must enable port security MAC move.

#### Procedure

Enter system view.

system-view

Enable VLAN check bypass for users moving between ports.

Enter interface view.

interface interface-type interface-number

Enable VLAN check bypass for users moving to the port from other ports.

port-security mac-move bypass-vlan-check

By default, the VLAN check bypass feature is disabled for users moving to a port from other ports.

## Command reference

### port-security mac-move bypass-vlan-check

Use port-security mac-move bypass-vlan-check to enable VLAN check bypass for users moving to a port from other ports.

Use undo port-security mac-move bypass-vlan-check to disable VLAN check bypass for users moving to a port from other ports.

Syntax

port-security mac-move bypass-vlan-check

undo port-security mac-move bypass-vlan-check

Default

VLAN check bypass is disabled for users moving to a port from other ports. When reauthenticating a user that has moved to the port, the device examines whether the VLAN to which the user belongs is permitted by the port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

VLAN check bypass skips checking VLAN information in the packets that trigger 802.1X or MAC reauthentication for users moving to the port from other ports.

On the destination port, an 802.1X or MAC authentication user will be reauthenticated in the VLAN authorized on the source port if the source port is enabled with MAC-based VLAN. If that VLAN is not permitted to pass through on the destination port, reauthentication will fail. To avoid this situation, enable VLAN check bypass on the destination port.

When you configure VLAN check bypass, follow these guidelines:

* To ensure a successful reauthentication, enable VLAN check bypass on a destination port if the source port is enabled with MAC-based VLAN.
* If the destination port is an 802.1X-enabled trunk port, you must configure it to send 802.1X protocol packets without VLAN tags.

Examples

# Enable VLAN check bypass for users moving to from other ports.

<Sysname> system-view

[Sysname] interface

[Sysname-] port-security mac-move bypass-vlan-check

Related commands

display port-security

dot1x eapol untag

port-security mac-move permit

# New feature: Strict intrusion protection

## Configuring strict intrusion protection

#### About strict intrusion protection

Strict intrusion protection allows the device to permanently or temporarily shut down a port if the port receives a frame that meets the following requirements: The source MAC address of the frame has been added to the secure MAC address table on another port in the same VLAN.

#### Restrictions and guidelines

Strict intrusion protection takes effect only when the intrusion protection action is disableport or disableport-temporarily. When strict intrusion protection is enabled on a port, you cannot change the intrusion protection action to blockmac on that port. To change the intrusion protection action to blockmac, you must first disable strict intrusion protection on that port.

#### Procedure

Enter system view.

system-view

Enter interface view.

interface interface-type interface-number

Enable strict intrusion protection.

port-security strict-intrusion-protection enable

By default, strict intrusion protection is disabled.

## Command reference

### port-security strict-intrusion-protection enable

Use port-security strict-intrusion-protection enable to enable strict intrusion protection.

Use undo port-security strict-intrusion-protection enable to disable strict intrusion protection.

Syntax

port-security strict-intrusion-protection enable

undo port-security strict-intrusion-protection enable

Default

Strict intrusion protection is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

Strict intrusion protection allows the device to permanently or temporarily shut down a port if the port receives a frame that meets the following requirements: The source MAC address of the frame has been added to the secure MAC address table on another port in the same VLAN.

Strict intrusion protection takes effect only when the intrusion protection action is disableport or disableport-temporarily.

Examples

# Enable strict intrusion protection on .

<Sysname> system-view

[Sysname] interface

[Sysname-] port-security strict-intrusion-protection enable

Related commands

port-security intrusion-mode

port-security port-mode

# New feature: Specifying the source IP address for outgoing SCP packets

## Specifying the source IP address for outgoing SCP packets

#### About specifying the source IP address for outgoing SCP packets

After you specify the source IP address for outgoing SCP packets on an SCP client, the client uses the specified IP address to communicate with the SCP server.

#### Restrictions and guidelines

As a best practice, specify the IP address of a loopback interface as the source address of outgoing SCP packets for the following purposes:

* Ensuring the communication between the SCP client and the SCP server.
* Improving the manageability of SCP clients in authentication service.

#### Procedure

Enter system view.

system-view

Specify the source address for outgoing SCP packets.

IPv4:

scp client source { interface interface-type interface-number | ip ip-address }

By default, an SCP client uses the primary IPv4 address of the output interface in the matching route as the source address of the outgoing SCP packets.

IPv6:

scp client ipv6 source { interface interface-type interface-number | ipv6 ipv6-address }

By default, an SCP client automatically selects an IPv6 address as the source address of the outgoing packets in compliance with RFC 3484.

## Command reference

### scp client ipv6 source

Use scp client ipv6 source to configure the source IPv6 address for SCP packets that are sent by the SCP client.

Use undo scp client ipv6 source to restore the default.

Syntax

scp client ipv6 source { interface interface-type interface-number | ipv6 ipv6-address }

undo scp client ipv6 source

Default

The source IPv6 address for outgoing SCP packets is not configured. The SCP client automatically selects an IPv6 address for outgoing SCP packets in compliance with RFC 3484.

Views

System view

Predefined user roles

network-admin

Parameters

interface interface-type interface-number: Specifies a source interface by its type and number. The SCP client selects the interface's address that most specifically matches the destination address of outgoing SCP packets as the source address of the SCP packets.

ipv6 ipv6-address: Specifies a source IPv6 address.

Usage guidelines

This command takes effect on all IPv6 SCP connections. The source IPv6 address specified in the scp ipv6 command takes effect only on the current IPv6 SCP connection. If you specify the source IPv6 address in both this command and the scp ipv6 command, the source IPv6 address specified in the scp ipv6 command takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

# Specify 2:2::2:2 as the source IPv6 address for SCP packets.

<Sysname> system-view

[Sysname] scp client ipv6 source ipv6 2:2::2:2

Related commands

display scp client source

### scp client source

Use scp client source to configure the source IPv4 address for SCP packets that are sent by the SCP client.

Use undo scp client source to restore the default.

Syntax

scp client source { interface interface-type interface-number | ip ip-address }

undo scp client source

Default

The source IPv4 address for outgoing SCP packets is not configured. The SCP client uses the primary IPv4 address of the output interface in the matching route as the source IPv4 address for outgoing SCP packets.

Views

System view

Predefined user roles

network-admin

Parameters

interface interface-type interface-number: Specifies a source interface by its type and number. The SCP client uses the primary IPv4 address of the interface as the source address of outgoing SCP packets.

ip ip-address: Specifies a source IPv4 address.

Usage guidelines

This command takes effect on all SCP connections. The source IPv4 address specified in the scp command takes effect only on the current SCP connection. If you specify the source IPv4 address in both this command and the scp command, the source IPv4 address specified in the scp command takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

# Specify 192.168.0.1 as the source IPv4 address for SCP packets.

<Sysname> system-view

[Sysname] scp client source ip 192.168.0.1

Related commands

display scp client source

# New feature: gRPC

## About gRPC

gRPC is an open source remote procedure call (RPC) system initially developed at Google. It uses HTTP 2.0 for transport and provides network device configuration and management methods that support multiple programming languages.

### gRPC protocol stack layers

Table 6 describes the gRPC protocol stack layers.

gRPC protocol stack layers

| Layer | Description |
| --- | --- |
| Content layer | Defines the data of the service module.  Two peers must notify each other of the data models that they are using. |
| Protocol buffer encoding layer | Encodes data by using the protocol buffer code format. |
| gRPC layer | Defines the protocol interaction format for remote procedure calls. |
| HTTP 2.0 layer | Carries gRPC. |
| TCP layer | Provides connection-oriented reliable data links. |

### Network architecture

As shown in Figure 2, the gRPC network uses the client/server model. It uses HTTP 2.0 for packet transport.

gRPC network architecture



The gRPC network uses the following mechanism:

The gRPC server listens to connection requests from clients at the gRPC service port.

A user runs the gRPC client application to log in to the gRPC server, and uses methods provided in the .proto file to send requests.

The gRPC server responds to requests from the gRPC client.

The device can act as the gRPC server or client.

### Telemetry technology based on gRPC

Telemetry is a remote data collection technology for monitoring device performance and operating status. HPE telemetry technology uses gRPC to push data from the device to the collectors on the NMSs. As shown in Figure 3, after a gRPC connection is established between the device and NMSs, the NMSs can subscribe to data of modules on the device.

Telemetry technology based on gRPC



### Telemetry modes

The device supports the following telemetry modes:

* Dial-in mode—The device acts as a gRPC server and the collectors act as gRPC clients. A collector initiates a gRPC connection to the device to subscribe to device data.

Dial-in mode applies to small networks where collectors need to deploy configurations to devices.

* Dial-out mode—The device acts as a gRPC client and the collectors act as gRPC servers. The device initiates a gRPC connection to the collectors and pushes subscribed device data to the collectors.

Dial-out mode applies to larger networks where devices need to push device data to collectors.

### Protocols

RFC 7540, Hypertext Transfer Protocol version 2 (HTTP/2)

## FIPS compliance

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see Security Configuration Guide.

gRPC is not supported in FIPS mode.

## Configuring the gRPC dial-in mode

### gRPC dial-in mode configuration tasks at a glance

To configure the gRPC dial-in mode, perform the following tasks:

Configuring the gRPC service

Configuring a gRPC user

### Configuring the gRPC service

#### Restrictions and guidelines

If the gRPC service fails to be enabled, use the display tcp or display ipv6 tcp command to verify whether the gRPC service port number has been used by another feature. If yes, specify a free port as the gRPC service port number and try to enable the gRPC service again. For more information about the display tcp and display ipv6 tcp commands, see Layer 3—IP Services Command Reference.

#### Procedure

Enter system view.

system-view

(Optional.) Set the gRPC service port number.

grpc port port-number

By default, the gRPC service port number is 50051.

Enable the gRPC service.

grpc enable

By default, the gRPC service is disabled.

(Optional.) Set the gRPC session idle timeout timer.

grpc idle-timeout minutes

By default, the gRPC session idle timeout timer is 5 minutes.

### Configuring a gRPC user

#### About gRPC users

For gRPC clients to establish gRPC sessions with the device, you must configure local users for the gRPC clients.

#### Procedure

Enter system view.

system-view

Add a local user with the device management right.

local-user user-name [ class manage ]

Configure a password for the user.

password [ { hash | simple } password ]

By default, no password is configured for a local user. A non-password-protected user can pass authentication after providing the correct username and passing attribute checks.

Assign user role network-admin to the user.

authorization-attribute user-role user-role

By default, a local user is assigned the network-operator role.

Authorize the user to use the HTTPS service.

service-type https

By default, no service types are authorized to a local user.

For more information about the local-user, password, authorization-attribute, and service-type commands, see AAA configuration in Security Command Reference.

## Configuring the gRPC dial-out mode

### gRPC dial-out mode configuration tasks at a glance

To configure the gRPC dial-out mode, perform the following tasks:

Enabling the gRPC service

Configuring sensors

Configuring collectors

Configuring a subscription

### Enabling the gRPC service

Enter system view.

system-view

Enable the gRPC service.

grpc enable

By default, the gRPC service is disabled.

### Configuring sensors

#### About sensors

The device uses sensors to sample data. A sensor path indicates a data source.

Supported data sampling types include:

* Event-triggered sampling—Sensors in a sensor group sample data when certain events occur. For sensor paths of this data sampling type, see NETCONF XML API Event Reference for the module.
* Periodic sampling—Sensors in a sensor group sample data at intervals. For sensor paths of this data sampling type, see the NETCONF XML API references for the module except for NETCONF XML API Event Reference.

#### Procedure

Enter system view.

system-view

Enter telemetry view.

telemetry

Create a sensor group and enter sensor group view.

sensor-group group-name

Specify a sensor path.

sensor path path

To specify multiple sensor paths, execute this command multiple times.

### Configuring collectors

#### About collectors

Collectors are used to receive sampled data from network devices. For the device to communicate with collectors, you must create a destination group and add collectors to the destination group.

#### Restrictions and guidelines

As a best practice, configure a maximum of five destination groups. If you configure too many destination groups, system performance might degrade.

#### Procedure

Enter system view.

system-view

Enter telemetry view.

telemetry

Create a destination group and enter destination group view.

destination-group group-name

Specify a collector.

IPv4:

ipv4-address ipv4-address [ port port-number ]

IPv6:

ipv6-address ipv6-address [ port port-number ]

To specify multiple collectors, execute this command multiple times. One collector must have a different address, port.

### Configuring a subscription

#### About configuring a subscription

A subscription binds sensor groups to destination groups. Then, the device pushes data from the specified sensors to the collectors.

#### Procedure

Enter system view.

system-view

Enter telemetry view.

telemetry

Create a subscription and enter subscription view.

subscription subscription-name

(Optional.) Specify the source IP address for packets sent to collectors.

source-address { ipv4-address | interface interface-type interface-number | ipv6 ipv6-address }

By default, the device uses the primary IPv4 address of the output interface for the route to the collectors as the source address.

Changing the source IP address for packets sent to collectors causes the device to re-establish the connection to the gRPC server.

Specify a sensor group.

sensor-group group-name [ sample-interval interval ]

Specify the sample-interval interval option for periodic sensor paths and only for periodic sensor paths.

* + If you specify the option for event-triggered sensor paths, the sensor paths do not take effect.
  + If you do not specify the option for periodic sensor paths, the device does not sample or push data.

Specify a destination group.

destination-group group-name

## Display and maintenance commands for gRPC

Execute display commands in any view.

| Task | Command |
| --- | --- |
| Display gRPC information in dial-in mode. | display grpc |

## gRPC configuration examples

These configuration examples describe only CLI configuration tasks on the device. The collectors need to run an extra application.

### Example: Configuring the gRPC dial-in mode

#### Network configuration

As shown in Figure 4, configure the gRPC dial-in mode on the device so the device acts as the gRPC server and the gRPC client can subscribe to LLDP events on the device.

Network diagram



#### Procedure

Assign IP addresses to interfaces on the gRPC server and client and configure routes. Make sure the server and client can reach each other.

Configure the device as the gRPC server:

# Enable the gRPC service.

<Device> system-view

[Device] grpc enable

# Create a local user named test. Set the password to test, and assign user role network-admin and the HTTPS service to the user.

[Device] local-user test

[Device-luser-manage-test] password simple test

[Device-luser-manage-test] authorization-attribute user-role network-admin

[Device-luser-manage-test] service-type https

[Device-luser-manage-test] quit

Configure the gRPC client.

Prepare a PC and install the gRPC environment on the PC. For more information, see the user guide for the gRPC environment.

Obtain the HPE proto definition file and uses the protocol buffer compiler to generate code of a specific language, for example, Java, Python, C/C++, or Go.

Create a client application to call the generated code.

Start the application to log in to the gRPC server.

#### Verifying the configuration

When an LLDP event occurs on the gRPC server, verify that the gRPC client receives the event.

### Example: Configuring the gRPC dial-out mode

#### Network configuration

As shown in Figure 5, the device is connected to a collector. The collector uses port 50050.

Configure gRPC dial-out mode on the device so the device pushes the device capability information of its interface module to the collector at 10-second intervals.

Network diagram



#### Procedure

# Configure IP addresses as required so the device and the collector can reach each other. (Details not shown.)

# Enable the gRPC service.

<Device> system-view

[Device] grpc enable

# Create a sensor group named test, and add sensor path ifmgr/devicecapabilities/.

[Device] telemetry

[Device-telemetry] sensor-group test

[Device-telemetry-sensor-group-test] sensor path ifmgr/devicecapabilities/

[Device-telemetry-sensor-group-test] quit

# Create a destination group named collector1. Specify a collector that uses IPv4 address 192.168.2.1 and port number 50050.

[Device-telemetry] destination-group collector1

[Device-telemetry-destination-group-collector1] ipv4-address 192.168.2.1 port 50050

[Device-telemetry-destination-group-collector1] quit

# Configure a subscription named A to bind sensor group test with destination group collector1. Set the sampling interval to 10 seconds.

[Device-telemetry] subscription A

[Device-telemetry-subscription-A] sensor-group test sample-interval 10

[Device-telemetry-subscription-A] destination-group collector1

[Device-telemetry-subscription-A] quit

#### Verifying the configuration

# Verify that the collector receives the device capability information of the interface module from the device at 10-second intervals. (Details not shown.)

## gRPC dial-in mode commands

### display grpc

Use display grpc to display gRPC dial-in mode information.

Syntax

display grpc

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

# Display gRPC dial-in mode information.

<Sysname> display grpc

gRPC status : enabled.

gRPC port : 50051

gRPC idle-timeout : 3 minutes

Session count: 1.

Session ID: 1

User name: test

Login time:2018-01-05 06:46:43 Idle time : 2 mins 56 s

Client IP address : 169.254.100.170:40810

Received RPCs : 0 Received error RPCs : 0

Received subscription: 0 Output notifications: 0

Command output

| Field | Description |
| --- | --- |
| gRPC status | Status of the gRPC service:   * + - * enabled—The gRPC service is enabled.       * disabled—The gRPC service is disabled. |
| gRPC idle-timeout | Setting for the gRPC session idle timeout timer. |
| Session count | Number of gRPC sessions. |
| Idle time | Duration in which the session idle timeout timer will expire. If the value of this field is 0, gRPC sessions will never be timed out. |
| Received error RPCs | Number of received erroneous gRPC requests. |
| Received subscription | Number of received gRPC subscription requests. |

### grpc enable

Use grpc enable to enable the gRPC service.

Use undo grpc enable to disable the gRPC service.

Syntax

grpc enable

undo grpc enable

Default

The gRPC service is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

If this command fails, use the display tcp or display ipv6 tcp command to verify whether the gRPC service port number has been used by another feature. If yes, specify a free port as the gRPC service port number and try to enable the gRPC service again.

Examples

# Enable the gRPC service.

<Sysname> system

[Sysname] grpc enable

Related commands

display ipv6 tcp (Layer 3—IP Services Command Reference)

display tcp (Layer 3—IP Services Command Reference)

grpc port

### grpc idle-timeout

Use grpc idle-timeout to set the gRPC session idle timeout timer.

Use undo grpc idle-timeout to restore the default.

Syntax

grpc idle-timeout minutes

undo grpc idle-timeout

Default

The gRPC session idle timeout timer is 5 minutes.

Views

System view

Predefined user roles

network-admin

Parameters

minutes: Specifies the gRPC session idle timeout timer in minutes, in the range of 0 to 30. To disable gRPC sessions from being timed out, set it to 0.

Usage guidelines

If no gRPC packet exchanges occur on the session between a gRPC and the server before the idle timeout timer expires, the device closes the session.

Examples

# Set the gRPC session idle timeout timer to 6 minutes.

<Sysname> system

[Sysname] grpc idle-timeout 6

### grpc port

Use grpc port to specify the gRPC service port number.

Use undo grpc port to restore the default.

Syntax

grpc port port-number

undo grpc port

Default

The gRPC service port number is 50051.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies the gRPC service port number, in the range of 1 to 65535.

Usage guidelines

You can configure this command only when the gRPC service is disabled.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

# Set the gRPC service port number to 50052.

<Sysname> system

[Sysname] grpc port 50052

Related commands

grpc enable

## gRPC dial-out mode commands

### destination-group (subscription view)

Use destination-group to specify a destination group for a subscription.

Use undo destination-group to remove a destination group from a subscription.

Syntax

destination-group group-name

undo destination-group group-name

Default

A subscription does not have a destination group.

Views

Subscription view

Predefined user roles

network-admin

Parameters

group-name: Specifies a destination group by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

A subscription binds sensor groups to destination groups. Then, the device pushes data from the specified sensors to the collectors.

The specified destination group must have been created by using the destination-group command in telemetry view.

You can specify a maximum of five destination groups for a subscription.

Examples

# Specify destination group collector1 for subscription A.

<Sysname> system-view

[Sysname] telemetry

[Sysname-telemetry] subscription A

[Sysname-telemetry-subscription-A] destination-group collector1

Related commands

destination-group (telemetry view)

### destination-group (telemetry view)

Use destination-group to create a destination group and enter its view, or enter the view of an existing destination group.

Use undo destination-group to delete a destination group.

Syntax

destination-group group-name

undo destination-group group-name

Default

No destination groups exist.

Views

Telemetry view

Predefined user roles

network-admin

Parameters

group-name: Specifies the destination group name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

As a best practice, configure a maximum of five destination groups. If you configure too many destination groups, system performance might degrade.

Examples

# Create a destination group named collector1.

<Sysname> system-view

[Sysname] telemetry

[Sysname-telemetry] destination-group collector1

[Sysname-telemetry-destination-group-collector1]

### ipv4-address

Use ipv4-address to add an IPv4 collector to a destination group.

Use undo ipv4-address to remove an IPv4 collector from a destination group.

Syntax

ipv4-address ipv4-address [ port port-number ]

undo ipv4-address ipv4-address [ port port-number ]

Default

A destination group does not have IPv4 collectors.

Views

Destination group view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies the IPv4 address of the collector.

port port-number: Specifies the listening port of the collector, in the range of 1 to 65535. The default is 50051.

Usage guidelines

To add multiple collectors to a destination group, execute this command multiple times.

One collector must have a different address or port than the other collectors.

You can specify a maximum of five collectors for a destination group.

Examples

# Add a collector that uses IPv4 address 192.168.21.21 and the default port number to destination group collector1.

<Sysname> system-view

[Sysname] telemetry

[Sysname-telemetry] destination-group collector1

[Sysname-telemetry-destination-group-collector1] ipv4-address 192.168.21.21

Related commands

destination-group (telemetry view)

### ipv6-address

Use ipv6-address to add an IPv6 collector to a destination group.

Use undo ipv6-address to remove an IPv6 collector from a destination group.

Syntax

ipv6-address ipv6-address [ port port-number ]

undo ipv6-address ipv6-address [ port port-number ]

Default

A destination group does not have IPv6 collectors.

Views

Destination group view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address of the collector.

port port-number: Specifies the listening port of the collector, in the range of 1 to 65535. The default is 50051.

Usage guidelines

To add multiple collectors to a destination group, execute this command multiple times.

One collector must have a different address or port than the other collectors.

You can specify a maximum of five collectors for a destination group.

Examples

# Add a collector that uses IPv6 address 1: : 1 and the default port number to destination group collector1.

<Sysname> system-view

[Sysname] telemetry

[Sysname-telemetry] destination-group collector1

[Sysname-telemetry-destination-group-collector1] ipv6-address 1: : 1

Related commands

destination-group (telemetry view)

### sensor path

Use sensor path to configure a sensor path.

Use undo sensor path to delete a sensor path.

Syntax

sensor path path

undo sensor path path

Default

No sensor paths exist.

Views

Sensor group view

Predefined user roles

network-admin

Parameters

path: Specifies a data path. For information about the available paths, enter a question mark (?) in the position of this argument.

Usage guidelines

To configure multiple sensor paths, execute this command multiple times.

The device supports a maximum of 128 sensor paths.

If the device does not support the specified sensor path, the command displays an error message.

Examples

# Configure sensor path ifmgr/devicecapabilities/ for sensor group test.

<Sysname> system-view

[Sysname] telemetry

[Sysname-telemetry] sensor-group test

[Sysname-telemetry-sensor-group-test] sensor path ifmgr/devicecapabilities/

Related commands

sensor-group (telemetry view)

### sensor-group (subscription view)

Use sensor-group to specify a sensor group for a subscription.

Use undo sensor-group to remove a sensor group from a subscription.

Syntax

sensor-group group-name [ sample-interval interval ]

undo sensor-group group-name

Default

A subscription does not have a sensor group.

Views

Subscription view

Predefined user roles

network-admin

Parameters

group-name: Specifies a sensor group by its name, a case-sensitive string of 1 to 31 characters.

sample-interval interval: Specifies the data sampling interval in seconds. The value range is 1 to 86400.

Usage guidelines

Specify the sample-interval interval option for periodic sensor paths and only for periodic sensor paths.

* If you specify the option for event-triggered sensor paths, the sensor paths do not take effect.
* If you do not specify the option for periodic sensor paths, the device does not sample or push data.

The specified sensor group must have been created by using the sensor-group command in telemetry view.

Examples

# Specify sensor group test for subscription A. Set the data sampling interval to 10 seconds.

<Sysname> system-view

[Sysname] telemetry

[Device-telemetry] subscription A

[Device-telemetry-subscription-A] sensor-group test sample-interval 10

Related commands

sensor path

sensor-group (telemetry view)

### sensor-group (telemetry view)

Use sensor-group to create a sensor group and enter its view, or enter the view of an existing sensor group.

Use undo sensor-group to delete a sensor group.

Syntax

sensor-group group-name

undo sensor-group group-name

Default

No sensor groups exist.

Views

Telemetry view

Predefined user roles

network-admin

Parameters

group-name: Specifies the sensor group name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

The device supports a maximum of 32 sensor groups.

Examples

# Create a sensor group named test.

<Sysname> system-view

[Sysname] telemetry

[Sysname-telemetry] sensor-group test

[Sysname-telemetry-sensor-group-test]

### source-address

Use source-address to specify the source IP address for packets sent to collectors.

Use undo source-address to restore the default.

Syntax

source-address { ipv4-address | interface interface-type interface-number | ipv6 ipv6-address }

undo source-address

Default

The device uses the primary IPv4 address of the output interface for the route to the collectors as the source address.

Views

Subscription view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies an IPv4 address.

interface interface-type interface-number: Specifies an interface by its type and number. In the current software version, you must specify a loopback interface. The device will use the interface's primary IPv4 address as the source address. If the interface does not have a primary IPv4 address, the device uses the primary IPv4 address of the output interface for the route to the collectors.

ipv6 ipv6-address: Specifies an IPv6 address.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Changing the source IP address for packets sent to collectors causes the device to re-establish the connection to the gRPC server.

Examples

# Specify the source IPv4 address of 169.254.1.1 for packets sent to collectors.

<Sysname> system-view

[Sysname] telemetry

[Sysname-telemetry] subscription A

[Sysname-telemetry-subscription-A] source-address 169.254.1.1

### subscription

Use subscription to create a subscription and enter its view, or enter the view of an existing subscription.

Use undo sensor-group to delete a subscription.

Syntax

subscription subscription-name

undo subscription subscription-name

Default

No subscription groups exist.

Views

Telemetry view

Predefined user roles

network-admin

Parameters

subscription-name: Specifies the subscription name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

The device supports a maximum of 10 subscriptions.

Examples

# Configure a subscription named A.

<Sysname> system-view

[Sysname] telemetry

[Sysname-telemetry] subscription A

[Sysname-telemetry-subscription-A]

Related commands

destination-group (subscription view)

sensor-group (subscription view)

### telemetry

Use telemetry to enter telemetry view.

Syntax

telemetry

Views

System view

Predefined user roles

network-admin

Usage guidelines

In telemetry view, you can configure telemetry parameters.

Examples

# Enter telemetry view.

<Sysname> system-view

[Sysname] telemetry

[Sysname-telemetry]

# Modified feature: Specifying the HTTPS redirect listening port number

## Feature change description

The default setting for the HTTPS redirect listening port number was changed.

## Command changes

### Modified command: http-redirect https-port

Syntax

http-redirect https-port port-number

undo http-redirect https-port

Views

System view

Change description

Before modification: By default, the HTTPS redirect listening port number is not specified.

After modification: By default, the HTTPS redirect listening port number is 6654.

# Modified feature: Specifying startup images

## Feature change description

In addition to boot, system, feature images, you can specify patch images when you specify startup images.

## Command changes

### Modified command: boot-loader file

Old syntax

boot-loader file boot filename system filename [ feature filename&<1-30> ] { all | slot slot-number } { backup | main }

boot-loader file ipe-filename { all | slot slot-number } { backup | main }

New syntax

boot-loader file boot filename system filename [ feature filename&<1-30> ] [ patch filename&<1-16> ] { all | slot slot-number } { backup | main }

boot-loader file ipe-filename [ patch filename&<1-16> ] { all | slot slot-number } { backup | main }

Views

User view

Change description

Before modification: The command does not support the patch filename&<1-16> option.

After modification: The command supports the patch filename&<1-16> option.

# Modified feature: Automatic configuration

## Feature change description

Before modification: To verify automatization configuration, you must examine the configuration file.

After modification: You can verify automatization configuration also by observing the system status LED. After the device starts up correctly, its system status LED turns steady green. After the device starts automatic configuration, its system status LED flashes green. After the device finishes automatic configuration, its system status LED turns steady green again.

## Command changes

None.

# Modified feature: Displaying ARP snooping entries

## Feature change description

The syntax of the command to display ARP snooping entries was changed.

## Command changes

### Modified command: display arp snooping

Old syntax

display arp snooping [ vlan vlan-id ] [ slot slot-number ] [ count ]

display arp snooping ip ip-address [ slot slot-number ]

New syntax

display arp snooping vlan [ vlan-id ] [ slot slot-number ] [ count ]

display arp snooping vlan ip ip-address [ slot slot-number ]

Views

Any view

Change description

Before modification: The vlan keyword is optional.

After modification: The vlan keyword is required.

# Modified feature: Clearing ARP snooping entries

## Feature change description

The syntax of the command to clear ARP snooping entries was changed.

## Command changes

### Modified command: reset arp snooping

Old syntax

reset arp snooping [ ip ip-address | vlan vlan-id ]

New syntax

reset arp snooping vlan [vlan-id ]

reset arp snooping vlan ip ip-address

Views

Any view

Change description

Before modification: The vlan keyword is optional.

After modification: The vlan keyword is required.

# Modified feature: Setting the DHCP server response timeout time for DHCP server switchover

## Feature change description

In this release, the value range for DHCP server response timeout time for DHCP server switchover was changed to 1 to 65535 seconds.

## Command changes

### Modified command: dhcp relay dhcp-server timeout

Syntax

dhcp relay dhcp-server timeout time

Default

The DHCP server response timeout time is 30 seconds.

Views

Interface view

Parameters

time: Specifies the DHCP server response timeout time in the range of 1 to 65535 seconds.

Change description

Before modification: The value range for the time argument is 30 to 65535 seconds.

After modification: The value range for the time argument is 1 to 65535 seconds.

### Modified command: dhcp-server timeout

Syntax

dhcp-server timeout time

Default

The DHCP server response timeout time is 30 seconds.

Views

DHCP address pool view

Parameters

time: Specifies the DHCP server response timeout time in the range of 1 to 65535 seconds.

Change description

Before modification: The value range for the time argument is 30 to 65535 seconds.

After modification: The value range for the time argument is 1 to 65535 seconds.

# Modified feature: Automatic configuration

## Feature change description

Before modification: The device supports automatic configuration only on IPv4 networks.

After modification: The device supports automatic configuration on both IPv4 and IPv6 networks.

## Command changes

None.

# Modified feature: Physical type of a combo interface

## Feature change description

In this version and later, the auto keyword is added to the combo enable command. This keyword configures a combo interface to automatically recognize the media inserted and activate the corresponding physical port.

## Command changes

### Modified command: combo enable

Old syntax

combo enable { copper | fiber }

New syntax

combo enable { auto | copper | fiber }

Views

Ethernet interface view

Parameters

auto: Specifies the combo interface to autonegotiate its physical type.

Usage guidelines

When a combo interface acts as an IRF physical interface, you must manually configure the physical type of the combo interface as copper or fiber.

A combo interface in auto mode does not support the duplex half, speed 10, or speed 100 command.

Change description

Before modification:

By default, the copper combo port is activated. You can specify the copper or fiber keyword to activate the copper or fiber combo port as needed.

After modification:

By default, a combo interface autonegotiates its physical type. When a combo autonegotiates its physical type, the actual physical type depends on the connected media:

* When the copper combo port is not connected to a twisted-pair cable and the fiber combo port has a transceiver module installed, the fiber combo port is activated.
* When the copper combo port is connected to a twisted-pair cable and is up:

If you install a transceiver module in the fiber combo port, the copper combo port is still activated before the device is rebooted.

After the device is rebooted, the fiber combo port is activated.

* When the copper combo port is connected to a twisted-pair cable and is down and the fiber combo port has a transceiver module installed, the fiber combo port is activated.
* When the fiber combo port has a transceiver module installed, the fiber combo port is activated even if you connect a twisted-pair cable to the copper combo port.

If you need to specify the physical type of a physical interface according to the network requirements, you can specify the copper or fiber keyword to activate the copper or fiber combo port.

# Modified feature: Physical state change suppression

## Feature change description

In this version and later, the syntax for configuring physical state change suppression on Ethernet interfaces and aggregate interfaces is modified.

## Command changes

### Modified command: link-delay

Old syntax

link-delay [ msec ] delay-time [ mode { up | updown } ]

undo link-delay [ msec ] delay-time [ mode { up | updown } ]

New syntax

link-delay { down | up } [ msec ] delay-time

undo link-delay { down | up }

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Parameters

down: Suppresses link-down events.

up: Suppresses link-up events.

msec: Enables the physical state change suppression interval to be accurate to milliseconds. If you do not specify this keyword, the suppression interval is accurate to seconds.

delay-time: Sets the physical state change suppression interval. A value of 0 means that physical state changes are immediately reported to the CPU and are not suppressed.

* If you do not specify the msec keyword, the physical state change suppression interval is in seconds and the value range is 0 to 30.
* If you specify the msec keyword, the value range is 0 to 10000 milliseconds, and the value must be a multiple of 100.

Change description

Before modification:

* If the mode keyword is not specified, the link-down events are suppressed.
* If the mode up keyword combination is specified, the link-up events are suppressed.
* If the mode updown keyword combination is specified, both link-down and link-up events are suppressed.
* If the suppression interval configured in the command without the mode keyword specified is the same as the suppression interval configured in the command with the mode up keyword combination specified on an interface, the two commands are automatically merged into the command with the mode updown keyword combination specified in the configuration file of the interface.

After modification:

* If the down keyword is not specified, the link-down events are suppressed.
* If the up keyword is specified, the link-up events are suppressed.
* You can set different link state change suppression intervals for link-down events and link-up events.

# Modified feature: MAC-to-VLAN entries

## Feature change description

In this version and later, the keyword for configuring 802.1p priorities in MAC-to-VLAN entries is modified to dot1p.

## Command changes

### Modified command: mac-vlan mac-address

Old syntax

mac-vlan mac-address mac-address [ mask mac-mask ] vlan vlan-id [ dot1q priority ]

New syntax

mac-vlan mac-address mac-address [ mask mac-mask ] vlan vlan-id [ dot1p priority ]

Views

System view

Change description

Before modification: The keyword for configuring 802.1p priorities in MAC-to-VLAN entries is dot1q.

After modification: The keyword for configuring 802.1p priorities in MAC-to-VLAN entries is dot1p.

### Modified command: display mac-vlan

Syntax

display mac-vlan { all | dynamic | mac-address mac-address [ mask mac-mask ] | static | vlan vlan-id }

Views

Any view

Old command output

# Display all MAC-to-VLAN entries.

<Sysname> display mac-vlan all

The following MAC VLAN entries exist:

State: S - Static, D - Dynamic

MAC address Mask VLAN ID Dot1q State

0008-0001-0000 ffff-ff00-0000 5 3 S

0002-0001-0000 ffff-ffff-ffff 5 3 S&D

Total MAC VLAN entries count: 2

New command output

# Display all MAC-to-VLAN entries.

<Sysname> display mac-vlan all

The following MAC VLAN entries exist:

State: S - Static, D - Dynamic

MAC address Mask VLAN ID Dot1p State

0008-0001-0000 ffff-ff00-0000 5 3 S

0002-0001-0000 ffff-ffff-ffff 5 3 S&D

Total MAC VLAN entries count: 2

Change description

Before modification: The field for displaying the 802.1p priority of a VLAN was Dot1q.

After modification: The field for displaying the 802.1p priority of a VLAN was Dot1p.

# Modified feature: Displaying the loop detection configuration and status

## Feature change description

Information about shutdown interfaces was added to the output from the display loopback-detection command.

## Command changes

### Modified command: display loopback-detection

Syntax

display loopback-detection

Views

Any view

Change description

Before modification: If the loop protection action is set to shutdown, this command does not display the interfaces shut down by loop detection.

# Display the loop detection configuration and status.

<Sysname> display loopback-detection

Loopback detection is enabled.

Loopback detection interval is 30 second(s).

Loopback is detected on following interfaces:

No loopback is detected.

After modification: If the loop protection action is set to shutdown, this command displays the interfaces shut down by loop detection.

# Display the loop detection configuration and status.

<Sysname> display loopback-detection

Loop detection is enabled.

Loop detection interval is 30 second(s).

Loop is detected on following interfaces:

Interface Action mode VLANs

GigabitEthernet1/0/1 Shutdown 10

# Modified feature: Setting the 802.1p priority for IGMP messages

## Feature change description

The default 802.1p priority of IGMP messages was changed to 6.

## Command changes

### Modified command: dot1p-priority

Syntax

dot1p-priority priority

undo dot1p-priority

Views

IGMP-snooping view

Change description

Before modification: By default, the 802.1p priority of IGMP messages is not configured. For IGMP messages generated by the device, the 802.1p priority is 0. For IGMP messages forwarded by the device, the 802.1p priority remains unchanged.

After modification: By default, the 802.1p priority of IGMP messages is 6.

### Modified command: igmp-snooping dot1p-priority

Syntax

igmp-snooping dot1p-priority priority

undo igmp-snooping dot1p-priority

Views

VLAN view

Change description

Before modification: By default, the 802.1p priority of IGMP messages is not configured. For IGMP messages generated by the device, the 802.1p priority is 0. For IGMP messages forwarded by the device, the 802.1p priority remains unchanged.

After modification: By default, the 802.1p priority of IGMP messages is 6.

# Modified feature: Setting the 802.1p priority for MLD messages

## Feature change description

The default 802.1p priority of MLD messages was changed to 6.

## Command changes

### Modified command: dot1p-priority

Syntax

dot1p-priority priority

undo dot1p-priority

Views

MLD-snooping view

Change description

Before modification: By default, the 802.1p priority of MLD messages is not configured. For MLD messages generated by the device, the 802.1p priority is 0. For MLD messages forwarded by the device, the 802.1p priority remains unchanged.

After modification: By default, the 802.1p priority of MLD messages is 6.

### Modified command: mld-snooping dot1p-priority

Syntax

mld-snooping dot1p-priority priority

undo mld-snooping dot1p-priority

Views

VLAN view

Change description

Before modification: By default, the 802.1p priority of MLD messages is not configured. For MLD messages generated by the device, the 802.1p priority is 0. For MLD messages forwarded by the device, the 802.1p priority remains unchanged.

After modification: By default, the 802.1p priority of MLD messages is 6.

# Modified feature: Displaying IPv4SG bindings

## Feature change description

The arp-snooping keyword was changed to the arp-snooping-vlan keyword in the command syntax.

## Command changes

### Modified command: display ip source binding

Old syntax

display ip source binding [ static | [ arp-snooping | dhcp-relay | dhcp-server | dhcp-snooping | dot1x ] ] [ ip-address ip-address ] [ mac-address mac-address ] [ vlan vlan-id ] [ interface interface-type interface-number ] [ slot slot-number ]

New syntax

display ip source binding [ static | [ arp-snooping-vlan | dhcp-relay | dhcp-server | dhcp-snooping | dot1x ] ] [ ip-address ip-address ] [ mac-address mac-address ] [ vlan vlan-id ] [ interface interface-type interface-number ] [ slot slot-number ]

Change description

The arp-snooping-vlan keyword replaces the arp-snooping keyword in the command to specify dynamic IPv4SG bindings generated based on ARP snooping.

# Modified feature: Displaying IPv6SG bindings

## Feature change description

The nd-snooping keyword was changed to the nd-snooping-vlan keyword in the command syntax.

## Command changes

### Modified command: display ipv6 source binding

Old syntax

display ipv6 source binding [ static | [ dhcpv6-relay | dhcpv6-snooping | dot1x | nd-snooping ] ] [ ip-address ipv6-address ] [ mac-address mac-address ] [ vlan vlan-id ] [ interface interface-type interface-number ] [ slot slot-number ]

New syntax

display ipv6 source binding [ static | [ dhcpv6-relay | dhcpv6-snooping | dot1x | nd-snooping-vlan ] ] [ ip-address ipv6-address ] [ mac-address mac-address ] [ vlan vlan-id ] [ interface interface-type interface-number ] [ slot slot-number ]

Change description

The nd-snooping-vlan keyword replaces the nd-snooping keyword in the command to specify dynamic IPv4SG bindings generated based on ND snooping.

# Modified feature: Displaying the MFF configuration for a VLAN

## Feature change description

In this release, the display mac-forced-forwarding vlan command does not support displaying the MFF operating mode.

## Command changes

### Modified command: display mac-forced-forwarding vlan

Syntax

display mac-forced-forwarding vlan vlan-id

Views

Any view

Examples

Before modification:

# Display the MFF configuration for VLAN 2.

<Sysname> display mac-forced-forwarding vlan 2

VLAN 2

Mode: Manual/Single

Gateway:

--------------------------------------------------------------------------

192.168.1.42 000f-e200-8046

Server:

--------------------------------------------------------------------------

192.168.1.48 192.168.1.49

Command output

| Field | Description |
| --- | --- |
| VLAN 2 | ID of the VLAN to which the gateways belong. |
| Mode | MFF operating mode:   * + - * Manual (Manual).       * Single-gateway (Single). |
| Gateway | IP and MAC addresses of gateways. If no address is learned, this field displays N/A. |
| Server | Server IP addresses. |

After modification:

# Display the MFF configuration for VLAN 2.

<Sysname> display mac-forced-forwarding vlan 2

VLAN 2

Gateway:

--------------------------------------------------------------------------

192.168.1.42 000f-e200-8046

Server:

--------------------------------------------------------------------------

192.168.1.48 192.168.1.49

Command output

| Field | Description |
| --- | --- |
| VLAN 2 | ID of the VLAN to which the gateways belong. |
| Gateway | IP and MAC addresses of gateways. If no address is learned, this field displays N/A. |
| Server | Server IP addresses. |

Change description

Before modification: The display mac-forced-forwarding vlan command supports displaying the Mode field.

After modification: The display mac-forced-forwarding vlan command does not support displaying the Mode field.

# Modified feature: Associating Track with application modules

## Feature change description

From this release, you cannot configure the notification delay when associating Track with application modules. Creating a track entry associated with an application module enters Track view. You can configure the delay only in Track view for notifying the application module of track entry state changes.

## Command changes

### Modified command: track bfd ctrl

Old syntax

track track-entry-number bfd ctrl [ interface interface-type interface-number ] remote ip remote-ip-address local ip local-ip-address [ delay { negative negative-time | positive positive-time } \* ]

New syntax

track track-entry-number bfd ctrl [ interface interface-type interface-number ] remote ip remote-ip-address local ip local-ip-address

Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

### Modified command: track bfd echo

Old syntax

track track-entry-number bfd echo interface interface-type interface-number remote ip remote-ip-address local ip local-ip-address [ delay { negative negative-time | positive positive-time } \* ]

New syntax

track track-entry-number bfd echo interface interface-type interface-number remote ip remote-ip-address local ip local-ip-address

Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

### Modified command: track cfd

Old syntax

track track-entry-number cfd cc service-instance instance-id mep mep-id [ delay { negative negative-time | positive positive-time } \* ]

New syntax

track track-entry-number cfd cc service-instance instance-id mep mep-id

Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

### Modified command: track interface

Old syntax

track track-entry-number interface interface-type interface-number [ delay { negative negative-time | positive positive-time } \* ]

New syntax

track track-entry-number interface interface-type interface-number

Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

### Modified command: track interface physical

Old syntax

track track-entry-number interface interface-type interface-number physical [ delay { negative negative-time | positive positive-time } \* ]

New syntax

track track-entry-number interface interface-type interface-number physical

Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

### Modified command: track interface protocol

Old syntax

track track-entry-number interface interface-type interface-number protocol { ipv4 | ipv6 } [ delay { negative negative-time | positive positive-time } \* ]

New syntax

track track-entry-number interface interface-type interface-number protocol { ipv4 | ipv6 }

Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

### Modified command: track ip route reachability

Old syntax

track track-entry-number ip route ip-address { mask-length | mask } reachability [ delay { negative negative-time | positive positive-time } \* ]

New syntax

track track-entry-number ip route ip-address { mask-length | mask } reachability

Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

### Modified command: track lldp neighbor

Old syntax

track track-entry-number lldp neighbor interface interface-type interface-number [ delay { negative negative-time | positive positive-time } \* ]

New syntax

track track-entry-number lldp neighbor interface interface-type interface-number

Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

### Modified command: track nqa

Old syntax

track track-entry-number nqa entry admin-name operation-tag reaction item-number [ delay { negative negative-time | positive positive-time } \* ]

New syntax

track track-entry-number nqa entry admin-name operation-tag reaction item-number

Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

# Modified feature: Configuring binding attributes for local users

## Feature change description

As from this version, the device supports configuring binding interfaces for device management users.

## Command changes

### Modified command: bind-attribute

Syntax

bind-attribute { ip ip-address | location interface interface-type interface-number | mac mac-address | vlan vlan-id } \*

Views

Local user view

Change description

Before modification: The location interface interface-type interface-number option is applicable only to LAN and portal users.

After modification: The location interface interface-type interface-number option is applicable to device management users in addition to LAN and portal users.

# Modified feature: Enabling password control

## Feature change description

This release supports enabling password control globally for network access users.

## Command changes

### Modified command: password-control enable

Old syntax

password-control enable

undo password-control enable

New syntax

password-control enable [ network-class ]

undo password-control enable [ network-class ]

Views

System view

Change description

Before modification: You can enable the password control feature globally only for device management users.

After modification: The network-class keyword was added. You can enable the password control feature globally for both device management users and network access users.

# Modified feature: Password management after global password control is enabled

## Feature change description

### Managing local user passwords for device management users

Before modification:

* A password set in plaintext form is stored in ciphertext form, and a password set in hashed form is not stored.
* If a user changes its own password in plaintext form, the new password must have a minimum of four characters different from the current password and any password in the history records. If the user changes its own password in hashed form, the system does not compare the new password with the current password or passwords in the history records.
* If a user deletes its own password, the system does not request the user to enter the current plaintext password.
* In FIPS mode, if a user with the network-admin user role changes its password, the system does not request the user to enter the current plaintext password.

After modification:

* All passwords in the history records are saved in hashed form.
* If a user changes its own password in plaintext form, the system requests the user to enter the current plaintext password. The new password must be different from all passwords in the history records and the current password. In addition, the new password must have a minimum of four characters different from the current password.
* If a user changes the password for another user in plaintext form, the new password must be different from the latter user's all passwords in the history records and current password.
* If a user deletes its own password, the system requests the user to enter the current plaintext password.
* Except the above listed situations, the system does not request a user to enter the current plaintext password or compare the new password with passwords in the history records and the current password.

### Managing super passwords

Before modification:

* If a super new password is set in plaintext form, the password is saved in encrypted form. If a new super password is set in hashed form, the password is not saved.
* If a super password is changed in plaintext form, the new password must have a minimum of four characters different from the current password and any password in the history records. If a super password is changed in hashed form, the system does not compare the new password with the current password and passwords in the history records.

After modification:

* All super passwords in the history records are saved in hashed form.
* If a super password is changed in plaintext form, the new password must be different from all passwords in the history records and the current password. If a super password is changed in hashed form, the system does not compare the new password with the current one and those stored in the history password records.

## Command changes

None.

# Modified feature: Setting the quiet timer for RADIUS servers in a RADIUS scheme

## Feature change description

The minimum value of the quiet time for RADIUS servers was changed from 1 minute to 0 minutes.

## Command changes

### Modified command: timer quiet (RADIUS scheme view)

Syntax

timer quiet minutes

undo timer quiet

Views

RADIUS scheme view

Change description

Before modification: The value range for the minutes argument is 1 to 255, in minutes.

After modification: The value range for the minutes argument is 0 to 255, in minutes. If you set this argument to 0, the device does not change the state of the current server for a user when the server is unreachable. It sends an authentication or accounting request of the user to the next server in active state. For an authentication or accounting request of a new user, it still tries to send the request to the current server because the current server is in active state.

# Modified feature: MAC-based MAC authentication user accounts for MAC authentication

## Feature change description

As from this version, the device allows you to configure a password shared by all MAC-based MAC authentication user accounts.

## Command changes

### Modified command: mac-authentication user-name-format

Old syntax

mac-authentication user-name-format { fixed [ account name ] [ password { cipher | simple } string ] | mac-address [ { with-hyphen | without-hyphen } [ lowercase | uppercase ] ] }

New syntax

mac-authentication user-name-format { fixed [ account name ] | mac-address [ { with-hyphen | without-hyphen } [ lowercase | uppercase ] ] } [ password { cipher | simple } string ]

Views

System view

Change description

Before modification: You cannot specify a password for MAC-based MAC authentication user accounts. The MAC address of each user is used as their password.

After modification: You can specify a password for all MAC-based MAC authentication user accounts by using the password { cipher | simple } string option. If you do not specify a password, each user uses its own MAC address as the password.

# Modified feature: MAC authentication VLAN mode

## Feature change description

As from this version, the port security MAC move feature determines how a port in MAC authentication single-VLAN mode handles an online user with an authorization VLAN when that user moves between VLANs.

Before modification:

In single-VLAN mode, the port does not reauthenticate an online user when traffic from that user contains a VLAN tag different than the VLAN in which the user was authenticated. The user will stay online in the authorization VLAN and cannot access any other VLANs until a logoff occurs.

After modification:

In single-VLAN mode, the port reauthenticates an online user when traffic received from that user contains a VLAN tag different from the VLAN in which the user was authenticated. The authentication process differs depending on the MAC move setting in port security, as follows:

* If MAC move is disabled in port security, the user cannot pass authentication and come online from the new VLAN until after it goes offline from the port.
* If MAC move is enabled in port security, the user can pass authentication on the new VLAN and come online without having to first go offline from the port. After the user passes authentication on the new VLAN, the original authentication session of the user is deleted from the port.

No changes were introduced to the command syntax.

|  |  |
| --- | --- |
|  | NOTE:   * + - * To enable single-VLAN mode, execute the undo form of the mac-authentication host-mode multi-vlan command.       * To enable the port security MAC move feature, use the port-security mac-move permit command. |

# Modified feature: Web authentication

Before modification: Web authentication supports only HTTP redirect. It does not support HTTPS redirect.

After modification: Web authentication supports both HTTP redirect and HTTPS redirect. To enable the device to redirect HTTPS packets in Web authentication, specify the HTTPS redirect listening port number by using the http-redirect https-port command in system view.

# Modified feature: Port security NTK feature

## Feature change description

As from this version, the device supports the ntkauto mode for the need to known (NTK) feature of port security. A port in ntkauto mode forwards only broadcast, multicast, and unicast frames with an authenticated destination MAC address, and only when the port has online users.

## Command changes

### Modified command: port-security ntk-mode

Old syntax

port-security ntk-mode { ntk-withbroadcasts | ntk-withmulticasts | ntkonly }

New syntax

port-security ntk-mode { ntk-withbroadcasts | ntk-withmulticasts | ntkauto | ntkonly }

Views

Layer 2 Ethernet interface view

Change description

Before modification: The ntkauto keyword was not available.

After modification: The ntkauto keyword was added to this command.

# Modified feature: Port security MAC move

## Feature change description

As from this version, the port security MAC move feature takes effect on users that move between VLANs on a port in addition to users that move between ports.

Before modification: Port security MAC move setting takes effect only on users that move between ports on the device.

After modification: Port security MAC move setting also take effect on users that move between VLANs on a port.

* If this feature is disabled, authenticated users must go offline from the original VLAN first before they can be reauthenticated successfully on the new VLAN and come online.
* If this feature is enabled, authenticated users can be reauthenticated successfully on the new VLAN without having to go offline from the original VLAN. The port will remove the users from the original VLAN immediately after the users are reauthenticated successfully on the new VLAN.

No changes were introduced to the command syntax.

|  |  |
| --- | --- |
|  | NOTE:  MAC authentication multi-VLAN mode has higher priority than MAC move for users moving between VLANs on a port. If MAC authentication multi-VLAN mode is enabled, these users can come online in the new VLAN without being reauthenticated. To enable MAC authentication multi-VLAN mode, use the mac-authentication host-mode multi-vlan command. |

# Modified feature: RSA key modulus length used for creating an RSA key pair

## Feature change description

The value range for the key modulus length used for creating an RSA local key pair was changed.

## Command changes

### Modified command: public-key local create

Syntax

In non-FIPS mode:

public-key local create { dsa | ecdsa [ secp192r1 | secp256r1 | secp384r1 | secp521r1 ] | rsa } [ name key-name ]

In FIPS mode:

public-key local create { dsa | ecdsa [ secp256r1 | secp384r1 | secp521r1 ] | rsa } [ name key-name ]

Views

System view

Change description

Before modification:

* In non-FIPS mode, the RSA key modulus length is in the range of 512 to 2048 bits. The default is 1024 bits.
* In FIPS mode, the RSA key modulus length is 2048 bits.

After modification:

* In non-FIPS mode, the RSA key modulus length is in the range of 512 to 4096 bits. The default is 1024 bits.
* In FIPS mode, the RSA key modulus length is a multiple of 256 in the range of 2048 to 4096 bits. The default is 2048 bits.

# Modified feature: RSA key modulus length used for PKI certificate request

## Feature change description

In PKI domain view, the value range for the RSA key modulus length used for certificate request was changed.

## Command changes

### Modified command: public-key rsa

Syntax

public-key rsa { { encryption name encryption-key-name [ length key-length ] | signature name signature-key-name [ length key-length ] } \* | general name key-name [ length key-length ] }

Views

PKI domain view

Change description

Before modification:

* In non-FIPS mode, the RSA key modulus length (key-length) is in the range of 512 to 2048 bits. The default is 1024 bits.
* In FIPS mode, the RSA key modulus length (key-length) is 2048 bits.

After modification:

* In non-FIPS mode, the RSA key modulus length (key-length) is in the range of 512 to 4096 bits. The default is 1024 bits.
* In FIPS mode, the RSA key modulus length (key-length) is a multiple of 256 in the range of 2048 to 4096 bits. The default is 2048 bits.

# Modified feature: SNMP notifications for IKE

## Feature change description

From this version, all SNMP notifications for IKE are disabled by default.

## Command changes

### Modified command: snmp-agent trap enable ike

Syntax

snmp-agent trap enable ike [ attr-not-support | auth-failure | cert-type-unsupport | cert-unavailable | decrypt-failure | encrypt-failure | global | invalid-cert-auth | invalid-cookie | invalid-id | invalid-proposal | invalid-protocol | invalid-sign | no-sa-failure | proposal-add | proposal–delete | tunnel-start | tunnel-stop | unsupport-exch-type ] \*

Views

System view

Change description

Before modification: All SNMP notifications for IKE are enabled by default.

After modification: All SNMP notifications for IKE are disabled by default.

# Modified feature: Configuring an SNMP notification target host

## Feature change description

A DSCP value can be set for SNMP notifications sent to the target host.

## Command changes

### Modified command: snmp-agent target-host

Old syntax

In non-FIPS mode:

snmp-agent target-host inform address udp-domain { ipv4-address | ipv6 ipv6-address } [ udp-port port-number ] params securityname security-string { v2c | v3 [ authentication | privacy ] }

snmp-agent target-host trap address udp-domain { ipv4-address | ipv6 ipv6-address } [ udp-port port-number ] params securityname security-string [ v1 | v2c | v3 [ authentication | privacy ] ]

undo snmp-agent target-host { trap | inform } address udp-domain { ipv4-address | ipv6 ipv6-address } params securityname security-string

In FIPS mode:

snmp-agent target-host inform address udp-domain { ipv4-address | ipv6 ipv6-address } [ udp-port port-number ] params securityname security-string v3 { authentication | privacy }

snmp-agent target-host trap address udp-domain { ipv4-address | ipv6 ipv6-address } [ udp-port port-number ] params securityname security-string v3 { authentication | privacy }

undo snmp-agent target-host { trap | inform } address udp-domain { ipv4-address | ipv6 ipv6-address } params securityname security-string

New syntax

In non-FIPS mode:

snmp-agent target-host inform address udp-domain { ipv4-target-host | ipv6 ipv6-target-host } [ udp-port port-number ] params securityname security-string { v2c | v3 [ authentication | privacy ] }

snmp-agent target-host trap address udp-domain { ipv4-target-host | ipv6 ipv6-target-host } [ udp-port port-number ] [ dscp dscp-value ] params securityname security-string [ v1 | v2c | v3 [ authentication | privacy ] ]

undo snmp-agent target-host { trap | inform } address udp-domain { ipv4-target-host | ipv6 ipv6-target-host } params securityname security-string

In FIPs mode:

snmp-agent target-host inform address udp-domain { ipv4-target-host | ipv6 ipv6-target-host } [ udp-port port-number ] params securityname security-string v3 { authentication | privacy }

snmp-agent target-host trap address udp-domain { ipv4-target-host | ipv6 ipv6-target-host } [ udp-port port-number ] [ dscp dscp-value ] params securityname security-string v3 { authentication | privacy }

undo snmp-agent target-host { trap | inform } address udp-domain { ipv4-target-host | ipv6 ipv6-target-host } params securityname security-string

Default

No SNMP notification target hosts exist.

Views

System view

Parameters

dscp-value: Sets the DSCP value for notifications sent to the target host, in the range of 0 to 63. The default value is 0. A greater DSCP value represents a higher priority. The DSCP value is encapsulated in the ToS field of an IP packet and affects the forwarding priority of the packet.

Change description

The dscp dscp-value option was added to the command.

# Modified feature: Displaying logs buffered over the last specified period of time

## Feature change description

From this release, you can display logs buffered over the last specified period of time.

## Command changes

### Modified command: display logbuffer

Old syntax

display logbuffer [ reverse ] [ level severity | size buffersize | slot slot-number ] \*

New syntax

display logbuffer [ reverse ] [ level severity | size buffersize | slot slot-number ] \* [ last-mins mins ]

Views

Any view

Examples

# Display log buffer information and logs buffered over the last 5 minutes.

<Sysname> display logbuffer last-mins 5

Log buffer: Enabled

Max buffer size: 1024

Actual buffer size: 512

Dropped messages: 0

Overwritten messages: 0

Current messages: 191

%Jan 1 01:00:06:784 2011 Sysname SHELL/6/SHELL\_CMD: -Line=vty0-IPAddr=192.168.1.242-User=\*\*; Command is display current-configuration

%Jan 1 01:03:19:691 2018 Sysname SHELL/5/SHELL\_LOGIN: VTY logged in from 192.168.1.33.

%Jan 1 01:03:21:269 2018 Sysname SHELL/6/SHELL\_CMD: -Line=vty1-IPAddr=192.168.1.33-User=\*\*; Command is display logbuffer last-mins 5

Change description

The last-mins mins option was added to the command.

last-mins mins: Displays logs buffered over the last specified period of time. The mins argument specifies a time period in the range of 1 to 43200 minutes. If you do not specify a time period, the command displays all logs in the log buffer.

# Modified feature: Specifying a log host and its output parameters

## Feature change description

From this release, you can specify the DSCP value in log packets sent to a log host and set the timestamp to be accurate to milliseconds for logs output to log hosts.

## Command changes

### Modified command: info-center loghost

Old syntax

info-center loghost { hostname | ipv4-address | ipv6 ipv6-address } [ port port-number ] [ facility local-number ]

New syntax

info-center loghost { hostname | ipv4-address | ipv6 ipv6-address } [ port port-number ] [ dscp dscp-value ] [ facility local-number ]

Default

No log hosts are specified.

Views

System view

Change description

The dscp dscp-value option was added to the command.

dscp dscp-value: Specifies the DSCP value in log packets sent to the log host. The value range for the dscp-value argument is 0 to 63, and the default is 0. The DSCP value of a packet defines the priority of the packet and affects the transmission priority of the packet. A greater DSCP value represents a higher priority.

### Modified command: info-center timestamp loghost

Old syntax

info-center timestamp loghost { date | iso [ with-timezone ] | no-year-date | none }

undo info-center timestamp loghost

New syntax

info-center timestamp loghost { date [ with-milliseconds ] | iso [ with-milliseconds | with-timezone ] \* | no-year-date | none }

undo info-center timestamp loghost

Views

System view

Change description

The with-milliseconds keyword was added to the command.

with-milliseconds: Sets the timestamp to be accurate to milliseconds for logs output to log hosts in date or ISO 8601 format. The millisecond value is appended to the time information in the timestamp with a dot as the separator. If you do not specify this keyword, the timestamp in date or ISO 8601 format is accurate to seconds.

* Example of a timestamp in date format with millisecond accuracy: Dec 8 10:12:21.708 2018.
* Example of a timestamp in ISO 8601 format with millisecond accuracy: 2018-09-21T15:32:55.708.

# Modified feature: Interface event

## Feature change description

In this version and later, you can specify multiple interfaces of the same type for an interface event.

## Command changes

### Modified command: event interface

Old syntax

event interface interface-type interface-number monitor-obj monitor-obj start-op start-op start-val start-val restart-op restart-op restart-val restart-val [ interval interval ]

New syntax

event interface interface-list monitor-obj monitor-obj start-op start-op start-val start-val restart-op restart-op restart-val restart-val [ interval interval ]

Views

CLI-defined policy view

Parameters

interface-list: Specifies a space-separated list of up to eight interface items. An item specifies an interface or specifies a range of interfaces in the form of interface-type interface-number to interface-type interface-number. The interfaces in an interface range must be same type. The start interface number must be smaller than the end interface number.

Change description

Before modification: Only one interface can be monitored.

After modification: Multiple interfaces can be monitored. The interfaces in an interface range must be same type. The start interface number must be smaller than the end interface number.

# Modified feature: NTP

## Feature change description

This release added support of maximum and minimum NTP polling intervals.

## Command changes

### Modified command: display ntp-service status

Syntax

display ntp-service status

Views

User view

Change description

Before modification: The command does not display the NTP polling interval.

After modification: The System poll interval field was added to the command output to display the NTP polling interval.

### Modified command: ntp-service unicast-peer

Old syntax

ntp-service unicast-peer { peer-name | ip-address } [ authentication-keyid keyid | priority | source interface-type interface-number | version number ] \*

New syntax

ntp-service unicast-peer { peer-name | ip-address } [ authentication-keyid keyid | maxpoll maxpoll-interval | minpoll minpoll-interval | priority | source interface-type interface-number | version number ] \*

Views

System view

Change description

The maxpoll maxpoll-interval and minpoll minpoll-interval options were added to the command to allow for specifying the maximum and minimum NTP polling intervals.

### Modified command: ntp-service unicast-server

Old syntax

ntp-service unicast-server { server-name | ip-address } [ authentication-keyid keyid | priority | source interface-type interface-number | version number ] \*

New syntax

ntp-service unicast-server { server-name | ip-address } [ authentication-keyid keyid | maxpoll maxpoll-interval | minpoll minpoll-interval | priority | source interface-type interface-number | version number ] \*

Views

System view

Change description

The maxpoll maxpoll-interval and minpoll minpoll-interval options were added to the command to allow for specifying the maximum and minimum NTP polling intervals.

### Modified command: ntp-service ipv6 unicast-peer

Old syntax

ntp-service ipv6 unicast-peer { peer-name | ipv6-address } [ authentication-keyid keyid | priority | source interface-type interface-number ] \*

New syntax

ntp-service ipv6 unicast-peer { peer-name | ipv6-address } [ authentication-keyid keyid | maxpoll maxpoll-interval | minpoll minpoll-interval | priority | source interface-type interface-number ] \*

Views

System view

Change description

The maxpoll maxpoll-interval and minpoll minpoll-interval options were added to the command to allow for specifying the maximum and minimum NTP polling intervals.

### Modified command: ntp-service ipv6 unicast-server

Old syntax

ntp-service ipv6 unicast-server { server-name | ipv6-address } [ authentication-keyid keyid | priority | source interface-type interface-number ] \*

New syntax

ntp-service ipv6 unicast-server { server-name | ipv6-address } [ authentication-keyid keyid | maxpoll maxpoll-interval | minpoll minpoll-interval | priority | source interface-type interface-number ] \*

Views

System view

Change description

The maxpoll maxpoll-interval and minpoll minpoll-interval options were added to the command to allow for specifying the maximum and minimum NTP polling intervals.

# Modified feature: Specifying the source IP address for NTP messages

## Feature change description

You can configure the source IP address for NTP messages directly or by specifying an interface. Before the modification, the source IP address can be configured only by specifying an interface.

## Command changes

### Modified command: ntp-service source

Old syntax

ntp-service source interface-type interface-number

New syntax

ntp-service source { interface-type interface-number | ip-address }

Views

System view

Parameter

interface-type interface-number: Specifies an interface by its type and number. The device uses the primary address of the specified source interface as the source address to send NTP messages. The destination address of the NTP response messages is the primary address of the specified source interface.

ip-address: Specifies the source IP address for NTP messages.

Change description

The ip-address argument was added to the command.

# Modified feature: sFlow counter sampling

## Feature change description

In this version and later, you can specify an sFlow instance for counter sampling.

## Command changes

### Modified command: sflow counter collector

Old syntax

sflow counter collector collector-id

undo sflow counter collector

New syntax

sflow counter [ instance instance-id ] collector collector-id

undo sflow counter [ instance instance-id ] collector

Views

Layer 2 Ethernet interface view

Parameters

instance instance-id: Specifies an sFlow instance by its ID in the range of 1 to 4. The default ID for an sFlow instance is 1. If you do not specify an sFlow instance, this command specifies sFlow instance 1 for counter sampling.

Change description

Before modification: You can specify only an sFlow collector for counter sampling.

After modification: You can specify an sFlow instance and an sFlow collector for counter sampling.

# Modified feature: sFlow flow sampling

## Feature change description

In this version and later, you can specify an sFlow instance for flow sampling.

## Command changes

### Modified command: sflow counter collector

Old syntax

sflow flow collector collector-id

undo sflow flow collector

New syntax

sflow flow [ instance instance-id ] collector collector-id

undo sflow flow [ instance instance-id ] collector

Views

Layer 2 Ethernet interface view

Parameters

instance instance-id: Specifies an sFlow instance by its ID in the range of 1 to 4. The default ID for an sFlow instance is 1. If you do not specify an sFlow instance, this command specifies sFlow instance 1 for flow sampling.

Change description

Before modification: You can specify only an sFlow collector for flow sampling.

After modification: You can specify an sFlow instance and an sFlow collector for flow sampling.

1. Release 3208P16

This release has the following changes:

* New feature: Setting the block timer for MAC addresses in the blocked MAC address list
* New feature: Logging off 802.1X users
* New feature: Logging off MAC authentication users

# New feature: Setting the block timer for MAC addresses in the blocked MAC address list

## Setting the block timer for MAC addresses in the blocked MAC address list

### About setting the block timer for MAC addresses in the blocked MAC address list

Use the block timer in conjunction with the intrusion protection action that blocks the source MAC addresses of illegal frames.

The block timer sets the amount of time that a MAC address must remain in the blocked MAC address list before it is unblocked.

### Procedure

Enter system view.

system-view

Set the block timer for blocked MAC addresses.

port-security timer blockmac time-value

By default, the block timer is 180 seconds.

## Command reference

### port-security timer blockmac

Use port-security timer blockmac to set the block timer for MAC addresses in the blocked MAC address list.

Use undo port-security timer blockmac to restore the default.

Syntax

port-security timer blockmac time-value

undo port-security timer blockmac

Default

The block timer for blocked MAC addresses is 180 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

time-value: Sets a timer value in the range of 1 to 3600 seconds.

Usage guidelines

Use the block timer in conjunction with the intrusion protection action that blocks the source MAC addresses of illegal frames.

The block timer sets the amount of time that a MAC address must remain in the blocked MAC address list before it is unblocked.

Examples

# Configure the intrusion protection action on GigabitEthernet 1/0/1 as blocking source MAC addresses of illegal frames, and set the block timer to 60 seconds.

<Sysname> system-view

[Sysname] port-security timer blockmac 60

[Sysname] interface gigabitethernet 1/0/1

[Sysname-GigabitEthernet1/0/1] port-security intrusion-mode blockmac

Related commands

display port-security

port-security intrusion-mode

# New feature: Logging off 802.1X users

## Logging off 802.1X users

#### About logging off 802.1X users

Perform this task to log off specific 802.1X users and clear information about these users from the device. These users must perform 802.1X authentication to come online again.

#### Procedure

To log off 802.1X users, execute the following command in user view:

reset dot1x access-user [ interface interface-type interface-number | mac mac-address | username username | vlan vlan-id ]

## Command reference

### reset dot1x access-user

Use reset dot1x access-user to log off 802.1X users.

Syntax

reset dot1x access-user [ interface interface-type interface-number | mac mac-address | username username | vlan vlan-id ]

Views

User view

Predefined user roles

network-admin

Parameters

interface interface-type interface-number: Specifies a port by its type and number.

mac mac-address: Specifies an 802.1X user by its MAC address. The mac-address argument is in the format of H-H-H.

username username: Specifies an 802.1X user by its name. The username argument is a case-sensitive string of 1 to 253 characters.

vlan vlan-id: Specifies a VLAN by its VLAN ID. The value range for the vlan-id argument is 1 to 4094.

Usage guidelines

Use this command to log off the specified 802.1X users and clear information about these users from the device. These users must perform 802.1X authentication to come online again.

If you specify a VLAN, this command logs off the following 802.1X users:

* Users that have passed 802.1X authentication and have been assigned the specified VLAN as the authorization VLAN.
* Users that have just passed 802.1X authentication and are to be assigned the specified VLAN as the authorization VLAN.
* Users that are performing 802.1X authentication in the specified VLAN.

If you do not specify any parameters, this command logs off all 802.1X users on the device.

Examples

# Log off all 802.1X users on GigabitEthernet 1/0/1.

<Sysname> reset dot1x access-user interface gigabitethernet 1/0/1

Related commands

display dot1x connection

# New feature: Logging off MAC authentication users

## Logging off MAC authentication users

#### About logging off MAC authentication users

Perform this task to log off specific MAC authentication users and clear information about these users from the device. These users must perform MAC authentication to come online again.

#### Procedure

To log off MAC authentication users, execute the following command in user view:

reset mac-authentication access-user [ interface interface-type interface-number | mac mac-address | username username | vlan vlan-id ]

## Command reference

### reset mac-authentication access-user

Use reset mac-authentication access-user to log off MAC authentication users.

Syntax

reset mac-authentication access-user [ interface interface-type interface-number | mac mac-address | username username | vlan vlan-id ]

Views

User view

Predefined user roles

network-admin

Parameters

interface interface-type interface-number: Specifies a port by its type and number.

mac mac-address: Specifies a MAC authentication user by its MAC address. The mac-address argument is in the format of H-H-H.

username username: Specifies a MAC authentication user by its name. The username argument is a case-sensitive string of 1 to 253 characters.

vlan vlan-id: Specifies a VLAN by its VLAN ID. The value range for the vlan-id argument is 1 to 4094.

Usage guidelines

Use this command to log off the specified MAC authentication users and clear information about these users from the device. These users must perform MAC authentication to come online again.

If you specify a VLAN, this command logs off the following MAC authentication users:

* Users that have passed MAC authentication and have been assigned the specified VLAN as their authorization VLAN.
* Users that have just passed MAC authentication and are to be assigned the specified VLAN as the authorization VLAN.
* Users that are performing MAC authentication in the specified VLAN.

If you do not specify any parameters, this command logs off all MAC authentication users on the device.

Examples

# Log off all MAC authentication users on GigabitEthernet 1/0/1.

<Sysname> reset mac-authentication access-user interface gigabitethernet 1/0/1

Related commands

display mac-authentication connection

1. Release 3208P15

This release has the following changes:

* New feature: Configuring zero-to-two VLAN mapping
* New feature: Specifying DNS server information in RA messages
* New feature: Specifying DNS suffix information in RA messages
* New feature: Suppressing advertising DNS information in RA messages
* New feature: HTTP redirect
* New feature: ERPS
* Modified feature: Physical type of a combo interface

# New feature: Configuring zero-to-two VLAN mapping

## Configuring zero-to-two VLAN mapping

#### About zero-to-two VLAN mapping

As shown in Figure 1, zero-to-two VLAN mapping is implemented on the customer-side port to add double tags to untagged uplink traffic. For zero-to-two VLAN mapping to take effect, the port PVID must be VLAN 1.

For correct downlink traffic transmission, the downlink traffic must be double-tagged. Then, the customer-side port removes both SVLAN and CVLAN tags from the traffic.

Use one of the following methods to ensure that the downlink traffic contains double tags on the customer-side port:

* Configure the port as a trunk port and assign it to the SVLAN, which must be different from the port PVID (VLAN 1).
* Configure the port as a hybrid port and assign it to the SVLAN as a tagged member.

Zero-to-two VLAN mapping implementation



‌

#### Configuration restrictions and guidelines

As a best practice, set the MTU to a minimum of 1504 bytes for ports on the forwarding path of the double-tagged packet in the service provider network.

#### Procedure

Enter system view.

system-view

Enter interface view.

* + Enter Layer 2 Ethernet interface view.

interface interface-type interface-number

* + Enter Layer 2 aggregate interface view.

interface bridge-aggregation interface-number

Set the link type of the port.

port link-type { hybrid | trunk }

By default, the link type of a port is access.

Set the port PVID to VLAN 1.

* + Set the PVID to VLAN 1 for the trunk port.

port trunk pvid vlan 1

* + Set the PVID to VLAN 1 for the hybrid port.

port hybrid pvid vlan 1

Assign the port to the SVLAN and the port PVID (VLAN 1).

* + Assign the trunk port to the SVLAN and the port PVID (VLAN 1).

port trunk permit vlan vlan-id-list

By default, a trunk port is assigned to VLAN 1.

The SVLAN of the trunk port must be different from the port PVID (VLAN 1).

* + Assign the hybrid port to the SVLAN and the port PVID (VLAN 1) as a tagged member.

port hybrid vlan vlan-id-list tagged

By default, a hybrid port is an untagged member of the VLAN to which the port belongs when its link type is access.

Configure a zero-to-two VLAN mapping.

vlan mapping untagged nested-outer-vlan outer-vlan-id nested-inner-vlan inner-vlan-id

By default, no VLAN mapping is configured on an interface.

## Command reference

### vlan mapping untagged

Use vlan mapping untagged to configure zero-to-two VLAN mapping on an interface.

Use undo vlan mapping untagged to remove the zero-to-two VLAN mapping configuration.

Syntax

vlan mapping untagged nested-outer-vlan outer-vlan-id nested-inner-vlan inner-vlan-id

undo vlan mapping untagged

Default

No zero-to-two VLAN mapping is configured on an interface.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

mdc-admin

Parameters

nested-outer-vlan outer-vlan-id: Specifies the SVLAN ID in the range of 1 to 4094.

nested-inner-vlan inner-vlan-id: Specifies the CVLAN ID in the range of 1 to 4094.

Usage guidelines

This command takes effect only on ports that use VLAN 1 as the PVID.

Before you modify a zero-to-two VLAN mapping, first execute the undo vlan mapping untagged command to remove the previous configuration.

As a best practice, set the MTU to a minimum of 1504 bytes for ports on the forwarding path of the double-tagged packet in the service provider network.

Examples

# Configure a zero-to-two VLAN mapping on to add SVLAN 200 and CVLAN 100 to untagged packets.

<Sysname> system-view

[Sysname] interface

[Sysname-] vlan mapping untagged nested-outer-vlan 200 nested-inner-vlan 100

# New feature: Specifying DNS server information in RA messages

## Specifying DNS server information in RA messages

### About specifying DNS server information in RA messages

The DNS server options in RA messages provide DNS server information for IPv6 hosts. The RA messages allow hosts to obtain their IPv6 addresses and the DNS server through stateless autoconfiguration. This method is useful in a network where DHCPv6 infrastructure is not provided.

One DNS server option contains one DNS server. All DNS server options are sorted in ascending order of the DNS server sequence number.

After you execute the ipv6 nd ra dns server command, the device immediately sends an RA message with the existing and newly specified DNS server information.

After you execute the undo ipv6 nd ra dns server command, the device immediately sends two RA messages.

* The first RA message carries information about all DNS servers, including the DNS servers specified in the undo command with their lifetime set to 0 seconds.
* The second RA message carries information about remaining DNS servers.

Each time the device sends an RA message from an interface, it immediately refreshes the RA message advertisement interval for that interface.

### Restrictions and guidelines

You can configure a maximum of eight DNS servers on an interface.

The default lifetime of a DNS server is three times the maximum interval for advertising RA messages. To set the maximum interval, use the ipv6 nd ra interval command.

### Procedure

Enter system view.

system-view

Enter interface view.

interface interface-type interface-number

Specify DNS server information to be advertised in RA messages.

ipv6 nd ra dns server ipv6-address [ seconds | infinite ] sequence seqno

By default, no DNS server information is specified and RA messages do not carry DNS server options.

## Command reference

### ipv6 nd ra dns server

Use ipv6 nd ra dns server to specify DNS server information to be advertised in RA messages.

Use undo ipv6 nd ra dns server to remove a DNS server from RA message advertisement.

Syntax

ipv6 nd ra dns server ipv6-address [ seconds | infinite ] sequence seqno

undo ipv6 nd ra dns server ipv6-address

Default

DNS server information is not specified and RA messages do not carry DNS server options.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address of the DNS server, which must be a global unicast address or a link-local address.

seconds: Specifies the lifetime of the DNS server, in seconds. The value range is 4 to 4294967295. Value 4294967295 indicates that the lifetime of the DNS server is infinite.

infinite: Sets the lifetime of the DNS server to infinite.

sequence seqno: Specifies the sequence number of the DNS server, in the range of 0 to 4294967295. The sequence number for a DNS server must be unique. A smaller sequence number represents a higher priority.

Usage guidelines

The DNS server option in RA messages provides DNS server information for hosts. The RA messages allow hosts to obtain their IPv6 addresses and the DNS server through stateless autoconfiguration. This method is useful in a network where DHCPv6 infrastructure is not provided.

The default lifetime of the DNS server is three times the maximum interval for advertising RA messages. To set the maximum interval, use the ipv6 nd ra interval command.

You can configure a maximum of eight DNS servers on an interface. One DNS server option contains one DNS server. All DNS server options are sorted in ascending order of the DNS server sequence number.

The sequence number uniquely identifies a DNS server. To modify the IPv6 address or sequence number of a DNS server, you must first use the undo ipv6 nd ra dns server command to remove the DNS server from RA message advertisement.

After you execute the ipv6 nd ra dns server command, the device immediately sends an RA message with the existing and newly specified DNS server options.

After you execute the undo ipv6 nd ra dns server command, the device immediately sends two RA messages.

* The first RA message carries information about all DNS servers, including the DNS servers specified in the undo command with their lifetime set to 0 seconds.
* The second RA message carries information about remaining DNS servers.

Each time the device sends an RA message from an interface, it immediately refreshes the RA message advertisement interval for that interface.

Examples

# Specify the DNS server address as 2001:10::100, the server lifetime as infinite, and the sequence number as 1 for RA messages on VLAN-interface 100.

<Sysname> system-view

[Sysname] interface vlan-interface 100

[Sysname-Vlan-interface100] ipv6 nd ra dns server 2001:10::100 infinite sequence 1

Related commands

* ipv6 nd ra dns server suppress
* ipv6 nd ra interval

# New feature: Specifying DNS suffix information in RA messages

## Specifying DNS suffix information in RA messages

### About specifying DNS suffix information in RA messages

The DNSSL option in RA messages provides suffix information for IPv6 hosts. The RA messages allow hosts to obtain their IPv6 addresses and the DNS suffix through stateless autoconfiguration. This method is useful in a network where DHCPv6 infrastructure is not provided.

One DNSSL option contains one DNS suffix. All DNSSL options are sorted in ascending order of the sequence number of the DNS suffix.

After you execute the ipv6 nd ra dns search-list command, the device immediately sends an RA message with the existing and newly specified DNS suffix information.

After you execute the undo ipv6 nd ra dns search-list command, the device immediately sends two RA messages.

* The first RA message carries information about all DNS suffixes, including DNS suffixes specified in the undo command with their lifetime set to 0 seconds.
* The second RA message carries information about remaining DNS suffixes.

Each time the device sends an RA message from an interface, it immediately refreshes the RA message advertisement interval for that interface.

### Restrictions and guidelines

You can configure a maximum of eight DNS suffixes on an interface.

The default lifetime of a DNS suffix is three times the maximum interval for advertising RA messages. To set the maximum interval, use the ipv6 nd ra interval command.

### Procedure

Enter system view.

system-view

Enter interface view.

interface interface-type interface-number

Specify DNS suffix information to be advertised in RA messages.

ipv6 nd ra dns search-list domain-name [ seconds | infinite ] sequence seqno

By default, no DNS suffix information is specified and RA messages do not carry DNS suffix options.

## Command reference

### ipv6 nd ra dns search-list

Use ipv6 nd ra dns search-list to specify DNS suffix information to be advertised in RA messages.

Use undo ipv6 nd ra dns search-list to remove a DNS suffix from RA message advertisement.

Syntax

ipv6 nd ra dns search-list domain-name [ seconds | infinite ] sequence seqno

undo ipv6 nd ra dns search-list domain-name

Default

DNS suffix information is not specified and RA messages do not carry DNS suffix options.

Views

Interface view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a DNS suffix. It is a dot-separated, case-insensitive string that can include letters, digits, hyphens (-), underscores (\_), and dots (.), for example, aabbcc.com. The DNS suffix can include a maximum of 253 characters, and each separated string includes no more than 63 characters.

seconds: Specifies the lifetime of the DNS suffix, in seconds. The value range is 4 to 4294967295. Value 4294967295 indicates that the lifetime of the DNS suffix is infinite.

infinite: Sets the lifetime of the DNS suffix to infinite.

seqno: Specifies the sequence number of the DNS suffix, in the range of 0 to 4294967295. The sequence number for a DNS suffix must be unique. A smaller sequence number represents a higher priority.

Usage guidelines

The DNS search list (DNSSL) option in RA messages provides DNS suffix information for hosts. The RA messages allow hosts to obtain their IPv6 addresses and the DNS suffix through stateless autoconfiguration. This method is useful in a network where DHCPv6 infrastructure is not provided.

The default lifetime of the DNS suffix is three times the maximum interval for advertising RA messages. To set the maximum interval, use the ipv6 nd ra interval command.

You can configure a maximum of eight DNS suffixes on an interface. One DNSSL option contains one DNS suffix. All DNSSL options are sorted in ascending order of the sequence number of the DNS suffix.

The sequence number uniquely identifies a DNS suffix. To modify a DNS suffix or its sequence number, you must first use the undo ipv6 nd ra dns search-list command to remove the DNS suffix from RA message advertisement.

After you execute the ipv6 nd ra dns search-list command, the device immediately sends an RA message with the existing and newly specified DNS suffix information.

After you execute the undo ipv6 nd ra dns search-list command, the device immediately sends two RA messages.

* The first RA message carries information about all DNS suffixes, including DNS suffixes specified in the undo command with their lifetime set to 0 seconds.
* The second RA message carries information about remaining DNS suffixes.

Each time the device sends an RA message from an interface, it immediately refreshes the RA message advertisement interval for that interface.

Examples

# Specify the DNS suffix as [com](http://www.h3c.com), the suffix lifetime as infinite, and the sequence number as 1 for RA messages on VLAN-interface 100.

<Sysname> system-view

[Sysname] interface vlan-interface 100

[Sysname-Vlan-interface100] ipv6 nd ra dns search-list com infinite sequence 1

Related commands

* ipv6 nd ra dns search-list suppress
* ipv6 nd ra interval

# New feature: Suppressing advertising DNS information in RA messages

## Suppressing advertising DNS information in RA messages

### About suppressing advertising DNS information in RA messages

Perform this task to suppress the device from advertising information about DNS server addresses and DNS suffixes in RA messages.

Whether enabling this feature on an interface will trigger sending RA message immediately for DNS server update depends on the interface configuration:

* If the interface has been configured with DNS server information, the device immediately sends two RA messages. In the first message, the lifetime for DNS server addresses is 0 seconds. The second RA message does not carry any DNS server options.
* If the interface has no DNS server information specified, no RA messages are triggered.
* If you specify a new DNS server or remove a DNS server, the device immediately sends an RA message without any DNS server address options.

Whether disabling this feature on an interface will trigger sending RA message immediately for DNS server update depends on the interface configuration:

* If the interface has been configured with the DNS server information, the device immediately sends an RA message carrying the DNS server information.
* If the interface has no DNS server information specified, no RA messages are triggered.

Each time the device sends an RA message from an interface, it immediately refreshes the RA message advertisement interval for that interface.

The same suppression mechanism applies when you enable or disable DNS suffix suppression in RA messages.

### Procedure

Enter system view.

system-view

Enter interface view.

interface interface-type interface-number

Enable DNS server suppression in RA messages.

ipv6 nd ra dns server suppress

By default, DNS server suppression in RA messages is disabled.

Enable DNS suffix suppression in RA messages.

ipv6 nd ra dns search-list suppress

By default, DNS suffix suppression in RA messages is disabled.

## Command reference

### ipv6 nd ra dns search-list suppress

Use ipv6 nd ra dns search-list suppress to enable DNS suffix suppression in RA messages.

Use undo ipv6 nd ra dns search-list suppress to disable DNS suffix suppression in RA messages.

Syntax

ipv6 nd ra dns search-list suppress

undo ipv6 nd ra dns search-list suppress

Default

DNS suffix suppression in RA messages is disabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This command suppresses advertising DNS suffixes in RA messages.

RA messages are suppressed by default. To disable RA message suppression, use the undo ipv6 nd ra halt command.

Whether enabling this feature on an interface will trigger sending RA message immediately for DNS suffix update depends on the interface configuration:

* If the interface has been configured with DNS suffix information, the device immediately sends two RA messages. In the first message, the lifetime for DNS suffixes is 0 seconds. The second RA message does not carry any DNSSL options.
* If the interface has no DNS suffix information specified, no RA messages are triggered.
* If you specify a new DNS suffix or remove a DNS suffix, the device immediately sends an RA message without any DNSSL options.

Whether disabling this feature on an interface will trigger sending RA message immediately for DNS suffix update depends on the interface configuration:

* If the interface has been configured with the DNS suffix information, the device immediately sends an RA message carrying the DNS suffix information.
* If the interface has no DNS suffix information specified, no RA messages are triggered.

Each time the device sends an RA message from an interface, it immediately refreshes the RA message advertisement interval for that interface.

Examples

# Enable DNS suffix suppression in RA messages on VLAN-interface 100.

<Sysname> system-view

[Sysname] interface vlan-interface 100

[Sysname-Vlan-interface100] ipv6 nd ra dns search-list suppress

Related commands

* ipv6 nd ra dns search-list

### ipv6 nd ra dns server suppress

Use ipv6 nd ra dns server suppress to enable DNS server suppression in RA messages.

Use undo ipv6 nd ra dns server suppress to disable DNS server suppression in RA messages.

Syntax

ipv6 nd ra dns server suppress

undo ipv6 nd ra dns server suppress

Default

DNS server suppression in RA messages is disabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This command suppresses advertising DNS server addresses in RA messages.

RA messages are suppressed by default. To disable RA message suppression, use the undo ipv6 nd ra halt command.

Whether enabling this feature on an interface will trigger sending RA message immediately for DNS server information update depends on the interface configuration:

* If the interface has been configured with DNS server information, the device immediately sends two RA messages. In the first message, the lifetime for DNS server addresses is 0 seconds. The second RA message does not carry any DNS server options.
* If the interface has no DNS server information specified, no RA messages are triggered.
* If you specify a new DNS server or remove a DNS server, the device immediately sends an RA message without any DNS server address options.

Whether disabling this feature on an interface will trigger sending RA message immediately for DNS server information update depends on the interface configuration:

* If the interface has been configured with the DNS server information, the device immediately sends an RA message carrying the DNS server information.
* If the interface has no DNS server information specified, no RA messages are triggered.

Each time the device sends an RA message from an interface, it immediately refreshes the RA message advertisement interval for that interface.

Examples

# Enable DNS server suppression in RA messages on VLAN-interface 100.

<Sysname> system-view

[Sysname] interface vlan-interface 100

[Sysname-Vlan-interface100] ipv6 nd ra dns server suppress

Related commands

* ipv6 nd ra dns server

# New feature: HTTP redirect

## About HTTP redirect

HTTP redirect is a method to redirect users' HTTP or HTTPS requests to a specific URL. It is used in the following features:

* Redirect URL assignment in 802.1X authentication, MAC authentication, and port security.
* EAD assistant URL redirection in 802.1X authentication.
* URL redirection services in portal.

## HTTP redirect tasks at a glance

No configuration is required to redirect HTTP requests.

To redirect HTTPS requests, perform the following tasks:

Specifying the HTTPS redirect listening port number

(Optional.) Associating an SSL server policy with the HTTPS redirect service

## Specifying the HTTPS redirect listening port number

#### About the HTTPS redirect listening port number

The device can redirect HTTPS requests only after you specify the TCP port number on which the HTTPS redirect service listens for HTTPS requests.

#### Restrictions and guidelines

To avoid service unavailability caused by port conflict, do not specify a TCP port number used by a well-known protocol or used by any other TCP-based service. To display TCP port numbers that have been used by services, use the display tcp command. For more information about this command, see IP performance optimization commands in Layer 3—IP Services Command Reference.

If you perform this task multiple times, the most recent configuration takes effect.

#### Procedure

Enter system view.

system-view

Specify the HTTPS redirect listening port number.

http-redirect https-port port-number

By default, no HTTPS redirect listening port number is specified.

## Associating an SSL server policy with the HTTPS redirect service

#### About associating an SSL server policy with the HTTPS redirect service

To improve the security of HTTPS redirect, you can associate an SSL server policy with the HTTPS redirect service. For more information about the SSL server policy configuration, see SSL in Security Configuration Guide.

#### Restrictions and guidelines

HTTPS redirect is unavailable if the associated SSL server policy does not exist. You can first associate a nonexistent SSL server policy with the HTTPS redirect service and then configure the SSL server policy.

If you change the SSL server policy associated with the HTTPS redirect service, the new policy takes effect immediately.

If you perform this task multiple times, the most recent configuration takes effect.

#### Procedure

Enter system view.

system-view

Associate an SSL server policy with the HTTPS redirect service.

http-redirect ssl-server-policy policy-name

By default, no SSL server policy is associated with the HTTPS redirect service. The HTTPS redirect service uses the self-assigned certificate and the default SSL parameters.

## Command reference

### http-redirect https-port

Use http-redirect https-port to specify the HTTPS redirect listening port number.

Use undo http-redirect https-port to restore the default.

Syntax

http-redirect https-port port-number

undo http-redirect https-port

Default

No HTTPS redirect listening port number is specified.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies the TCP port number on which the HTTPS redirect service listens for HTTPS requests. The value range for the port number is 1 to 65535.

Usage guidelines

To avoid service unavailability caused by port conflict, do not specify a TCP port number used by a well-known protocol or used by any other service. To display TCP port numbers that have been used by services, use the display tcp command.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

# Specify 8888 as the HTTPS redirect listening port number.

<Sysname> system-view

[Sysname] http-redirect https-port 8888

### http-redirect ssl-server-policy

Use http-redirect ssl-server-policy to associate an SSL server policy with the HTTPS redirect service.

Use undo http-redirect ssl-server-policy to restore the default.

Syntax

http-redirect ssl-server-policy policy-name

undo http-redirect ssl-server-policy

Default

No SSL server policy is associated with the HTTPS redirect service. The HTTPS redirect service uses a self-assigned certificate and the default SSL parameters.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies an SSL server policy by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

HTTPS redirect is unavailable if the associated SSL server policy does not exist. You can first associate a nonexistent SSL server policy with the HTTPS redirect service and then configure the SSL server policy.

If you change the SSL server policy associated with the HTTPS redirect service, the new policy takes effect immediately.

If you perform this task multiple times, the most recent configuration takes effect.

Examples

# Associate SSL server policy policy1 with the HTTPS redirect service.

<Sysname> system-view

[Sysname] http-redirect ssl-server-policy policy1

Related commands

ssl server-policy

# New feature: ERPS

## Configuring ERPS

### About ERPS

Ethernet Ring Protection Switching (ERPS) is a robust link layer protocol that ensures a loop-free topology and implements quick link recovery.

#### ERPS structure

ERPS ring structure



##### Rings

ERPS rings can be divided into major rings and subrings. An ERPS network consists of one major ring or multiple major rings, and multiple subrings. By default, a ring is a major ring. You can configure a ring as a subring manually.

As shown in Figure 2, a major ring is a closed ring formed by Device A, Device B, Device C, and Device D. A subring is an open ring formed by the link Device C<—>Device E<—>Device F<—>Device D.

##### RPL

An ERPS ring is composed of many nodes. Some nodes use ring protection links (RPLs) to prevent loops on the ERPS ring. As shown in Figure 2, the link between Device A and Device B and the link between Device E and Device F are RPLs.

##### Nodes

ERPS nodes include owner nodes, neighbor nodes, interconnection nodes, and normal nodes.

* The owner node and neighbor node block and unblock ports on the RPL to prevent loops and switch traffic. An RPL connects an owner node and a neighbor node.
* Interconnection nodes connect different rings. Interconnection nodes reside on subrings and forward service packets but not protocol packets.
* Normal nodes forward both service packets and protocol packets.

As shown in Figure 2, on the major ring, Device A is the owner node and Device B is the neighbor node. On the subring, Device E is the owner node and Device F is the neighbor node. Devices C and D are interconnection nodes.

##### Ports

Each node consists of two ERPS ring member ports: Port 0 and port 1. ERPS ring member ports have the following types:

* RPL port—Port on an RPL link.
* Interconnection port—Port that connects a subring to a major ring.
* Normal port—Default type of a port that forwards both service packets and protocol packets.

As shown in Figure 2, ports A1, B1, E1, and F1 are RPL ports. Ports C3 and D3 are interconnection ports. Other ports are normal ports.

#### Instances

An ERPS ring supports multiple ERPS instances. An ERPS instance is a logical ring to process service and protocol packets. Each ERPS instance has its own owner node and maintains its own state and data. An ERPS instance is uniquely identified by the ring ID and VLAN ID of ERPS packets. The ring ID indicates the ring of ERPS packets. It can be represented by the last byte in the destination MAC address of the packets. The VLAN ID indicates the ERPS instance of the packets.

#### ERPS protocol packets

ERPS protocol packets are Ring Automatic Protection Switching (R-APS) packets. You can configure the R-APS packet level. A node does not process R-APS packets whose levels are greater than the level of the packets sent by the node. On a ring, the levels of R-APS packets must be the same for all nodes in an ERPS instance.

R-APS packet types and functions

| Packet type | Function |
| --- | --- |
| No request, RPL block (NR-RB) | When the link is stable, an owner node in idle state periodically sends NR-RB packets to inform other nodes that the RPL ports are blocked. The nodes that receive the NR-RB packets unblock available ports and update MAC address entries. |
| No request (NR) | After the link fault is cleared, the node that detects the recovery periodically sends NR packets. When the owner node receives the NR packets, it starts the WTR timer. The node stops sending NR packets after receiving NR-RB packets from the owner node. |
| Signal fail (SF) | When a link fails to send or receive signals, the node that detects the fault periodically sends SF packets. When the owner node and neighbor node receive the FS packets, they unblock the RPL ports.  The node stops sending SF packets after the fault is cleared. |
| Manual switch (MS) | A port configured with the MS mode is blocked and periodically sends MS packets. When other nodes receive the MS packets, they unblock available ports and update MAC address entries. |
| Forced switch (FS) | A port configured with the FS mode is blocked and periodically sends FS packets. When other nodes receive the FS packets, they unblock all ports and update MAC address entries. |
| Flush | If the topology of a subring changes, the interconnection ports on the subring broadcasts flush packets. All nodes that receive the flush packets update MAC address entries. |

|  | NOTE:  Typically R-APS packets are transmitted within a ring. The flush packets sourced from the subring can be forwarded to the major ring.  Service packets can be transmitted between different rings. |
| --- | --- |

#### ERPS node states

ERPS states

| State | Description |
| --- | --- |
| Init | State for a non-interconnection node that has less than two ERPS ring member ports or for an interconnection node that does not have ERPS ring member ports. |
| Idle | Stable state when all non-RPL links are available. In this state, the owner node blocks the RPL port and periodically sends NR-RB packets. The neighbor node blocks the RPL port. All nodes enter the idle state after the owner node enters the idle state. |
| Protection | State when a non-RPL link is faulty. In this state, the RPL link is unblocked to forward traffic. All nodes enter the protection state after a node enters the protection state. |
| MS | State when traffic paths are manually switched. All nodes enter the MS state after a node is configured with the MS mode. |
| FS | State when traffic paths are forcibly switched. All nodes enter the FS state after a node is configured with the FS mode. |
| Pending | Transient state between the previous states. |

#### ERPS timers

##### Hold-off timer

The hold-off timer starts when the port detects a link fault. The port reports the link fault if the fault persists when the timer expires.

This timer delays the fault report time and affects the link switching performance.

##### Guard timer

The guard timer starts when the port detects a link recovery. The port does not process R-APS packets before the timer expires.

This timer prevents R-APS packets from impacting the network and affects the link switching performance when multiple points of failures exist.

##### WTR timer

In revertive mode, the WTR timer starts when the owner node in protection state receives NR packets. The RPL is unblocked and the recovered node is blocked before the timer expires. The owner node blocks the RPL and sends NR-RB packets when the timer expires. If the port receives SF packets before the timer expires, the timer stops and the RPL remains unblocked.

This timer prevents intermittent link failures from impacting the network.

##### WTB timer

In revertive mode, the WTB timer starts when the owner node in MS or FS state receives NR packets. The RPL is unblocked and the recovered node sends NR packets before the timer expires. The owner node blocks the RPL and sends NR-RB packets when the timer expires. If the port receives SF packets before the timer expires, the timer stops and the RPL remains unblocked.

This timer prevents the RPL ports from being blocked and unblocked frequently.

#### ERPS operation mechanism

ERPS uses the detection mechanism defined in ITU-T G.8032/Y.1344 to locate the point of failure and identify unidirectional or bidirectional faults.

ERPS uses the SF packets to report signal failures on a link and the NR packets to report link recovery. When a node detects a link status change, the node sends three packets first and then sends subsequent packets every five seconds.

##### Link-down report mechanism

Link-down report mechanism



As shown in Figure 3, the link-down report mechanism uses the following process:

Device C and Device D detect the link failure and perform the following operations:

Block the ports on both side of the faulty link.

Periodically send SF packets to other nodes.

Device A and Device B receive the SF packets and perform the following operations:

Unblock RPL ports.

Update the MAC address entries.

Service packets are switched to the RPL link.

##### Link recovery mechanism

Link recovery mechanism



As shown in Figure 4, the link recovery mechanism uses the following process:

Device C and Device D detect the link recovery and perform the following operations:

Block the recovered ports.

Start the guard timer.

Send NR packets.

When Device A (owner node) receives the NR packets, it does not perform any operations if it is in non-revertive mode. If Device A is in revertive mode, it performs the following operations:

Starts the WTR timer.

Blocks the RPL port and periodically sends NR-RB packets when the WTR timer expires.

When other nodes receive the NR-RB packets, they perform the following operations:

Device B (neighbor port) blocks the RPL port.

Device C and Device D unblock the recovered ports.

Service packets are switched to the recovered link.

##### Multi-instance load balancing mechanism

Multi-instance load balancing mechanism



An ERPS ring topology might carry traffic from multiple VLANs. Traffic from different VLANs can be load balanced among different ERPS instances.

ERPS uses the following types of VLANs:

* Control VLAN—Carries ERPS protocol packets. Each ERPS instance has its own control VLAN.
* Protected VLAN—Carries data packets. Each ERPS instance has its own protected VLAN. Protected VLANs are configured by using the mappings between VLANs and MSTIs.

As shown in Figure 5, the ERPS ring is configured with instance 1 and instance 2. For instance 1, the owner node is Device A, and the RPL is the link between Device A and Device B. For instance 2, the owner node is Device C, and the RPL is the link between Device C and Device D. Traffic from different VLANs can be load balanced among different links.

##### Manual configuration mechanism

ERPS supports the following manual configuration modes:

* MS—Use the erps switch manual command to block an ERPS ring member port. A port in MS mode is blocked and sends MS packets. The nodes that receive the MS packets unblock available ports. If the nodes in MS mode receive an SF packet, they unblock the blocked ports.
* FS—Use the erps switch force ring command to block an ERPS ring member port. A port in FS mode is blocked and sends FS packets. The nodes that receive the FS packets unblock available ports. If the nodes in FS mode receive an SF packet, they do not unblock the blocked ports.

##### Collaboration mechanism

To detect and clear link faults typically for a fiber link, use ERPS with CFD and Track. You can associate ERPS ring member ports with the continuity check function of CFD through track entries. CFD reports link events only when the monitored VLAN is the control VLAN of the ERPS instance for the port. For more information about CFD and Track, see "Configuring CFD" and "Configuring Track."

#### ERPS network diagrams

##### One major ring

The network has one major ring.

Network diagram



##### One major ring connecting one subring

The network has one major ring and one subring.

Network diagram



##### One major ring connecting multiple subrings

The network has three or more rings. Each subring is connected to the major ring by two interconnection nodes.

Network diagram



##### One subring connecting multiple subrings

The network has three or more rings. As shown in Figure 9, subring 1 is connected to the major ring. Other subrings are connected to subring 1 by two interconnection nodes.

Network diagram



##### One subring connecting multiple rings

The network has three or more rings. A minimum of one subring is connected to two rings. As shown in Figure 10, one interconnection node on subring 2 is connected to the major ring; and another interconnection node is connected to subring 1. As shown in Figure 11, subring 3 is connected to subring 1 and subring 2.

Network diagram 1



Network diagram 2



#### Protocols and standards

* ITU-T G.8032, Recommendation ITU-T G.8032/Y.1344, Ethernet ring protection switching
* IEEE 802.1D, IEEE Std 802.1D™-2004, IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Bridges
* IEEE 802.3, IEEE Std 802.3-2008, IEEE Standard for Information technology

### Restrictions and guidelines: ERPS configuration

ERPS does not provide an election mechanism. To implement ring detection and protection, configure all nodes correctly.

### ERPS tasks at a glance

To configure ERPS, perform the following tasks:

Enabling ERPS globally

Perform this task on devices you want to configure as ERPS nodes.

Configuring an ERPS ring

Perform this task on all nodes on an ERPS ring.

Creating an ERPS ring

Configuring ERPS ring member ports

Configuring control VLANs

Configuring protected VLANs

Configuring the node role

Enabling ERPS for an instance

Perform this task on all nodes on an ERPS ring.

(Optional.) Enabling R-APS packets to carry the ring ID in the destination MAC address

Perform this task on all nodes on an ERPS ring.

(Optional.) Configuring R-APS packet levels

(Optional.) Setting ERPS timers

Perform this task on the owner node on an ERPS ring.

(Optional.) Setting the non-revertive mode

Perform this task on the owner node on an ERPS ring.

(Optional.) Setting a switchover mode

Perform this task on the nodes that you want to block their ports.

(Optional.) Associating a ring with a subring

Perform this task on the interconnection node on an ERPS ring.

(Optional.) Enabling flush packet transparent transmission

Perform this task on the interconnection node on an ERPS ring.

(Optional.) Associating an ERPS ring member port with a track entry

(Optional.) Removing the MS mode and FS mode settings for an ERPS ring

### Prerequisites

Before you configure ERPS, complete the following tasks:

* Establish the Ethernet ring topology.
* Determine the ERPS rings, ERPS instances, control VLANs, protected VLANs, and node roles.

### Enabling ERPS globally

##### Restrictions and guidelines

* Perform this task on devices you want to configure as ERPS nodes.
* For ERPS to take effect for an instance, enable it globally first.

##### Procedure

Enter system view.

system-view

Enable ERPS globally.

erps enable

By default, ERPS is disabled globally.

### Configuring an ERPS ring

#### Creating an ERPS ring

##### Restrictions and guidelines

* Perform this task on all nodes on an ERPS ring.
* A ring ID uniquely identifies an ERPS ring. All nodes on an ERPS ring must be configured with the same ring ID.

##### Procedure

Enter system view.

system-view

Create an ERPS ring.

erps ring ring-id

(Optional.) Configure the ring type.

ring-type sub-ring

By default, an ERPS ring is a major ring.

#### Configuring ERPS ring member ports

##### Restrictions and guidelines

* Perform this task on each node's ports intended for accessing ERPS rings.
* ERPS ring member ports automatically allow packets from the control VLAN to pass through.
* Do not enable Ethernet OAM remote loopback for ERPS ring member ports. This feature might cause a broadcast storm. For more information about Ethernet OAM, see "Configuring Ethernet OAM."
* For faster topology convergence, use the link-delay command on ERPS ring member ports to set the physical state change suppression interval to 0 seconds. For more information about the link-delay command, see Interface Command Reference.
* You must configure ERPS ring member ports as trunk ports.
* Do not assign an interface to both an aggregation group and an ERPS ring. If you do so, the interface does not take effect on the ERPS ring and cannot be displayed by using the display erps detail command.

#### Configuring ERPS ring member port attributes

Enter system view.

system-view

Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.

interface interface-type interface-number

Configure the port as a trunk port.

port link-type trunk

By default, a port is an access port.

For more information about this command, see Layer 2—LAN Switching Command Reference.

Assign the trunk port to protected VLANs.

port trunk permit vlan { vlan-id-list | all }

By default, a trunk port is assigned only to VLAN 1.

For more information about this command, see Layer 2—LAN Switching Command Reference.

Disable the spanning tree feature.

undo stp enable

By default, the spanning tree feature is enabled.

For more information about this command, see Layer 2—LAN Switching Command Reference.

#### Configuring an ERPS ring member port

Enter system view.

system-view

Enter ERPS ring view.

erps ring ring-id

Configure an ERPS ring member port.

{ port0 | port1 } interface interface-type interface-number

By default, an ERPS ring does not have ERPS ring member ports.

#### Configuring control VLANs

##### Restrictions and guidelines

* Perform this task on all nodes on an ERPS ring.
* The control VLAN must be a VLAN that has not been created on the device.
* Configure the same control VLAN for all nodes in an ERPS instance.
* Do not configure the default VLAN of an ERPS ring member port as the control VLAN.
* Do not enable QinQ or VLAN mapping on control VLANs. If you do, ERPS packets cannot be correctly forwarded and received.
* Make sure the ERPS instance has been configured. After the ERPS instance is enabled, the control VLAN cannot be changed.
* For a device not configured with ERPS to transparently transmit ERPS packets, make sure only the two ports accessing the ERPS ring permit packets from the control VLAN. If other ports on the device permit packets from the control VLAN, the packets from other VLANs might enter the control VLAN and strike the ERPS ring.

##### Procedure

Enter system view.

system-view

Enter ERPS ring view.

erps ring ring-id

Enable ERPS instance view.

instance instance-id

Configure a control VLAN.

control-vlan vlan-id

#### Configuring protected VLANs

##### Restrictions and guidelines

* Perform this task on all nodes on an ERPS ring.
* Configure the same protected VLAN for all nodes of an ERPS instance. To implement load balancing, configure different protected VLANs for different ERPS instances.

##### Prerequisites

Before you configure protected VLANs, you must configure an MST region and the VLAN-to-instance mapping table. For more information about MST regions, see spanning tree configuration in Layer 2—LAN Switching Configuration Guide.

##### Procedure

Enter system view.

system-view

Enter ERPS ring view.

erps ring ring-id

Enable ERPS instance view.

instance instance-id

Configure the protected VLANs.

protected-vlan reference-instance instance-id-list

#### Configuring the node role

##### Restrictions and guidelines

* Perform this task on all nodes on an ERPS ring.
* For the owner node to work correctly, you must configure only one owner node for an ERPS ring.
* You can only configure the interconnection node for subrings.

##### Procedure

Enter system view.

system-view

Enter ERPS ring view.

erps ring ring-id

Enter ERPS instance view.

instance instance-id

Configure the node role.

node-role { { owner | neighbor } rpl | interconnection } { port0 | port1 }

By default, a node is a normal node.

### Enabling ERPS for an instance

##### Restrictions and guidelines

* Perform this task on all nodes on an ERPS ring.
* You can enable ERPS for an instance only when it is configured with a control VLAN and a protected VLAN.

##### Procedure

Enter system view.

system-view

Enter ERPS ring view.

erps ring ring-id

Enter ERPS instance view.

instance instance-id

Enable ERPS for the instance.

instance enable

By default, ERPS is disabled for an instance.

### Enabling R-APS packets to carry the ring ID in the destination MAC address

##### About this feature

Perform this task to configure the ring ID as the last byte of the destination MAC address for R-APS packets. The ring of R-APS packets can be identified by their destination MAC addresses.

##### Restrictions and guidelines

Perform this task on all nodes on an ERPS ring.

##### Procedure

Enter system view.

system-view

Enter ERPS ring view.

erps ring ring-id

Enable R-APS packets to carry the ring ID in the destination MAC address.

r-aps ring-mac

By default, R-APS packets do not carry ring IDs in their destination MAC addresses. The last byte of the destination MAC address is 1.

### Configuring R-APS packet levels

##### Restrictions and guidelines

Perform this task on all nodes on an ERPS ring.

On a ring, the levels of R-APS packets must be the same for all nodes in an ERPS instance.

A node does not process R-APS packets whose levels are greater than the level of R-APS packets sent by the node.

##### Procedure

Enter system view.

system-view

Enter ERPS ring view.

erps ring ring-id

Enter ERPS instance view.

instance instance-id

Configure the R-APS packet level.

r-aps level level-value

By default, the level for R-APS packets is 7.

### Setting ERPS timers

##### Restrictions and guidelines

Perform this task on the owner node on an ERPS ring.

##### Procedure

Enter system view.

system-view

Enter ERPS ring view.

erps ring ring-id

Enter ERPS instance view.

instance instance-id

Set the guard timer.

timer guard guard-value

By default, the guard timer is 500 milliseconds.

Set the hold-off timer.

timer hold-off hold-off-value

By default, the hold-off timer is 0 milliseconds.

Set the WTR timer.

timer wtr wtr-value

By default, the WTR timer is 5 minutes.

### Setting the non-revertive mode

##### About setting the non-revertive mode

Perform this task if you do not want to switch back to the recovered link after the link fault is cleared.

##### Restrictions and guidelines

Perform this task on the owner node on an ERPS ring.

##### Procedure

Enter system view.

system-view

Enter ERPS ring view.

erps ring ring-id

Enter ERPS instance view.

instance instance-id

Set the non-revertive mode.

revertive-operation non-revertive

By default, revertive mode is used.

### Setting a switchover mode

##### Restrictions and guidelines

Perform this task on the nodes that you want to block their ports.

##### Procedure

Enter system view.

system-view

Set a switchover mode.

erps switch { force | manual } ring ring-id instance instance-id { port0 | port1 }

By default, no switchover mode is not set.

### Associating a ring with a subring

##### About associating a ring with a subring

On a multi-ring network, perform this task if you want to advertise topology changes in a subring to a ring.

##### Restrictions and guidelines

Perform this task on the interconnection node on an ERPS ring.

##### Procedure

Enter system view.

system-view

Enter ERPS ring view.

erps ring ring-id

Configure the ERPS ring as a subring.

ring-type sub-ring

By default, an ERPS ring is a major ring.

Enter ERPS instance view.

instance instance-id

Associate a ring with the subring.

sub-ring connect ring ring-id instance instance-id

By default, a subring is not associated with any rings.

### Enabling flush packet transparent transmission

##### About enabling flush packet transparent transmission

This feature enables the interconnection nodes to forward flush packets for topology changes in the subring to the ring associated with the subring. The associated ring can flush the MAC address table quickly to speed up convergence.

##### Restrictions and guidelines

Perform this task on the interconnection node on an ERPS ring.

To use this feature, you must also associate a subring on the interconnection node with the ring.

##### Procedure

Enter system view.

system-view

Enable flush packet transparent transmission.

erps tcn-propagation

By default, flush packet transparent transmission is disabled.

### Associating an ERPS ring member port with a track entry

##### Restrictions and guidelines

Before you associate a port with a track entry, make sure the port has joined an ERPS instance.

##### Procedure

Enter system view.

system-view

Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.

interface interface-type interface-number

Associate an ERPS ring member port with a track entry.

port erps ring ring-id instance instance-id track track-entry-index

By default, an ERPS ring member port is not associated with any track entries.

### Removing the MS mode and FS mode settings for an ERPS ring

##### About removing the MS mode and FS mode settings

After you configure this task, the owner node can ignore the WTR timer and immediately switch traffic to the recovered link upon link recovery.

This task also switches an ERPS ring in non-revertive mode to revertive mode.

##### Procedure

Enter system view.

system-view

Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.

erps clear ring ring-id instance instance-id

### Displaying and maintaining ERPS

Execute display commands in any view and reset commands in user view.

| Task | Command |
| --- | --- |
| Display brief ERPS information. | display erps |
| Display detailed ERPS information. | display erps detail ring ring-id [ instance instance-id ] |
| Display ERPS packet statistics. | display erps statistics [ ring ring-id [ instance instance-id ] ] |
| Clear ERPS packet statistics. | reset erps statistics ring ring-id [ instance instance-id ] |

### ERPS configuration examples

#### Example: Configuring one ring

##### Network configuration

As shown in Figure 12, perform the following tasks to eliminate loops on the network:

* Configure the ring as ERPS ring 1.
* Configure VLAN 100 as the control VLAN for ERPS ring 1.
* Configure VLANs 1 to 30 as the protected VLANs for ERPS ring 1.
* Configure Device A as the owner node, as ERPS ring member port 0 and the RPL port, and as ERPS ring member port 1.
* Configure Device B as the neighbor node, as ERPS ring member port 0 and the RPL port, and as ERPS ring member port 1.
* Configure Device C and Device D as normal nodes, as ERPS ring member port 0, and as ERPS ring member port 1.

Network diagram



‌

##### Procedure

Configure Device A.

# Create VLANs 1 to 30, map these VLANs to MSTI 1, and activate the MST region configuration.

<DeviceA> system-view

[DeviceA] vlan 1 to 30

[DeviceA] stp region-configuration

[DeviceA-mst-region] instance 1 vlan 1 to 30

[DeviceA-mst-region] active region-configuration

[DeviceA-mst-region] quit

# Set the link state change suppression interval to 0 seconds on .

[DeviceA] interface

[DeviceA-] link-delay 0

# Disable the spanning tree feature on the port.

[DeviceA-] undo stp enable

# Configure the port as a trunk port and assign it to VLANs 1 to 30.

[DeviceA-] port link-type trunk

[DeviceA-] port trunk permit vlan 1 to 30

[DeviceA-] quit

# Configure in the same way is configured.

[DeviceA] interface

[DeviceA-] link-delay 0

[DeviceA-] undo stp enable

[DeviceA-] port link-type trunk

[DeviceA-] port trunk permit vlan 1 to 30

[DeviceA-] quit

# Create ERPS ring 1.

[DeviceA] erps ring 1

# Configure ERPS ring member ports.

[DeviceA-erps-ring1] port0 interface

[DeviceA-erps-ring1] port1 interface

# Enable R-APS packets to carry ring ID in the destination MAC address.

[DeviceA-erps-ring1] r-aps ring-mac

# Create ERPS instance 1.

[DeviceA-erps-ring1] instance 1

# Configure the node role.

[DeviceA-erps-ring1-inst1] node-role owner rpl port0

# Configure the control VLAN.

[DeviceA-erps-ring1-inst1] control-vlan 100

# Configure the protected VLANs.

[DeviceA-erps-ring1-inst1] protected-vlan reference-instance 1

# Enable ERPS for instance 1.

[DeviceA-erps-ring1-inst1] instance enable

[DeviceA-erps-ring1-inst1] quit

[DeviceA-erps-ring1] quit

# Enable CFD, and create a level-5 MD named MD\_A.

[DeviceA] cfd enable

[DeviceA] cfd md MD\_A level 5

# Create Ethernet service instance 1, in which the MA is identified by a VLAN and serves VLAN 1.

[DeviceA] cfd service-instance 1 ma-id vlan-based md MD\_A vlan 1

# Configure a MEP list in Ethernet service instance 1, create outward-facing MEP 1001 in Ethernet service instance 1, and enable CCM sending on .

[DeviceA] cfd meplist 1001 1002 service-instance 1

[DeviceA] interface

[DeviceA-] cfd mep 1001 service-instance 1 outbound

[DeviceA-] cfd cc service-instance 1 mep 1001 enable

[DeviceA-] quit

# Create Ethernet service instance 2, in which the MA is identified by a VLAN and serves VLAN 2.

[DeviceA] cfd service-instance 2 ma-id vlan-based md MD\_A vlan 2

# Configure a MEP list in Ethernet service instance 2, create outward-facing MEP 2001 in Ethernet service instance 1, and enable CCM sending on .

[DeviceA] cfd meplist 2001 2002 service-instance 2

[DeviceA] interface

[DeviceA-] cfd mep 2001 service-instance 2 outbound

[DeviceA-] cfd cc service-instance 2 mep 2001 enable

[DeviceA-] quit

# Create track entry 1 and associate it with the CC function of CFD for MEP 1001 in Ethernet service instance 1.

[DeviceA] track 1 cfd cc service-instance 1 mep 1001

# Associate with track entry 1 and bring up the port.

[DeviceA] interface

[DeviceA-] port erps ring 1 instance 1 track 1

[DeviceA-] undo shutdown

[DeviceA-] quit

# Create track entry 2 and associate it with the CC function of CFD for MEP 2001 in Ethernet service instance 2.

[DeviceA] track 2 cfd cc service-instance 2 mep 2001

# Associate with track entry 2 and bring up the port.

[DeviceA] interface

[DeviceA-] port erps ring 1 instance 1 track 2

[DeviceA-] undo shutdown

[DeviceA-] quit

# Enable ERPS.

[DeviceA] erps enable

Configure Device B.

# Create VLANs 1 to 30, map these VLANs to MSTI 1, and activate the MST region configuration.

<DeviceB> system-view

[DeviceB] vlan 1 to 30

[DeviceB] stp region-configuration

[DeviceB-mst-region] instance 1 vlan 1 to 30

[DeviceB-mst-region] active region-configuration

[DeviceB-mst-region] quit

# Set the link state change suppression interval to 0 seconds on .

[DeviceB] interface

[DeviceB-] link-delay 0

# Disable the spanning tree feature on the port.

[DeviceB-] undo stp enable

[DeviceB-] port link-type trunk

# Configure the port as a trunk port and assign it to VLANs 1 to 30.

[DeviceB-] port trunk permit vlan 1 to 30

[DeviceB-] quit

# Configure in the same way is configured.

[DeviceB] interface

[DeviceB-] link-delay 0

[DeviceB-] undo stp enable

[DeviceB-] port link-type trunk

[DeviceB-] port trunk permit vlan 1 to 30

[DeviceB-] quit

# Create ERPS ring 1.

[DeviceB] erps ring 1

# Configure ERPS ring member ports.

[DeviceB-erps-ring1] port0 interface

[DeviceB-erps-ring1] port1 interface

# Enable R-APS packets to carry ring ID in the destination MAC address.

[DeviceB-erps-ring1] r-aps ring-mac

# Create ERPS instance 1.

[DeviceB-erps-ring1] instance 1

# Configure the node role.

[DeviceB-erps-ring1-inst1] node-role neighbor rpl port0

# Configure the control VLAN.

[DeviceB-erps-ring1-inst1] control-vlan 100

# Configure the protected VLANs.

[DeviceB-erps-ring1-inst1] protected-vlan reference-instance 1

# Enable ERPS for instance 1.

[DeviceB-erps-ring1-inst1] instance enable

[DeviceB-erps-ring1-inst1] quit

[DeviceB-erps-ring1] quit

# Enable CFD, and create a level-5 MD named MD\_A.

[DeviceB] cfd enable

[DeviceB] cfd md MD\_A level 5

# Create Ethernet service instance 1, in which the MA is identified by a VLAN and serves VLAN 1.

[DeviceB] cfd service-instance 1 ma-id vlan-based md MD\_A vlan 1

# Configure a MEP list in Ethernet service instance 1, create outward-facing MEP 1002 in Ethernet service instance 1, and enable CCM sending on .

[DeviceB] cfd meplist 1001 1002 service-instance 1

[DeviceB] interface

[DeviceB-] cfd mep 1002 service-instance 1 outbound

[DeviceB-] cfd cc service-instance 1 mep 1002 enable

[DeviceB-] quit

# Create Ethernet service instance 3, in which the MA is identified by a VLAN and serves VLAN 3.

[DeviceB] cfd service-instance 3 ma-id vlan-based md MD\_A vlan 3

# Configure a MEP list in Ethernet service instance 3, create outward-facing MEP 3002 in Ethernet service instance 1, and enable CCM sending on .

[DeviceB] cfd meplist 3001 3002 service-instance 3

[DeviceB] interface

[DeviceB-] cfd mep 3002 service-instance 3 outbound

[DeviceB-] cfd cc service-instance 3 mep 3002 enable

[DeviceB-] quit

# Create track entry 1 and associate it with the CC function of CFD for MEP 1002 in Ethernet service instance 1.

[DeviceB] track 1 cfd cc service-instance 1 mep 1002

# Associate with track entry 1 and bring up the port.

[DeviceB] interface

[DeviceB-] port erps ring 1 instance 1 track 1

[DeviceB-] undo shutdown

[DeviceB-] quit

# Create track entry 3 and associate it with the CC function of CFD for MEP 3002 in Ethernet service instance 3.

[DeviceB] track 3 cfd cc service-instance 3 mep 3002

# Associate with track entry 3 and bring up the port.

[DeviceB] interface

[DeviceB-] port erps ring 1 instance 1 track 2

[DeviceB-] undo shutdown

[DeviceB-] quit

# Enable ERPS.

[DeviceB] erps enable

Configure Device C.

# Create VLANs 1 to 30, map these VLANs to MSTI 1, and activate the MST region configuration.

<DeviceC> system-view

[DeviceC] vlan 1 to 30

[DeviceC] stp region-configuration

[DeviceC-mst-region] instance 1 vlan 1 to 30

[DeviceC-mst-region] active region-configuration

[DeviceC-mst-region] quit

# Set the link state change suppression interval to 0 seconds on .

[DeviceC] interface

[DeviceC-] link-delay 0

# Disable the spanning tree feature on the port.

[DeviceC-] undo stp enable

# Configure the port as a trunk port and assign it to VLANs 1 to 30.

[DeviceC-] port link-type trunk

[DeviceC-] port trunk permit vlan 1 to 30

[DeviceC-] quit

# Configure in the same way is configured.

[DeviceC] interface

[DeviceC-] link-delay 0

[DeviceC-] undo stp enable

[DeviceC-] port link-type trunk

[DeviceC-] port trunk permit vlan 1 to 30

[DeviceC-] quit

# Create ERPS ring 1.

[DeviceC] erps ring 1

# Configure ERPS ring member ports.

[DeviceC-erps-ring1] port0 interface

[DeviceC-erps-ring1] port1 interface

# Enable R-APS packets to carry ring ID in the destination MAC address.

[DeviceC-erps-ring1] r-aps ring-mac

# Create ERPS instance 1.

[DeviceC-erps-ring1] instance 1

# Configure the control VLAN.

[DeviceC-erps-ring1-inst1] control-vlan 100

# Configure the protected VLANs.

[DeviceC-erps-ring1-inst1] protected-vlan reference-instance 1

# Enable ERPS for instance 1.

[DeviceC-erps-ring1-inst1] instance enable

[DeviceC-erps-ring1-inst1] quit

[DeviceC-erps-ring1] quit

# Enable CFD, and create a level-5 MD named MD\_A.

[DeviceC] cfd enable

[DeviceC] cfd md MD\_A level 5

# Create Ethernet service instance 3, in which the MA is identified by a VLAN and serves VLAN 3.

[DeviceC] cfd service-instance 3 ma-id vlan-based md MD\_A vlan 3

# Configure a MEP list in Ethernet service instance 3, create outward-facing MEP 3001 in Ethernet service instance 3, and enable CCM sending on .

[DeviceC] cfd meplist 3001 3002 service-instance 3

[DeviceC] interface

[DeviceC-] cfd mep 3001 service-instance 3 outbound

[DeviceC-] cfd cc service-instance 3 mep 3001 enable

[DeviceC-] quit

# Create Ethernet service instance 4, in which the MA is identified by a VLAN and serves VLAN 4.

[DeviceC] cfd service-instance 4 ma-id vlan-based md MD\_A vlan 4

# Configure a MEP list in Ethernet service instance 4, create outward-facing MEP 4001 in Ethernet service instance 4, and enable CCM sending on .

[DeviceC] cfd meplist 4001 4002 service-instance 4

[DeviceC] interface

[DeviceC-] cfd mep 4001 service-instance 4 outbound

[DeviceC-] cfd cc service-instance 4 mep 4001 enable

[DeviceC-] quit

# Create track entry 1 and associate it with the CC function of CFD for MEP 3001 in Ethernet service instance 3.

[DeviceC] track 1 cfd cc service-instance 3 mep 3001

# Associate with track entry 1 and bring up the port.

[DeviceC] interface

[DeviceC-] port erps ring 1 instance 1 track 1

[DeviceC-] undo shutdown

[DeviceC-] quit

# Create track entry 2 and associate it with the CC function of CFD for MEP 4001 in Ethernet service instance 4.

[DeviceC] track 2 cfd cc service-instance 4 mep 4001

# Associate with track entry 3 and bring up the port.

[DeviceC] interface

[DeviceC-] port erps ring 1 instance 1 track 2

[DeviceC-] undo shutdown

[DeviceC-] quit

# Enable ERPS.

[DeviceC] erps enable

Configure Device D.

# Create VLANs 1 to 30, map these VLANs to MSTI 1, and activate the MST region configuration.

<DeviceD> system-view

[DeviceD] vlan 1 to 30

[DeviceD] stp region-configuration

[DeviceD-mst-region] instance 1 vlan 1 to 30

[DeviceD-mst-region] active region-configuration

[DeviceD-mst-region] quit

# Set the link state change suppression interval to 0 seconds on .

[DeviceD] interface

[DeviceD-] link-delay 0

# Disable the spanning tree feature on the port.

[DeviceD-] undo stp enable

# Configure the port as a trunk port and assign it to VLANs 1 to 30.

[DeviceD-] port link-type trunk

[DeviceD-] port trunk permit vlan 1 to 30

[DeviceD-] quit

# Configure in the same way is configured.

[DeviceD] interface

[DeviceD-] link-delay 0

[DeviceD-] undo stp enable

[DeviceD-] port link-type trunk

[DeviceD-] port trunk permit vlan 1 to 30

[DeviceD-] quit

# Create ERPS ring 1.

[DeviceD] erps ring 1

# Configure ERPS ring member ports.

[DeviceD-erps-ring1] port0 interface

[DeviceD-erps-ring1] port1 interface

# Enable R-APS packets to carry ring ID in the destination MAC address.

[DeviceD-erps-ring1] r-aps ring-mac

# Create ERPS instance 1.

[DeviceD-erps-ring1] instance 1

# Configure the control VLAN.

[DeviceD-erps-ring1-inst1] control-vlan 100

# Configure the protected VLANs.

[DeviceD-erps-ring1-inst1] protected-vlan reference-instance 1

# Enable ERPS for instance 1.

[DeviceD-erps-ring1-inst1] instance enable

[DeviceD-erps-ring1-inst1] quit

[DeviceD-erps-ring1] quit

# Enable CFD, and create a level-5 MD named MD\_A.

[DeviceD] cfd enable

[DeviceD] cfd md MD\_A level 5

# Create Ethernet service instance 2, in which the MA is identified by a VLAN and serves VLAN 2.

[DeviceD] cfd service-instance 2 ma-id vlan-based md MD\_A vlan 2

# Configure a MEP list in Ethernet service instance 2, create outward-facing MEP 2002 in Ethernet service instance 2, and enable CCM sending on .

[DeviceD] cfd meplist 2001 2002 service-instance 2

[DeviceD] interface

[DeviceD-] cfd mep 2002 service-instance 2 outbound

[DeviceD-] cfd cc service-instance 2 mep 2002 enable

[DeviceD-] quit

# Create Ethernet service instance 4, in which the MA is identified by a VLAN and serves VLAN 4.

[DeviceD] cfd service-instance 4 ma-id vlan-based md MD\_A vlan 4

# Configure a MEP list in Ethernet service instance 4, create outward-facing MEP 4002 in Ethernet service instance 4, and enable CCM sending on .

[DeviceD] cfd meplist 4001 4002 service-instance 4

[DeviceD] interface

[DeviceD-] cfd mep 4002 service-instance 4 outbound

[DeviceD-] cfd cc service-instance 4 mep 4002 enable

[DeviceD-] quit

# Create track entry 1 and associate it with the CC function of CFD for MEP 2002 in Ethernet service instance 2.

[DeviceD] track 1 cfd cc service-instance 2 mep 2002

# Associate with track entry 1 and bring up the port.

[DeviceD] interface

[DeviceD-] port erps ring 1 instance 1 track 1

[DeviceD-] undo shutdown

[DeviceD-] quit

# Create track entry 2 and associate it with the CC function of CFD for MEP 4002 in Ethernet service instance 4.

[DeviceD] track 2 cfd cc service-instance 4 mep 4002

# Associate with track entry 2 and bring up the port.

[DeviceD] interface

[DeviceD-] port erps ring 1 instance 1 track 2

[DeviceD-] undo shutdown

[DeviceD-] quit

# Enable ERPS.

[DeviceD] erps enable

##### Verifying the configuration

# Display information about ERPS instance 1 for Device A.

[DeviceA] display erps detail ring 1

Ring ID : 1

Port0 :

Port1 :

Subring : No

Default MAC : No

Instance ID : 1

Node role : Owner

Node state : Idle

Connect(ring/instance): -

Control VLAN : 100

Protected VLAN : Reference-instance 1

Guard timer : 500 ms

Hold-off timer : 0 ms

WTR timer : 5 min

Revertive operation : Revertive

Enable status : Yes, Active status : Yes

R-APS level : 7

Port PortRole PortStatus

----------------------------------------------------------------------------

Port0 RPL Block

Port1 Non-RPL Up

The output shows the following information:

* Device A is the owner node.
* The ERPS ring is in idle state.
* The RPL port is blocked.
* The non-RPL port is unblocked.

#### Example: Configuring one subring

##### Network configuration

As shown in Figure 13, perform the following tasks to eliminate loops on the network:

* Configure VLAN 100 and VLAN 200 as the control VLANs for the major ring and the subring, respectively.
* Configure VLANs 1 to 30 as the protected VLANs for the major ring and subring.
* Configure Device A as the owner node for the major ring, as ERPS ring member port 0 and the RPL port, and as ERPS ring member port 1.
* Configure Device B as the neighbor node for the major ring, as ERPS ring member port 0 and the RPL port, and as ERPS ring member port 1.
* Configure Devices C and D as interconnection nodes, as ERPS ring member port 0, as ERPS ring member port 1, and GigabitEthernet 1/0/3 as the interconnection port.
* Configure Device E as the owner node for the subring, as ERPS ring member port 0 and the RPL port, and as ERPS ring member port 1.
* Configure Device F as the neighbor node for the subring, as ERPS ring member port 0 and the RPL port, and as ERPS ring member port 1.

Network diagram



‌

##### Procedure

Configure Device A.

# Create VLANs 1 to 30, map these VLANs to MSTI 1, and activate the MST region configuration.

<DeviceA> system-view

[DeviceA] vlan 1 to 30

[DeviceA] stp region-configuration

[DeviceA-mst-region] instance 1 vlan 1 to 30

[DeviceA-mst-region] active region-configuration

[DeviceA-mst-region] quit

# Set the link state change suppression interval to 0 seconds on .

[DeviceA] interface

[DeviceA-] link-delay 0

# Disable the spanning tree feature on the port.

[DeviceA-] undo stp enable

# Configure the port as a trunk port and assign it to VLANs 1 to 30.

[DeviceA-] port link-type trunk

[DeviceA-] port trunk permit vlan 1 to 30

[DeviceA-] quit

# Configure in the same way is configured.

[DeviceA] interface

[DeviceA-] link-delay 0

[DeviceA-] undo stp enable

[DeviceA-] port link-type trunk

[DeviceA-] port trunk permit vlan 1 to 30

[DeviceA-] quit

# Create ERPS ring 1.

[DeviceA] erps ring 1

# Configure ERPS ring member ports.

[DeviceA-erps-ring1] port0 interface

[DeviceA-erps-ring1] port1 interface

# Create ERPS instance 1.

[DeviceA-erps-ring1] instance 1

# Configure the node role.

[DeviceA-erps-ring1-inst1] node-role owner rpl port0

# Configure the control VLAN.

[DeviceA-erps-ring1-inst1] control-vlan 100

# Configure the protected VLANs.

[DeviceA-erps-ring1-inst1] protected-vlan reference-instance 1

# Enable ERPS for instance 1.

[DeviceA-erps-ring1-inst1] instance enable

[DeviceA-erps-ring1-inst1] quit

[DeviceA-erps-ring1] quit

# Enable CFD, and create a level-5 MD named MD\_A.

[DeviceA] cfd enable

[DeviceA] cfd md MD\_A level 5

# Create Ethernet service instance 1, in which the MA is identified by a VLAN and serves VLAN 1.

[DeviceA] cfd service-instance 1 ma-id vlan-based md MD\_A vlan 1

# Configure a MEP list in Ethernet service instance 1, create outward-facing MEP 1001 in Ethernet service instance 1, and enable CCM sending on .

[DeviceA] cfd meplist 1001 1002 service-instance 1

[DeviceA] interface

[DeviceA-] cfd mep 1001 service-instance 1 outbound

[DeviceA-] cfd cc service-instance 1 mep 1001 enable

[DeviceA-] quit

# Create Ethernet service instance 2, in which the MA is identified by a VLAN and serves VLAN 2.

[DeviceA] cfd service-instance 2 ma-id vlan-based md MD\_A vlan 2

# Configure a MEP list in Ethernet service instance 2, create outward-facing MEP 2001 in Ethernet service instance 1, and enable CCM sending on .

[DeviceA] cfd meplist 2001 2002 service-instance 2

[DeviceA] interface

[DeviceA-] cfd mep 2001 service-instance 2 outbound

[DeviceA-] cfd cc service-instance 2 mep 2001 enable

[DeviceA-] quit

# Create track entry 1 and associate it with the CC function of CFD for MEP 1001 in Ethernet service instance 1.

[DeviceA] track 1 cfd cc service-instance 1 mep 1001

# Associate with track entry 1 and bring up the port.

[DeviceA] interface

[DeviceA-] port erps ring 1 instance 1 track 1

[DeviceA-] undo shutdown

[DeviceA-] quit

# Create track entry 2 and associate it with the CC function of CFD for MEP 2001 in Ethernet service instance 2.

[DeviceA] track 2 cfd cc service-instance 2 mep 2001

# Associate with track entry 2 and bring up the port.

[DeviceA] interface

[DeviceA-] port erps ring 1 instance 1 track 2

[DeviceA-] undo shutdown

[DeviceA-] quit

# Enable ERPS.

[DeviceA] erps enable

Configure Device B.

# Create VLANs 1 to 30, map these VLANs to MSTI 1, and activate the MST region configuration.

<DeviceB> system-view

[DeviceB] vlan 1 to 30

[DeviceB] stp region-configuration

[DeviceB-mst-region] instance 1 vlan 1 to 30

[DeviceB-mst-region] active region-configuration

[DeviceB-mst-region] quit

# Set the link state change suppression interval to 0 seconds on .

[DeviceB] interface

[DeviceB-] link-delay 0

# Disable the spanning tree feature on the port.

[DeviceB-] undo stp enable

# Configure the port as a trunk port and assign it to VLANs 1 to 30.

[DeviceB-] port link-type trunk

[DeviceB-] port trunk permit vlan 1 to 30

[DeviceB-] quit

# Configure in the same way is configured.

[DeviceB] interface

[DeviceB-] link-delay 0

[DeviceB-] undo stp enable

[DeviceB-] port link-type trunk

[DeviceB-] port trunk permit vlan 1 to 30

[DeviceB-] quit

# Create ERPS ring 1.

[DeviceB] erps ring 1

# Configure ERPS ring member ports.

[DeviceB-erps-ring1] port0 interface

[DeviceB-erps-ring1] port1 interface

# Create ERPS instance 1.

[DeviceB-erps-ring1] instance 1

# Configure the node role.

[DeviceB-erps-ring1-inst1] node-role neighbor rpl port0

# Configure the control VLAN.

[DeviceB-erps-ring1-inst1] control-vlan 100

# Configure the protected VLANs.

[DeviceB-erps-ring1-inst1] protected-vlan reference-instance 1

# Enable ERPS for instance 1.

[DeviceB-erps-ring1-inst1] instance enable

[DeviceB-erps-ring1-inst1] quit

[DeviceB-erps-ring1] quit

# Enable CFD, and create a level-5 MD named MD\_A.

[DeviceB] cfd enable

[DeviceB] cfd md MD\_A level 5

# Create Ethernet service instance 1, in which the MA is identified by a VLAN and serves VLAN 1.

[DeviceB] cfd service-instance 1 ma-id vlan-based md MD\_A vlan 1

# Configure a MEP list in Ethernet service instance 1, create outward-facing MEP 1002 in Ethernet service instance 1, and enable CCM sending on .

[DeviceB] cfd meplist 1001 1002 service-instance 1

[DeviceB] interface

[DeviceB-] cfd mep 1002 service-instance 1 outbound

[DeviceB-] cfd cc service-instance 1 mep 1002 enable

[DeviceB-] quit

# Create Ethernet service instance 3, in which the MA is identified by a VLAN and serves VLAN 3.

[DeviceB] cfd service-instance 3 ma-id vlan-based md MD\_A vlan 3

# Configure a MEP list in Ethernet service instance 3, create outward-facing MEP 3002 in Ethernet service instance 2, and enable CCM sending on .

[DeviceB] cfd meplist 3001 3002 service-instance 3

[DeviceB] interface

[DeviceB-] cfd mep 3002 service-instance 3 outbound

[DeviceB-] cfd cc service-instance 3 mep 3002 enable

[DeviceB-] quit

# Create track entry 1 and associate it with the CC function of CFD for MEP 1002 in Ethernet service instance 1.

[DeviceB] track 1 cfd cc service-instance 1 mep 1002

# Associate with track entry 1 and bring up the port.

[DeviceB] interface

[DeviceB-] port erps ring 1 instance 1 track 1

[DeviceB-] undo shutdown

[DeviceB-] quit

# Create track entry 3 and associate it with the CC function of CFD for MEP 3002 in Ethernet service instance 3.

[DeviceB] track 3 cfd cc service-instance 3 mep 3002

# Associate with track entry 3 and bring up the port.

[DeviceB] interface

[DeviceB-] port erps ring 1 instance 1 track 2

[DeviceB-] undo shutdown

[DeviceB-] quit

# Enable ERPS.

[DeviceB] erps enable

Configure Device C.

# Create VLANs 1 to 30, map these VLANs to MSTI 1, and activate the MST region configuration.

<DeviceC> system-view

[DeviceC] vlan 1 to 30

[DeviceC] stp region-configuration

[DeviceC-mst-region] instance 1 vlan 1 to 30

[DeviceC-mst-region] active region-configuration

[DeviceC-mst-region] quit

# Set the link state change suppression interval to 0 seconds on .

[DeviceC] interface

[DeviceC-] link-delay 0

# Disable the spanning tree feature on the port.

[DeviceC-] undo stp enable

# Configure the port as a trunk port and assign it to VLANs 1 to 30.

[DeviceC-] port link-type trunk

[DeviceC-] port trunk permit vlan 1 to 30

[DeviceC-] quit

# Configure in the same way is configured.

[DeviceC] interface

[DeviceC-] link-delay 0

[DeviceC-] undo stp enable

[DeviceC-] port link-type trunk

[DeviceC-] port trunk permit vlan 1 to 30

[DeviceC-] quit

# Configure in the same way is configured.

[DeviceC] interface

[DeviceC-] link-delay 0

[DeviceC-] undo stp enable

[DeviceC-] port link-type trunk

[DeviceC-] port trunk permit vlan 1 to 30

[DeviceC-] quit

# Create ERPS ring 1.

[DeviceC] erps ring 1

# Configure ERPS ring member ports.

[DeviceC-erps-ring1] port0 interface

[DeviceC-erps-ring1] port1 interface

# Create ERPS instance 1.

[DeviceC-erps-ring1] instance 1

# Configure the control VLAN.

[DeviceC-erps-ring1-inst1] control-vlan 100

# Configure the protected VLANs.

[DeviceC-erps-ring1-inst1] protected-vlan reference-instance 1

# Enable ERPS for instance 1.

[DeviceC-erps-ring1-inst1] instance enable

[DeviceC-erps-ring1-inst1] quit

[DeviceC-erps-ring1] quit

# Enable CFD, and create a level-5 MD named MD\_A.

[DeviceC] cfd enable

[DeviceC] cfd md MD\_A level 5

# Create Ethernet service instance 3, in which the MA is identified by a VLAN and serves VLAN 3.

[DeviceC] cfd service-instance 3 ma-id vlan-based md MD\_A vlan 3

# Configure a MEP list in Ethernet service instance 3, create outward-facing MEP 3001 in Ethernet service instance 3, and enable CCM sending on .

[DeviceC] cfd meplist 3001 3002 service-instance 3

[DeviceC] interface

[DeviceC-] cfd mep 3001 service-instance 3 outbound

[DeviceC-] cfd cc service-instance 3 mep 3001 enable

[DeviceC-] quit

# Create Ethernet service instance 4, in which the MA is identified by a VLAN and serves VLAN 4.

[DeviceC] cfd service-instance 4 ma-id vlan-based md MD\_A vlan 4

# Configure a MEP list in Ethernet service instance 4, create outward-facing MEP 4001 in Ethernet service instance 4, and enable CCM sending on .

[DeviceC] cfd meplist 4001 4002 service-instance 4

[DeviceC] interface

[DeviceC-] cfd mep 4001 service-instance 4 outbound

[DeviceC-] cfd cc service-instance 4 mep 4001 enable

[DeviceC-] quit

# Create track entry 1 and associate it with the CC function of CFD for MEP 3001 in Ethernet service instance 3.

[DeviceC] track 1 cfd cc service-instance 3 mep 3001

# Associate with track entry 1 and bring up the port.

[DeviceC] interface

[DeviceC-] port erps ring 1 instance 1 track 1

[DeviceC-] undo shutdown

[DeviceC-] quit

# Create track entry 2 and associate it with the CC function of CFD for MEP 4001 in Ethernet service instance 4.

[DeviceC] track 2 cfd cc service-instance 4 mep 4001

# Associate with track entry 2 and bring up the port.

[DeviceC] interface

[DeviceC-] port erps ring 1 instance 1 track 2

[DeviceC-] undo shutdown

[DeviceC-] quit

# Create ERPS ring 2.

[DeviceC] erps ring 2

# Configure ERPS ring member ports.

[DeviceC-erps-ring2] port0 interface

# Configure ERPS ring 2 as the subring.

[DeviceC-erps-ring2] ring-type sub-ring

# Create ERPS instance 1.

[DeviceC-erps-ring2] instance 1

# Configure the node role.

[DeviceC-erps-ring2-inst1] node-role interconnection port0

# Configure the control VLAN.

[DeviceC-erps-ring2-inst1] control-vlan 110

# Configure the protected VLANs.

[DeviceC-erps-ring2-inst1] protected-vlan reference-instance 1

# Enable ERPS for instance 1.

[DeviceC-erps-ring2-inst1] instance enable

[DeviceC-erps-ring2-inst1] quit

[DeviceC-erps-ring2] quit

# Create Ethernet service instance 5, in which the MA is identified by a VLAN and serves VLAN 5.

[DeviceC] cfd service-instance 5 ma-id vlan-based md MD\_A vlan 5

# Configure a MEP list in Ethernet service instance 5, create outward-facing MEP 5001 in Ethernet service instance 3, and enable CCM sending on .

[DeviceC] cfd meplist 5001 5002 service-instance 5

[DeviceC] interface

[DeviceC-] cfd mep 5001 service-instance 5 outbound

[DeviceC-] cfd cc service-instance 5 mep 5001 enable

[DeviceC-] quit

# Create track entry 1 and associate it with the CC function of CFD for MEP 5001 in Ethernet service instance 3.

[DeviceC] track 1 cfd cc service-instance 5 mep 5001

# Associate with track entry 1 and bring up the port.

[DeviceC] interface

[DeviceC-] port erps ring 2 instance 1 track 1

[DeviceC-] undo shutdown

[DeviceC-] quit

# Enable ERPS.

[DeviceC] erps enable

Configure Device D.

# Create VLANs 1 to 30, map these VLANs to MSTI 1, and activate the MST region configuration.

<DeviceD> system-view

[DeviceD] vlan 1 to 30

[DeviceD] stp region-configuration

[DeviceD-mst-region] instance 1 vlan 1 to 30

[DeviceD-mst-region] active region-configuration

[DeviceD-mst-region] quit

# Set the link state change suppression interval to 0 seconds on .

[DeviceD] interface

[DeviceD-] link-delay 0

# Disable the spanning tree feature on the port.

[DeviceD-] undo stp enable

# Configure the port as a trunk port and assign it to VLANs 1 to 30.

[DeviceD-] port link-type trunk

[DeviceD-] port trunk permit vlan 1 to 30

[DeviceD-] quit

# Configure in the same way is configured.

[DeviceD] interface

[DeviceD-] link-delay 0

[DeviceD-] undo stp enable

[DeviceD-] port link-type trunk

[DeviceD-] port trunk permit vlan 1 to 30

[DeviceD-] quit

# Configure in the same way is configured.

[DeviceD] interface

[DeviceD-] link-delay 0

[DeviceD-] undo stp enable

[DeviceD-] port link-type trunk

[DeviceD-] port trunk permit vlan 1 to 30

[DeviceD-] quit

# Create ERPS ring 1.

[DeviceD] erps ring 1

# Configure ERPS ring member ports.

[DeviceD-erps-ring1] port0 interface

[DeviceD-erps-ring1] port1 interface

# Create ERPS instance 1.

[DeviceD-erps-ring1] instance 1

# Configure the control VLAN.

[DeviceD-erps-ring1-inst1] control-vlan 100

# Configure the protected VLANs.

[DeviceD-erps-ring1-inst1] protected-vlan reference-instance 1

# Enable ERPS for instance 1.

[DeviceD-erps-ring1-inst1] instance enable

[DeviceD-erps-ring1-inst1] quit

[DeviceD-erps-ring1] quit

# Enable CFD, and create a level-5 MD named MD\_A.

[DeviceD] cfd enable

[DeviceD] cfd md MD\_A level 5

# Create Ethernet service instance 2, in which the MA is identified by a VLAN and serves VLAN 2.

[DeviceD] cfd service-instance 2 ma-id vlan-based md MD\_A vlan 2

# Configure a MEP list in Ethernet service instance 2, create outward-facing MEP 2002 in Ethernet service instance 2, and enable CCM sending on .

[DeviceD] cfd meplist 2001 2002 service-instance 2

[DeviceD] interface

[DeviceD-] cfd mep 2002 service-instance 2 outbound

[DeviceD-] cfd cc service-instance 2 mep 2002 enable

[DeviceD-] quit

# Create Ethernet service instance 4, in which the MA is identified by a VLAN and serves VLAN 4.

[DeviceD] cfd service-instance 4 ma-id vlan-based md MD\_A vlan 4

# Configure a MEP list in Ethernet service instance 4, create outward-facing MEP 4002 in Ethernet service instance 4, and enable CCM sending on .

[DeviceD] cfd meplist 4001 4002 service-instance 4

[DeviceD] interface

[DeviceD-] cfd mep 4002 service-instance 4 outbound

[DeviceD-] cfd cc service-instance 4 mep 4002 enable

[DeviceD-] quit

# Create track entry 1 and associate it with the CC function of CFD for MEP 2002 in Ethernet service instance 2.

[DeviceD] track 1 cfd cc service-instance 2 mep 2002

# Associate with track entry 1 and bring up the port.

[DeviceD] interface

[DeviceD-] port erps ring 1 instance 1 track 1

[DeviceD-] undo shutdown

[DeviceD-] quit

# Create track entry 2 and associate it with the CC function of CFD for MEP 4002 in Ethernet service instance 4.

[DeviceD] track 2 cfd cc service-instance 4 mep 4002

# Associate with track entry 2 and bring up the port.

[DeviceD] interface

[DeviceD-] port erps ring 1 instance 1 track 2

[DeviceD-] undo shutdown

[DeviceD-] quit

# Create ERPS ring 2.

[DeviceD] erps ring 2

# Configure ERPS ring member ports.

[DeviceD-erps-ring2] port0 interface

# Configure ERPS ring 2 as the subring.

[DeviceD-erps-ring2] ring-type sub-ring

# Create ERPS instance 1.

[DeviceD-erps-ring2] instance 1

# Configure the node role.

[DeviceD-erps-ring2-inst1] node-role interconnection port0

# Configure the control VLAN.

[DeviceD-erps-ring2-inst1] control-vlan 110

# Configure the protected VLANs.

[DeviceD-erps-ring2-inst1] protected-vlan reference-instance 1

# Enable ERPS for instance 1.

[DeviceD-erps-ring2-inst1] instance enable

[DeviceD-erps-ring2-inst1] quit

[DeviceD-erps-ring2] quit

# Create Ethernet service instance 6, in which the MA is identified by a VLAN and serves VLAN 6.

[DeviceD] cfd service-instance 6 ma-id vlan-based md MD\_A vlan 6

# Configure a MEP list in Ethernet service instance 6, create outward-facing MEP 6002 in Ethernet service instance 3, and enable CCM sending on .

[DeviceD] cfd meplist 6001 6002 service-instance 6

[DeviceD] interface

[DeviceD-] cfd mep 6002 service-instance 6 outbound

[DeviceD-] cfd cc service-instance 6 mep 6002 enable

[DeviceD-] quit

# Create track entry 3 and associate it with the CC function of CFD for MEP 6002 in Ethernet service instance 6.

[DeviceD] track 3 cfd cc service-instance 6 mep 6002

# Associate with track entry 3 and bring up the port.

[DeviceD] interface

[DeviceD-] port erps ring 2 instance 1 track 3

[DeviceD-] undo shutdown

[DeviceD-] quit

# Enable ERPS.

[DeviceD] erps enable

Configure Device E.

# Create VLANs 1 to 30, map these VLANs to MSTI 1, and activate the MST region configuration.

<DeviceE> system-view

[DeviceE] vlan 1 to 30

[DeviceE] stp region-configuration

[DeviceE-mst-region] instance 1 vlan 1 to 30

[DeviceE-mst-region] active region-configuration

[DeviceE-mst-region] quit

# Set the link state change suppression interval to 0 seconds on .

[DeviceE] interface

[DeviceE-] link-delay 0

# Disable the spanning tree feature on the port.

[DeviceE-] undo stp enable

# Configure the port as a trunk port and assign it to VLANs 1 to 30.

[DeviceE-] port link-type trunk

[DeviceE-] port trunk permit vlan 1 to 30

[DeviceE-] quit

# Configure in the same way is configured.

[DeviceE] interface

[DeviceE-] link-delay 0

[DeviceE-] undo stp enable

[DeviceE-] port link-type trunk

[DeviceE-] port trunk permit vlan 1 to 30

[DeviceE-] quit

# Create ERPS ring 2.

[DeviceE] erps ring 2

# Configure ERPS ring member ports.

[DeviceE-erps-ring2] port0 interface

[DeviceE-erps-ring2] port1 interface

# Configure ERPS ring 2 as the subring.

[DeviceE-erps-ring2] ring-type sub-ring

# Create ERPS instance 1.

[DeviceE-erps-ring2] instance 1

# Configure the node role.

[DeviceE-erps-ring2] node-role owner rpl port0

# Configure the control VLAN.

[DeviceE-erps-ring2-inst1] control-vlan 110

# Configure the protected VLANs.

[DeviceE-erps-ring2-inst1] protected-vlan reference-instance 1

# Enable ERPS for instance 1.

[DeviceE-erps-ring2-inst1] instance enable

[DeviceE-erps-ring2-inst1] quit

[DeviceE-erps-ring2] quit

# Enable CFD, and create a level-5 MD named MD\_A.

[DeviceE] cfd enable

[DeviceE] cfd md MD\_A level 5

# Create Ethernet service instance 6, in which the MA is identified by a VLAN and serves VLAN 6.

[DeviceE] cfd service-instance 6 ma-id vlan-based md MD\_A vlan 6

# Configure a MEP list in Ethernet service instance 6, create outward-facing MEP 6001 in Ethernet service instance 6, and enable CCM sending on .

[DeviceE] cfd meplist 6001 6002 service-instance 6

[DeviceE] interface

[DeviceE-] cfd mep 6001 service-instance 6 outbound

[DeviceE-] cfd cc service-instance 6 mep 6001 enable

[DeviceE-] quit

# Create Ethernet service instance 7, in which the MA is identified by a VLAN and serves VLAN 7.

[DeviceE] cfd service-instance 7 ma-id vlan-based md MD\_A vlan 7

# Configure a MEP list in Ethernet service instance 7, create outward-facing MEP 7001 in Ethernet service instance 7, and enable CCM sending on .

[DeviceE] cfd meplist 7001 7002 service-instance 7

[DeviceE] interface

[DeviceE-] cfd mep 7001 service-instance 7 outbound

[DeviceE-] cfd cc service-instance 7 mep 7001 enable

[DeviceE-] quit

# Create track entry 1 and associate it with the CC function of CFD for MEP 6001 in Ethernet service instance 6.

[DeviceE] track 1 cfd cc service-instance 6 mep 6001

# Associate with track entry 1 and bring up the port.

[DeviceE] interface

[DeviceE-] port erps ring 2 instance 1 track 1

[DeviceE-] undo shutdown

[DeviceE-] quit

# Create track entry 2 and associate it with the CC function of CFD for MEP 7001 in Ethernet service instance 7.

[DeviceE] track 2 cfd cc service-instance 7 mep 7001

# Associate with track entry 2 and bring up the port.

[DeviceE] interface

[DeviceE-] port erps ring 2 instance 1 track 2

[DeviceE-] undo shutdown

[DeviceE-] quit

# Enable ERPS.

[DeviceE] erps enable

Configure Device F.

# Create VLANs 1 to 30, map these VLANs to MSTI 1, and activate the MST region configuration.

<DeviceF> system-view

[DeviceF] vlan 1 to 30

[DeviceF] stp region-configuration

[DeviceF-mst-region] instance 1 vlan 1 to 30

[DeviceF-mst-region] active region-configuration

[DeviceF-mst-region] quit

# Set the link state change suppression interval to 0 seconds on .

[DeviceF] interface

[DeviceF-] link-delay 0

# Disable the spanning tree feature on the port.

[DeviceF-] undo stp enable

[DeviceF-] port link-type trunk

# Configure the port as a trunk port and assign it to VLANs 1 to 30.

[DeviceF-] port trunk permit vlan 1 to 30

[DeviceF-] quit

# Configure in the same way is configured.

[DeviceF] interface

[DeviceF-] link-delay 0

[DeviceF-] undo stp enable

[DeviceF-] port link-type trunk

[DeviceF-] port trunk permit vlan 1 to 30

[DeviceF-] quit

# Create ERPS ring 2.

[DeviceF] erps ring 2

# Configure ERPS ring member ports.

[DeviceF-erps-ring2] port0 interface

[DeviceF-erps-ring2] port1 interface

# Configure ERPS ring 2 as the subring.

[DeviceF-erps-ring2] ring-type sub-ring

# Create ERPS instance 1.

[DeviceF-erps-ring2] instance 1

# Configure the node role.

[DeviceF-erps-ring2] node-role neighbor rpl port0

# Configure the control VLAN.

[DeviceF-erps-ring2-inst1] control-vlan 110

# Configure the protected VLANs.

[DeviceF-erps-ring2-inst1] protected-vlan reference-instance 1

# Enable ERPS for instance 1.

[DeviceF-erps-ring2-inst1] instance enable

[DeviceF-erps-ring2-inst1] quit

[DeviceF-erps-ring2] quit

# Enable CFD, and create a level-5 MD named MD\_A.

[DeviceF] cfd enable

[DeviceF] cfd md MD\_A level 5

# Create Ethernet service instance 5, in which the MA is identified by a VLAN and serves VLAN 5.

[DeviceF] cfd service-instance 5 ma-id vlan-based md MD\_A vlan 5

# Configure a MEP list in Ethernet service instance 5, create outward-facing MEP 5002 in Ethernet service instance 5, and enable CCM sending on .

[DeviceF] cfd meplist 5001 5002 service-instance 5

[DeviceF] interface

[DeviceF-] cfd mep 5002 service-instance 5 outbound

[DeviceF-] cfd cc service-instance 5 mep 5002 enable

[DeviceF-] quit

# Create Ethernet service instance 7, in which the MA is identified by a VLAN and serves VLAN 7.

[DeviceF] cfd service-instance 7 ma-id vlan-based md MD\_A vlan 7

# Configure a MEP list in Ethernet service instance 7, create outward-facing MEP 7002 in Ethernet service instance 7, and enable CCM sending on .

[DeviceF] cfd meplist 7001 7002 service-instance 7

[DeviceF] interface

[DeviceF-] cfd mep 7002 service-instance 7 outbound

[DeviceF-] cfd cc service-instance 7 mep 7002 enable

[DeviceF-] quit

# Create track entry 1 and associate it with the CC function of CFD for MEP 5001 in Ethernet service instance 5.

[DeviceF] track 1 cfd cc service-instance 5 mep 5002

# Associate with track entry 1 and bring up the port.

[DeviceF] interface

[DeviceF-] port erps ring 2 instance 1 track 1

[DeviceF-] undo shutdown

[DeviceF-] quit

# Create track entry 2 and associate it with the CC function of CFD for MEP 7002 in Ethernet service instance 7.

[DeviceF] track 2 cfd cc service-instance 7 mep 7002

# Associate with track entry 2 and bring up the port.

[DeviceF] interface

[DeviceF-] port erps ring 2 instance 1 track 2

[DeviceF-] undo shutdown

[DeviceF-] quit

# Enable ERPS.

[DeviceF] erps enable

##### Verifying the configuration

# Display information about ERPS instance 1 for Device A.

[Device A] display erps detail ring 1

Ring ID : 1

Port0 :

Port1 :

Subring : Yes

Default MAC : No

Instance ID : 1

Node role : Owner

Node state : Idle

Connect(ring/instance): -

Control VLAN : 100

Protected VLAN : Reference-instance 1

Guard timer : 500 ms

Hold-off timer : 0 ms

WTR timer : 5 min

Revertive operation : Revertive

Enable status : Yes, Active status : Yes

R-APS level : 7

Port PortRole PortStatus

----------------------------------------------------------------------------

Port0 RPL Block

Port1 Non-RPL Up

The output shows the following information:

* Device A is the owner node.
* The ERPS ring is in idle state.
* The RPL port is blocked.
* The non-RPL port is unblocked.

#### Example: Configuring one-ring multi-instance load balancing

##### Network configuration

As shown in Figure 14, perform the following tasks to improve network resource utilization and implement load balancing among links:

* Configure ERPS instances 1 and 2 on the ERPS ring.
* For ERPS instance 1, configure the following items:
  + Configure Device A as the owner node.
  + Configure the link between Devices A and Device B as the RPL.
  + Configure VLAN 100 as the control VLAN.
  + Configure VLANs 1 to 30 as the protected VLANs.
* For ERPS instance 2, configure the following items:
  + Configure Device A as the owner node.
  + Configure the link between Devices C and Device D as the RPL.
  + Configure VLAN 100 as the control VLAN.
  + Configure VLANs 31 to 60 as the protected VLANs.

Network diagram



‌

##### Procedure

Configure Device A.

# Create VLANs 1 to 60, map VLANs 1 to 30 to MSTI 1, map VLANs 31 to 60 to MSTI 2, and activate the MST region configuration.

<DeviceA> system-view

[DeviceA] vlan 1 to 60

[DeviceA] stp region-configuration

[DeviceA-mst-region] instance 1 vlan 1 to 30

[DeviceA-mst-region] instance 2 vlan 31 to 60

[DeviceA-mst-region] active region-configuration

[DeviceA-mst-region] quit

# Set the link state change suppression interval to 0 seconds on .

[DeviceA] interface

[DeviceA-] link-delay 0

# Disable the spanning tree feature on the port.

[DeviceA-] undo stp enable

# Configure the port as a trunk port and assign it to VLANs 1 to 60.

[DeviceA-] port link-type trunk

[DeviceA-] port trunk permit vlan 1 to 60

[DeviceA-] quit

# Configure in the same way is configured.

[DeviceA] interface

[DeviceA-] link-delay 0

[DeviceA-] undo stp enable

[DeviceA-] port link-type trunk

[DeviceA-] port trunk permit vlan 1 to 60

[DeviceA-] quit

# Create ERPS ring 1.

[DeviceA] erps ring 1

# Configure ERPS ring member ports.

[DeviceA-erps-ring1] port0 interface

[DeviceA-erps-ring1] port1 interface

# Create ERPS instance 1.

[DeviceA-erps-ring1] instance 1

# Configure the node role.

[DeviceA-erps-ring1-inst1] node-role owner rpl port0

# Configure the control VLAN.

[DeviceA-erps-ring1-inst1] control-vlan 100

# Configure the protected VLANs.

[DeviceA-erps-ring1-inst1] protected-vlan reference-instance 1

# Enable ERPS for instance 1.

[DeviceA-erps-ring1-inst1] instance enable

[DeviceA-erps-ring1-inst1] quit

[DeviceA-erps-ring1] quit

# Create ERPS instance 2.

[DeviceA-erps-ring1] instance 2

# Configure the control VLAN.

[DeviceA-erps-ring1-inst2] control-vlan 110

# Configure the protected VLANs.

[DeviceA-erps-ring1-inst2] protected-vlan reference-instance 2

# Enable ERPS for instance 2.

[DeviceA-erps-ring1-inst2] instance enable

[DeviceA-erps-ring1-inst2] quit

[DeviceA-erps-ring1] quit

# Enable CFD, and create a level-5 MD named MD\_A.

[DeviceA] cfd enable

[DeviceA] cfd md MD\_A level 5

# Create Ethernet service instance 1, in which the MA is identified by a VLAN and serves VLAN 1.

[DeviceA] cfd service-instance 1 ma-id vlan-based md MD\_A vlan 1

# Configure a MEP list in Ethernet service instance 1, create outward-facing MEP 1001 in Ethernet service instance 1, and enable CCM sending on .

[DeviceA] cfd meplist 1001 1002 service-instance 1

[DeviceA] interface

[DeviceA-] cfd mep 1001 service-instance 1 outbound

[DeviceA-] cfd cc service-instance 1 mep 1001 enable

[DeviceA-] quit

# Create Ethernet service instance 2, in which the MA is identified by a VLAN and serves VLAN 2.

[DeviceA] cfd service-instance 2 ma-id vlan-based md MD\_A vlan 2

# Configure a MEP list in Ethernet service instance 2, create outward-facing MEP 2001 in Ethernet service instance 1, and enable CCM sending on .

[DeviceA] cfd meplist 2001 2002 service-instance 2

[DeviceA] interface

[DeviceA-] cfd mep 2001 service-instance 2 outbound

[DeviceA-] cfd cc service-instance 2 mep 2001 enable

[DeviceA-] quit

# Create track entry 1 and associate it with the CC function of CFD for MEP 1001 in Ethernet service instance 1.

[DeviceA] track 1 cfd cc service-instance 1 mep 1001

# Associate with track entry 1 and bring up the port for ERPS instances 1 and 2.

[DeviceA] interface

[DeviceA-] port erps ring 1 instance 1 track 1

[DeviceA-] port erps ring 1 instance 2 track 1

[DeviceA-] undo shutdown

[DeviceA-] quit

# Create track entry 2 and associate it with the CC function of CFD for MEP 2001 in Ethernet service instance 2.

[DeviceA] track 2 cfd cc service-instance 2 mep 2001

# Associate with track entry 2 and bring up the port for ERPS instances 1 and 2.

[DeviceA] interface

[DeviceA-] port erps ring 1 instance 1 track 2

[DeviceA-] port erps ring 1 instance 2 track 2

[DeviceA-] undo shutdown

[DeviceA-] quit

# Enable ERPS.

[DeviceA] erps enable

Configure Device B.

# Create VLANs 1 to 60, map VLANs 1 to 30 to MSTI 1, map VLANs 31 to 60 to MSTI 2, and activate the MST region configuration.

<DeviceB> system-view

[DeviceB] vlan 1 to 60

[DeviceB] stp region-configuration

[DeviceB-mst-region] instance 1 vlan 1 to 30

[DeviceB-mst-region] instance 2 vlan 31 to 60

[DeviceB-mst-region] active region-configuration

[DeviceB-mst-region] quit

# Set the link state change suppression interval to 0 seconds on .

[DeviceB] interface

[DeviceB-] link-delay 0

# Disable the spanning tree feature on the port.

[DeviceB-] undo stp enable

# Configure the port as a trunk port and assign it to VLANs 1 to 60.

[DeviceB-] port link-type trunk

[DeviceB-] port trunk permit vlan 1 to 60

[DeviceB-] quit

# Configure in the same way is configured.

[DeviceB] interface

[DeviceB-] link-delay 0

[DeviceB-] undo stp enable

[DeviceB-] port link-type trunk

[DeviceB-] port trunk permit vlan 1 to 60

[DeviceB-] quit

# Create ERPS ring 1.

[DeviceB] erps ring 1

# Configure ERPS ring member ports.

[DeviceB-erps-ring1] port0 interface

[DeviceB-erps-ring1] port1 interface

# Create ERPS instance 1.

[DeviceB-erps-ring1] instance 1

# Configure the node role.

[DeviceB-erps-ring1-inst1] node-role neighbor rpl port0

# Configure the control VLAN.

[DeviceB-erps-ring1-inst1] control-vlan 100

# Configure the protected VLANs.

[DeviceB-erps-ring1-inst1] protected-vlan reference-instance 1

# Enable ERPS for instance 1.

[DeviceB-erps-ring1-inst1] instance enable

[DeviceB-erps-ring1-inst1] quit

[DeviceB-erps-ring1] quit

# Create ERPS instance 2.

[DeviceB-erps-ring1] instance 2

# Configure the control VLAN.

[DeviceB-erps-ring1-inst2] control-vlan 110

# Configure the protected VLANs.

[DeviceB-erps-ring1-inst2] protected-vlan reference-instance 2

# Enable ERPS for instance 2.

[DeviceB-erps-ring1-inst2] instance enable

[DeviceB-erps-ring1-inst2] quit

[DeviceB-erps-ring1] quit

# Enable CFD, and create a level-5 MD named MD\_A.

[DeviceB] cfd enable

[DeviceB] cfd md MD\_A level 5

# Create Ethernet service instance 1, in which the MA is identified by a VLAN and serves VLAN 1.

[DeviceB] cfd service-instance 1 ma-id vlan-based md MD\_A vlan 1

# Configure a MEP list in Ethernet service instance 1, create outward-facing MEP 1002 in Ethernet service instance 1, and enable CCM sending on .

[DeviceB] cfd meplist 1001 1002 service-instance 1

[DeviceB] interface

[DeviceB-] cfd mep 1002 service-instance 1 outbound

[DeviceB-] cfd cc service-instance 1 mep 1002 enable

[DeviceB-] quit

# Create Ethernet service instance 3, in which the MA is identified by a VLAN and serves VLAN 3.

[DeviceB] cfd service-instance 3 ma-id vlan-based md MD\_A vlan 3

# Configure a MEP list in Ethernet service instance 3, create outward-facing MEP 3002 in Ethernet service instance 3, and enable CCM sending on .

[DeviceB] cfd meplist 3001 3002 service-instance 3

[DeviceB] interface

[DeviceB-] cfd mep 3002 service-instance 3 outbound

[DeviceB-] cfd cc service-instance 3 mep 3002 enable

[DeviceB-] quit

# Create track entry 1 and associate it with the CC function of CFD for MEP 1002 in Ethernet service instance 1.

[DeviceB] track 1 cfd cc service-instance 1 mep 1002

# Associate with track entry 1 and bring up the port for ERPS instances 1 and 2.

[DeviceB] interface

[DeviceB-] port erps ring 1 instance 1 track 1

[DeviceB-] port erps ring 1 instance 2 track 1

[DeviceB-] undo shutdown

[DeviceB-] quit

# Create track entry 2 and associate it with the CC function of CFD for MEP 3002 in Ethernet service instance 3.

[DeviceB] track 2 cfd cc service-instance 3 mep 3002

# Associate with track entry 2 and bring up the port for ERPS instances 1 and 2.

[DeviceB] interface

[DeviceB-] port erps ring 1 instance 1 track 2

[DeviceB-] port erps ring 1 instance 2 track 2

[DeviceB-] undo shutdown

[DeviceB-] quit

# Enable ERPS.

[DeviceB] erps enable

Configure Device C.

# Create VLANs 1 to 60, map VLANs 1 to 30 to MSTI 1, map VLANs 31 to 60 to MSTI 2, and activate the MST region configuration.

<DeviceC> system-view

[DeviceC] vlan 1 to 60

[DeviceC] stp region-configuration

[DeviceC-mst-region] instance 1 vlan 1 to 30

[DeviceC-mst-region] instance 2 vlan 31 to 60

[DeviceC-mst-region] active region-configuration

[DeviceC-mst-region] quit

# Set the link state change suppression interval to 0 seconds on .

[DeviceC] interface

[DeviceC-] link-delay 0

# Disable the spanning tree feature on the port.

[DeviceC-] undo stp enable

# Configure the port as a trunk port and assign it to VLANs 1 to 60.

[DeviceC-] port link-type trunk

[DeviceC-] port trunk permit vlan 1 to 60

[DeviceC-] quit

# Configure in the same way is configured.

[DeviceC] interface

[DeviceC-] link-delay 0

[DeviceC-] undo stp enable

[DeviceC-] port link-type trunk

[DeviceC-] port trunk permit vlan 1 to 60

[DeviceC-] quit

# Create ERPS ring 1.

[DeviceC] erps ring 1

# Configure ERPS ring member ports.

[DeviceC-erps-ring1] port0 interface

[DeviceC-erps-ring1] port1 interface

# Create ERPS instance 1.

[DeviceC-erps-ring1] instance 1

# Configure the control VLAN.

[DeviceC-erps-ring1-inst1] control-vlan 100

# Configure the protected VLANs.

[DeviceC-erps-ring1-inst1] protected-vlan reference-instance 1

# Enable ERPS for instance 1.

[DeviceC-erps-ring1-inst1] instance enable

[DeviceC-erps-ring1-inst1] quit

[DeviceC-erps-ring1] quit

# Create ERPS instance 2.

[DeviceC-erps-ring1] instance 2

# Configure the node role.

[DeviceC-erps-ring1-inst2] node-role owner rpl port0

# Configure the control VLAN.

[DeviceC-erps-ring1-inst2] control-vlan 110

# Configure the protected VLANs.

[DeviceC-erps-ring1-inst2] protected-vlan reference-instance 2

# Enable ERPS for instance 2.

[DeviceC-erps-ring1-inst2] instance enable

[DeviceC-erps-ring1-inst2] quit

[DeviceC-erps-ring1] quit

# Enable CFD, and create a level-5 MD named MD\_A.

[DeviceC] cfd enable

[DeviceC] cfd md MD\_A level 5

# Create Ethernet service instance 3, in which the MA is identified by a VLAN and serves VLAN 3.

[DeviceC] cfd service-instance 3 ma-id vlan-based md MD\_A vlan 3

# Configure a MEP list in Ethernet service instance 3, create outward-facing MEP 3001 in Ethernet service instance 3, and enable CCM sending on .

[DeviceC] cfd meplist 3001 3002 service-instance 3

[DeviceC] interface

[DeviceC-] cfd mep 3001 service-instance 3 outbound

[DeviceC-] cfd cc service-instance 3 mep 3001 enable

[DeviceC-] quit

# Create Ethernet service instance 4, in which the MA is identified by a VLAN and serves VLAN 4.

[DeviceC] cfd service-instance 4 ma-id vlan-based md MD\_A vlan 4

# Configure a MEP list in Ethernet service instance 4, create outward-facing MEP 4001 in Ethernet service instance 4, and enable CCM sending on .

[DeviceC] cfd meplist 4001 4002 service-instance 4

[DeviceC] interface

[DeviceC-] cfd mep 4001 service-instance 4 outbound

[DeviceC-] cfd cc service-instance 4 mep 4001 enable

[DeviceC-] quit

# Create track entry 1 and associate it with the CC function of CFD for MEP 3001 in Ethernet service instance 3.

[DeviceC] track 1 cfd cc service-instance 3 mep 3001

# Associate with track entry 1 and bring up the port for ERPS instances 1 and 2.

[DeviceC] interface

[DeviceC-] port erps ring 1 instance 1 track 1

[DeviceC-] port erps ring 1 instance 2 track 1

[DeviceC-] undo shutdown

[DeviceC-] quit

# Create track entry 2 and associate it with the CC function of CFD for MEP 4001 in Ethernet service instance 4.

[DeviceC] track 2 cfd cc service-instance 4 mep 4001

# Associate with track entry 2 and bring up the port for ERPS instances 1 and 2.

[DeviceC] interface

[DeviceC-] port erps ring 1 instance 1 track 2

[DeviceC-] port erps ring 1 instance 2 track 2

[DeviceC-] undo shutdown

[DeviceC-] quit

# Enable ERPS.

[DeviceC] erps enable

Configure Device D.

# Create VLANs 1 to 60, map VLANs 1 to 30 to MSTI 1, map VLANs 31 to 60 to MSTI 2, and activate the MST region configuration.

<DeviceD> system-view

[DeviceD] vlan 1 to 60

[DeviceD] stp region-configuration

[DeviceD-mst-region] instance 1 vlan 1 to 30

[DeviceD-mst-region] instance 2 vlan 31 to 60

[DeviceD-mst-region] active region-configuration

[DeviceD-mst-region] quit

# Set the link state change suppression interval to 0 seconds on .

[DeviceD] interface

[DeviceD-] link-delay 0

# Disable the spanning tree feature on the port.

[DeviceD-] undo stp enable

# Configure the port as a trunk port and assign it to VLANs 1 to 60.

[DeviceD-] port link-type trunk

[DeviceD-] port trunk permit vlan 1 to 60

[DeviceD-] quit

# Configure in the same way is configured.

[DeviceD] interface

[DeviceD-] link-delay 0

[DeviceD-] undo stp enable

[DeviceD-] port link-type trunk

[DeviceD-] port trunk permit vlan 1 to 60

[DeviceD-] quit

# Create ERPS ring 1.

[DeviceD] erps ring 1

# Configure ERPS ring member ports.

[DeviceD-erps-ring1] port0 interface

[DeviceD-erps-ring1] port1 interface

# Create ERPS instance 1.

[DeviceD-erps-ring1] instance 1

# Configure the control VLAN.

[DeviceD-erps-ring1-inst1] control-vlan 100

# Configure the protected VLANs.

[DeviceD-erps-ring1-inst1] protected-vlan reference-instance 1

# Enable ERPS for instance 1.

[DeviceD-erps-ring1-inst1] instance enable

[DeviceD-erps-ring1-inst1] quit

# Create ERPS instance 2.

[DeviceD-erps-ring1] instance 2

# Configure the node role.

[DeviceD-erps-ring1-inst2] node-role neighbor rpl port0

# Configure the control VLAN.

[DeviceD-erps-ring1-inst2] control-vlan 110

# Configure the protected VLANs.

[DeviceD-erps-ring1-inst2] protected-vlan reference-instance 2

# Enable ERPS for instance 2.

[DeviceD-erps-ring1-inst2] instance enable

[DeviceD-erps-ring1-inst2] quit

[DeviceD-erps-ring1] quit

# Enable CFD, and create a level-5 MD named MD\_A.

[DeviceD] cfd enable

[DeviceD] cfd md MD\_A level 5

# Create Ethernet service instance 2, in which the MA is identified by a VLAN and serves VLAN 2.

[DeviceD] cfd service-instance 2 ma-id vlan-based md MD\_A vlan 2

# Configure a MEP list in Ethernet service instance 2, create outward-facing MEP 2002 in Ethernet service instance 2, and enable CCM sending on .

[DeviceD] cfd meplist 2001 2002 service-instance 2

[DeviceD] interface

[DeviceD-] cfd mep 2002 service-instance 2 outbound

[DeviceD-] cfd cc service-instance 2 mep 2002 enable

[DeviceD-] quit

# Create Ethernet service instance 4, in which the MA is identified by a VLAN and serves VLAN 4.

[DeviceD] cfd service-instance 4 ma-id vlan-based md MD\_A vlan 4

# Configure a MEP list in Ethernet service instance 4, create outward-facing MEP 4002 in Ethernet service instance 4, and enable CCM sending on .

[DeviceD] cfd meplist 4001 4002 service-instance 4

[DeviceD] interface

[DeviceD-] cfd mep 4002 service-instance 4 outbound

[DeviceD-] cfd cc service-instance 4 mep 4002 enable

[DeviceD-] quit

# Create track entry 1 and associate it with the CC function of CFD for MEP 2002 in Ethernet service instance 2.

[DeviceD] track 1 cfd cc service-instance 2 mep 2002

# Associate with track entry 1 and bring up the port for ERPS instances 1 and 2.

[DeviceD] interface

[DeviceD-] port erps ring 1 instance 1 track 1

[DeviceD-] port erps ring 1 instance 2 track 1

[DeviceD-] undo shutdown

[DeviceD-] quit

# Create track entry 2 and associate it with the CC function of CFD for MEP 4002 in Ethernet service instance 4.

[DeviceD] track 2 cfd cc service-instance 4 mep 4002

# Associate with track entry 2 and bring up the port for ERPS instances 1 and 2.

[DeviceD] interface

[DeviceD-] port erps ring 1 instance 1 track 2

[DeviceD-] port erps ring 1 instance 2 track 2

[DeviceD-] undo shutdown

[DeviceD-] quit

# Enable ERPS.

[DeviceD] erps enable

##### Verifying the configuration

# Display information about ERPS instance 1 for Device A.

[Device A] display erps detail ring 1

Ring ID : 1

Port0 :

Port1 :

Subring : No

Default MAC : No

Instance ID : 1

Node role : Owner

Node state : Idle

Connect(ring/instance): -

Control VLAN : 100

Protected VLAN : Reference-instance 1

Guard timer : 500 ms

Hold-off timer : 0 ms

WTR timer : 5 min

Revertive operation : Revertive

Enable status : Yes, Active status : Yes

R-APS level : 7

Port PortRole PortStatus

----------------------------------------------------------------------------

Port0 RPL Block

Port1 Non-RPL Up

Instance ID : 2

Node role : Normal

Node state : Idle

Connect(ring/instance): -

Control VLAN : 100

Protected VLAN : Reference-instance 2

Guard timer : 500 ms

Hold-off timer : 0 ms

WTR timer : 5 min

Revertive operation : Revertive

Enable status : Yes, Active status : Yes

R-APS level : 7

Port PortRole PortStatus

----------------------------------------------------------------------------

Port0 Non-RPL Up

Port1 Non-RPL Up

The output shows the following information:

* For ERPS instance 1:
  + Device A is the owner node.
  + The ERPS ring is in idle state.
  + The RPL port is blocked.
  + The non-RPL port is unblocked.
* For ERPS instance 2:
  + Device A is a normal node.
  + The ERPS ring is in idle state.
  + The non-RPL port is unblocked.

### Troubleshooting ERPS

#### The owner node cannot receive SF packets from a faulty node when the link state is normal

##### Symptom

The link between the owner node and the faulty node is available, but the owner node cannot receive SF packets sent by the faulty node. The RPL port is blocked.

##### Analysis

Possible reasons include:

* ERPS is not enabled for some nodes on the ERPS ring.
* The ring IDs are different for the nodes on the same ERPS ring.
* The control VLAN IDs are different for the nodes in the same ERPS instance.
* A port on the ERPS ring is faulty.

##### Solutions

To resolve the problem:

* Use the display erps command to examine whether ERPS is enabled for all nodes on the ERPS ring. If ERPS is disabled for some nodes, use the erps enable command to enable ERPS for the nodes.
* Set the same ring ID for all nodes on a ERPS ring and configure the same control VLAN for all nodes in an ERPS instance.
* Use the display erps detail command to examine the port status for all nodes. Bring up the ports in down state.
* Use the debugging erps command on all nodes to view debugging information about packets and node status.

## Command reference

### control-vlan

Use control-vlan to configure the control VLAN for an ERPS instance.

Use undo control-vlan to restore the default.

Syntax

control-vlan vlan-id

undo control-vlan

Default

An ERPS instance does not have control VLANs.

Views

ERPS instance view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies the ID of the control VLAN, in the range of 2 to 4094.

Examples

# Configure VLAN 100 as the control VLAN for instance 1 of ERPS ring 1.

<Sysname> system-view

[Sysname] erps ring 1

[Sysname-erps-ring1] instance 1

[Sysname-erps-ring1-inst1] control-vlan 100

Related commands

instance

### display erps

Use display erps to display brief ERPS ring information.

Syntax

display erps

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

# Display brief ERPS ring information.

<Sysname> display erps

ERPS protocol status: Enabled

ERPS tcn-propagation: Enabled

Flags: R -- RPL, F -- Faulty, B -- Blocked,

FS -- Forced switch, MS -- Manual switch

Ring Instance NodeRole NodeState Port0 Port1 Status

-----------------------------------------------------------------------

1 1 Owner Idle R,B Enabled

1 2 Normal Idle Disabled

2 1 Owner Idle R,B Enabled

2 2 Normal Idle Disabled

Command output

| Field | Description |
| --- | --- |
| ERPS protocol status | ERPS state:   * + - * Enabled—Globally enabled.       * Disabled—Globally disabled. |
| ERPS tcn-propagation | State of the flush packet transparent transmission feature:   * + - * Enabled—Globally enabled.       * Disabled—Globally disabled. |
| Ring | ERPS ring ID. |
| Instance | ERPS instance ID. |
| NodeRole | Node type:   * + - * Owner.       * Neighbor.       * Interconnection.       * Normal. |
| NodeState | Node state:   * + - * Idle—The ERPS ring enters the idle state after initialization.       * Protection—The ERPS ring enters the protection state when a link fails.       * MS—Manual switching mode.       * FS—Forced switching mode.       * Pending—Transient mode between any two states.       * -—ERPS is disabled for the ERPS instance or disabled globally. |
| Port0 | State of port 0:   * + - * R—The port is an RPL port.       * B—The port is blocked.       * F—The port is unavailable and the link for the port is faulty.       * FS—The port is in FS mode.       * MS—The port is in MS mode.       * -—The port is not an ERPS ring member port.   If this field is blank, the port is not in any of the previous states. |
| Port1 | State of port 1:   * + - * R—The port is an RPL port.       * B—The port is blocked.       * F—The port is unavailable and the link for the port is faulty.       * FS—The port is in FS mode.       * MS—The port is in MS mode.       * -—The port is not an ERPS ring member port.   If this field is blank, the port is not in any of the previous states. |
| Status | State of the ERPS instance:   * + - * Enabled.       * Disabled. |

### display erps detail

Use display erps detail to display detailed ERPS ring information.

Syntax

display erps detail ring ring-id [ instance instance-id ]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ring ring-id: Specifies an ERPS ring by its ID in the range of 1 to 255.

instance instance-id: Specifies an ERPS instance by its ID in the range of 1 to 64. If you do not specify this option, this command displays detailed information about all instances for the ERPS ring.

Examples

# Display detailed information about instance 1 of ERPS ring 1.

<Sysname> display erps detail ring 1 instance 1

Ring ID : 1

Port0 :

Port1 :

Subring : Yes

Default MAC : Yes

Instance ID : 1

Node role : Owner

Node state : Idle

Connect (ring/instance): (1/2), (2/3)

Control VLAN : 100

Protected VLAN : Reference-instance 0 to 2

Guard timer : 500 ms

Hold-off timer : 1 sec

WTR timer : 5 min

Revertive operation : Non-revertive

Enable status : Yes, Active Status : Yes

R-APS level : 1

Port PortRole PortStatus

--------------------------------------------------------------------

Port0 RPL Block

Port1 Non-RPL Up

# Display detailed information about all instances of ERPS ring 1.

<Sysname> display erps detail ring 1

Ring ID : 1

Port0 :

Port1 :

Subring : Yes

Default MAC : Yes

Instance ID : 1

Node role : Owner

Node state : Idle

Connect(ring/instance): (1/2), (2/3)

Control VLAN : 100

Protected VLAN : Reference-instance 0 to 2

Guard timer : 500 ms

Hold-off timer : 1 sec

WTR timer : 5 min

Revertive operation : Non-revertive

Enable status : Yes, Active Status : Yes

R-APS level : 1

Port PortRole PortStatus

----------------------------------------------------------------------

Port0 RPL Block

Port1 Non-RPL Up

Instance ID : 2

Node role : Neighbor

Node state : Idle

Connect(ring/instance): (1/2), (2/3)

Control VLAN : 200

Protected VLAN : Reference-instance 3

Guard timer : 500 ms

Hold-off timer : 1 sec

Wtr timer : 5 min

Revertive operation : Non-revertive

Enable status : Yes, Active Status : Yes

R-APS level : 1

Port PortRole PortStatus

-------------------------------------------------------------------

Port0 RPL Block

Port1 Non-RPL Up

Command output

| Field | Description |
| --- | --- |
| Port0 | ERPS ring member port 0. |
| Port1 | ERPS ring member port 1. |
| Subring | ERPS subring status:   * + - * Yes—The ring is a subring.       * No—The ring is not a subring. |
| Default MAC | Default MAC address status:   * + - * Yes—The last byte is 1 in the destination MAC address of R-APS packets.       * No—The last byte is the ring ID in the destination MAC address of R-APS packets. |
| Node role | Node type:   * + - * Owner.       * Neighbor.       * Interconnection.       * Normal. |
| Node state | Node state:   * + - * Idle—The ERPS ring enters the idle status after initialization.       * Protection—The ERPS ring enters the protection state when a link fails.       * MS—Manual switching mode.       * FS—Forced switching mode.       * Pending—Transient mode between any two states.       * -—ERPS is disabled for the ERPS instance or disabled globally. |
| Connect(ring/instance) | Ring or instance associated with the ERPS instance. |
| Control VLAN | Control VLAN of the ERPS instance. |
| Protected VLAN | List of VLANs protected by the ERPS instance, which are represented by MSTIs.  To view the mapping between MSTIs and VLANs, use the display stp region-configuration command. |
| Guard timer | Guard timer in milliseconds. |
| Hold-off timer | Hold-off timer in milliseconds. |
| WTR timer | WTR timer in minutes. |
| Revertive operation | Revertive mode:   * + - * Non-revertive.       * Revertive. |
| Enable status | ERPS status for the instance:   * + - * Yes—Enabled.       * No—Disabled. |
| Active Status | Global ERPS status and ERPS status for the instance:   * + - * Yes—Enabled.       * No—Disabled. |
| R-APS level | Level of the R-APS packets. |
| Port | ERPS ring member port. |
| PortRole | Port role:   * + - * RPL—The port is an RPL port.       * Non-RPL—The port is not an RPL port. |
| Port Status | Port status:   * + - * Block—The port is blocked.       * Up—The link is up.       * Down—The link is down. |

### display erps statistics

Use display erps statistics to display ERPS packet statistics.

Syntax

display erps statistics ring-id [ instance instance-id ]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ring ring-id: Specifies an ERPS ring by its ID in the range of 1 to 255.

instance instance-id: Specifies an ERPS instance by its ID in the range of 1 to 64. If you do not specify this option, this command displays packet statistics for all instances of the ERPS ring.

Examples

# Display packet statistics for all instances of ERPS ring 1.

<Sysname> display erps statistics ring 1

Statistics for ERPS ring 1 instance 1:

R-APS Port0(Tx/Rx) Port1(Tx/Rx)

----------------------------------------------------

NR 1/1 1/1

NR,RB 0/1 0/1

SF 1/0 1/0

MS 0/0 0/0

FS 0/0 0/0

Total 2/2 2/2

Statistics for ERPS ring 1 instance 2:

R-APS Port0(Tx/Rx) Port1(Tx/Rx)

----------------------------------------------------

NR 1/1 1/1

NR,RB 0/1 0/1

SF 1/0 1/0

MS 0/0 0/0

FS 0/0 0/0

Total 2/2 2/2

Command output

| Field | Description |
| --- | --- |
| R-APS | Packet type. |
| Port0(Tx/Rx) | Packet statistics for port 0:   * + - * Tx—Transmitted packets.       * Rx—Received packets. |
| Port1(Tx/Rx) | Packet statistics for port 1:   * + - * Tx—Transmitted packets.       * Rx—Received packets. |

### erps clear

Use erps clear to remove the MS mode and FS mode settings for an ERPS ring.

Syntax

erps clear ring-id instance instance-id

Views

System view

Predefined user roles

network-admin

Parameters

ring ring-id: Specifies an ERPS ring by its ID in the range of 1 to 255.

instance instance-id: Specifies an ERPS instance by its ID in the range of 1 to 64.

Usage guidelines

After you configure this command, the owner node can ignore the WTR timer and immediately switch traffic to the recovered link upon link recovery.

This command also switches an ERPS ring in non-revertive mode to revertive mode.

Examples

# Remove the MS mode and FS mode settings for instance 1 on ERPS ring 1.

<Sysname> system-view

[Sysname] erps clear ring 1 instance 1

### erps enable

Use erps enable to enable ERPS globally.

Use undo erps enable to restore the default.

Syntax

erps enable

undo erps enable

Default

ERPS is disabled globally.

Views

System view

Predefined user roles

network-admin

Examples

# Enable ERPS.

<Sysname> system-view

[Sysname] erps enable

### erps ring

Use erps ring to create an ERPS ring.

Use undo erps ring to delete an ERPS ring.

Syntax

erps ring ring-id

undo erps ring ring-id

Default

No ERPS rings exist.

Views

System view

Predefined user roles

network-admin

Parameters

ring ring-id: Specifies an ERPS ring by its ID in the range of 1 to 255.

Usage guideline

To delete an ERPS ring successfully, delete all ERPS instances on the ring first.

Examples

# Create ERPS ring 1.

<Sysname> system-view

[Sysname] erps ring 1

[Sysname-erps-ring1]

Related commands

instance

### erps switch

Use erps switch to configure the switching mode for an ERPS ring.

Syntax

erps switch { force | manual } ring ring-id instance instance-id { port0 | port1 }

Views

System view

Predefined user roles

network-admin

Parameters

force: Configures the forced switching mode.

manual: Configures the manual switching mode.

port0: Specifies the ERPS ring member port 0.

port1: Specifies the ERPS ring member port 1.

ring ring-id: Specifies an ERPS ring by its ID in the range of 1 to 255.

instance instance-id: Specifies an ERPS instance by its ID in the range of 1 to 64.

Examples

# Configure the forced switching mode for port 1 of instance 1 on ERPS ring 1.

<Sysname> system-view

[Sysname] erps switch force ring 1 instance 1 port0

### erps tcn-propagation

Use erps tcn-propagation to enable flush packet transparent transmission for an interconnection node.

Use undo erps tcn-propagation to restore the default.

Syntax

erps tcn-propagation

undo erps tcn-propagation

Default

Flush packet transparent transmission is disabled for an interconnection node.

Views

System view

Predefined user roles

network-admin

Usage guideline

This command must be used together with the sub-ring connect command.

Examples

# Enable flush packet transparent transmission for the interconnection node.

<Sysname> system-view

[Sysname] erps tcn-propagation

Related commands

sub-ring connect

### instance

Use instance to create an instance for an ERPS ring.

Use undo instance to delete an instance from an ERPS ring.

Syntax

instance instance-id

undo instance instance-id

Default

An ERPS ring does not have instances.

Views

ERPS ring view

Predefined user roles

network-admin

Parameters

instance instance-id: Specifies an ERPS instance by its ID in the range of 1 to 64.

Usage guidelines

You can create multiple instances for an ERPS ring. Each instance has its own protected VLAN, control VLAN, and RPL owner. Each instance maintains its own state machine and data. You can locate an ERPS instance by its ring ID and VLAN ID.

Examples

# Create instance 1 for ERPS ring 1.

<Sysname> system-view

[Sysname] erps ring 1

[Sysname-erps-ring1] instance 1

[Sysname-erps-ring1-inst1]

Related commands

erps ring

### instance enable

Use instance enable to enable ERPS for an ERPS instance.

Use undo instance enable to disable ERPS for an ERPS instance.

Syntax

instance enable

undo instance enable

Default

ERPS is disabled for ERPS instances.

Views

ERPS instance view

Predefined user roles

network-admin

Examples

# Create ERPS instance 1 and enable ERPS for the instance.

<Sysname> system-view

[Sysname] erps ring 1

[Sysname-erps-ring1] instance 1

[Sysname-erps-ring1-inst1] control-vlan 100

[Sysname-erps-ring1-inst1] protected-vlan reference-instance 0 1 2

[Sysname-erps-ring1-inst1] instance enable

Related commands

instance

### node-role

Use node-role to configure the role for an ERPS node.

Use undo node-role to restore the default.

Syntax

node-role { { owner | neighbor } rpl | interconnection } { port0 | port1 }

undo node-role

Default

An ERPS node is a normal node.

Views

ERPS instance view

Predefined user roles

network-admin

Parameters

owner: Configures the owner node.

neighbor: Configures the neighbor node.

interconnection: Configures the interconnection node for connecting the major ring and subring.

Usage guidelines

You can configure an interconnection node only for a subring.

Examples

# Configure instance 1 of ERPS ring 1 as an RPL owner node and configure port 0 as an RPL port.

<Sysname> system-view

[Sysname] erps ring 1

[Sysname-erps-ring1] instance 1

[Sysname-erps-ring1-inst1] node-role owner rpl port0

### port erps track

Use port erps track to associate an ERPS ring member port with a track entry.

Use undo port erps track to remove the association between an ERPS ring member port and a track entry.

Syntax

port erps ring ring-id instance instance-id track track-entry-index

undo port erps ring ring-id instance instance-id track

Default

An ERPS ring member port is not associated with track entries.

Views

Interface view

Predefined user roles

network-admin

Parameters

ring ring-id: Specifies an ERPS ring by its ID in the range of 1 to 255.

instance instance-id: Specifies an ERPS instance by its ID in the range of 1 to 64.

track-entry-index: Specifies a track entry by its ID in the range of 1 to 1024. For more information about specifying the track entry ID, see the track cfd command in "Track commands."

Usage guidelines

An ERPS ring member port collaborates with link detection protocols through track entries. ERPS supports only the CC feature of CFD to implement link detection.

Examples

# Associate a track entry with on the RPL owner node in instance 1 of ERPS ring 1.

<Sysname> system-view

[Sysname] erps ring 1

[Sysname-erps-ring1] port0 interface

[Sysname-erps-ring1] instance 1

[Sysname-erps-ring1-inst1] node-role owner rpl port0

[Sysname-erps-ring1-inst1] quit

[Sysname-erps-ring1] quit

[Sysname] interface

[Sysname-] port erps ring 1 instance 1 track 3

Related commands

track cfd

### port0

Use port0 to specify the first member port for an ERPS ring.

Use undo port0 to restore the default.

Syntax

port0 interface interface-type interface-number

undo port0

Default

No member ports exist in an ERPS ring.

Views

ERPS ring view

Predefined user roles

network-admin

Parameters

interface interface-type interface-number: Specifies a Layer 2 Ethernet interface or a Layer 2 aggregate interface by its type and number.

Examples

# Specify as the first member port for ERPS ring 1.

<Sysname> system-view

[Sysname] erps ring 1

[Sysname-erps-ring1] port0 interface

### port1

Use port1 to specify the second member port for an ERPS ring.

Use undo port1 to restore the default.

Syntax

port1 interface interface-type interface-number

undo port1

Default

No member ports exist in an ERPS ring.

Views

ERPS ring view

Predefined user roles

network-admin

Parameters

interface interface-type interface-number: Specifies a Layer 2 Ethernet interface or a Layer 2 aggregate interface by its type and number.

Examples

# Specify as the second member port for ERPS ring 1.

<Sysname> system-view

[Sysname] erps ring 1

[Sysname-erps-ring1] port1 interface

### protected-vlan

Use protected-vlan to configure protected VLANs for an ERPS instance.

Use undo protected-vlan to delete protected VLANs for an ERPS instance.

Syntax

protected-vlan reference-instance instance-id-list

undo protected-vlan [ reference-instance instance-id-list ]

Default

No protected VLANs exist in an ERPS instance.

Views

ERPS instance view

Predefined user roles

network-admin

Parameters

instance-id-list: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of instance-id1 to instance-id2. The value for instance-id2 must be greater than or equal to the value for instance-id1. The value range for the instance-id argument is 0 to 4094. The value 0 indicates CIST. You can use the display stp region-configuration command to display the VLAN-to-instance mappings. In PVST mode, the system automatically maps VLANs to MSTIs.

Usage guidelines

If you do not specify the reference-instance instance-id-list option, the undo protected-vlan command deletes all mappings between MSTIs and VLANs in the ERPS instance. The protected VLANs change if the mappings between the MSTIs and VLANs change.

Examples

# Configure the protected VLANs for instance 1 of ERPS ring 1.

<Sysname> system-view

[Sysname] erps ring 1

[Sysname-erps-ring1] instance 1

[Sysname-erps-ring1-inst1] protected-vlan reference-instance 0 1 2

Related commands

display stp region-configuration

### r-aps level

Use r-aps level to configure the level for R-APS packets.

Use undo r-aps level to restore the default.

Syntax

r-aps level level-value

undo r-aps level

Default

The R-APS packet level is 7.

Views

ERPS instance view

Predefined user roles

network-admin

Parameters

level-value: Specifies the R-APS packet level in the range of 0 to 7.

Usage guidelines

The R-APS packet level must be the same for all nodes in an instance of an ERPS ring.

Examples

# Configure the R-APS packet level as 1 for instance 1 of ERPS ring 1.

<Sysname> system-view

[Sysname] erps ring 1

[Sysname-erps-ring1] instance 1

[Sysname-erps-ring1-inst1] r-aps level 1

### r-aps ring-mac

Use r-aps ring-mac to configure the ring ID as the last byte of the destination MAC address for R-APS packets.

Use undo r-aps ring-mac to restore the default.

Syntax

r-aps ring-mac

undo r-aps ring-mac

Default

The last byte of the destination MAC address is 1 for the R-APS packets.

Views

ERPS ring view

Predefined user roles

network-admin

Examples

# Configure the ID of ERPS ring 2 as the last byte of the destination MAC address for R-APS packets.

<Sysname> system-view

[Sysname] erps ring 2

[Sysname-erps-ring2] r-aps ring-mac

### reset erps statistics

Use reset erps statistics to clear ERPS packet statistics.

Syntax

reset erps statistics ring ring-id [ instance instance-id ]

Views

User view

Predefined user roles

network-admin

Parameters

ring ring-id: Specifies an ERPS ring by its ID in the range of 1 to 255.

instance instance-id: Specifies an ERPS instance by its ID in the range of 1 to 64. If you do not specify this option, this command clears packet statistics for all instances of the ERPS ring.

Examples

# Clear packet statistics for instance 1 of ERPS ring 1.

<Sysname> reset erps statistics ring 1 instance 1

Related commands

display erps statistics

### revertive-operation

Use revertive-operation non-revertive to set the non-revertive mode for an ERPS ring.

Use undo revertive-operation to restore the default.

Syntax

revertive-operation non-revertive

undo revertive-operation

Default

An ERPS ring operates in revertive mode.

Views

ERPS instance view

Predefined user roles

network-admin

Usage guidelines

In non-revertive mode, an owner node does not perform any operations when receiving NR packets. You can use the erps clear command to restore the revertive mode.

Examples

# Set the non-revertive mode for instance 1 of ERPS ring 1.

<Sysname> system-view

[Sysname] erps ring 1

[Sysname-erps-ring1] instance 1

[Sysname-erps-ring1-inst1] revertive-operation non-revertive

### ring-type sub-ring

Use ring-type sub-ring to configure the ERPS ring as a subring.

Use undo ring-type sub-ring to restore the default.

Syntax

ring-type sub-ring

undo ring-type

Default

An ERPS ring is a major ring.

Views

ERPS ring view

Predefined user roles

network-admin

Examples

# Configure ERPS ring 1 as a subring.

<Sysname> system-view

[Sysname] erps ring 1

[Sysname-erps-ring1] ring-type sub-ring

### sub-ring connect

Use sub-ring connect to associate the subring with an ERPS ring.

Use undo sub-ring connect to remove the association.

Syntax

sub-ring connect ring ring-id instance instance-id

undo sub-ring connect ring ring-id instance instance-id

Default

A subring is not associated with ERPS rings.

Views

ERPS instance view

Predefined user roles

network-admin

Parameters

ring ring-id: Specifies an ERPS ring by its ID in the range of 1 to 255.

instance instance-id: Specifies an ERPS instance by its ID in the range of 1 to 64.

Examples

# Configure ERPS ring 1 as a subring for instance 1, and associate the subring with ERPS ring 2.

<Sysname> system-view

[Sysname] erps ring 2

[Sysname-erps-ring2] instance 1

[Sysname-erps-ring2] quit

[Sysname] erps ring 1

[Sysname-erps-ring1] ring-type sub-ring

[Sysname-erps-ring1] instance 1

[Sysname-erps-ring1-inst1] sub-ring connect ring 2 instance 1

Related commands

ring-type sub-ring

### timer guard

Use timer guard to set the guard timer for an ERPS instance.

Use undo timer guard to restore the default.

Syntax

timer guard guard-value

undo timer guard

Default

The guard timer is 500 milliseconds for an ERPS instance.

Views

ERPS instance view

Predefined user roles

network-admin

Parameters

guard-value: Specifies the guard timer in the range of 0 to 2000 milliseconds and in step of 10.

Usage guidelines

The guard timer starts when the link recovers. The system processes only the flush packets before the guard timer expires. The guard timer prevents SF messages from impacting the network.

Examples

# Set the guard timer to 30 milliseconds for instance 1 of ERPS ring 1.

<Sysname> system-view

[Sysname] erps ring 1

[Sysname-erps-ring1] instance 1

[Sysname-erps-ring1-inst1] timer guard 30

### timer hold-off

Use timer hold-off to set the hold-off timer for an ERPS instance.

Use undo timer hold-off to restore the default.

Syntax

timer hold-off hold-off-value

undo timer hold-off

Default

The hold-off timer is 0 milliseconds for an ERPS instance.

Views

ERPS instance view

Predefined user roles

network-admin

Parameters

hold-off-value: Specifies the hold-off timer in the range of 0 to 10000 milliseconds and in step of 100.

Usage guidelines

The hold-off timer starts when the port detects a link fault. If the link fault persists when the hold-off timer expires, the port reports the link fault. The hold-off timer delays the fault report time and might impact the link recovery performance.

Examples

# Set the hold-off timer to 300 milliseconds for instance 1 of ERPS ring 1.

<Sysname> system-view

[Sysname] erps ring 1

[Sysname-erps-ring1] instance 1

[Sysname-erps-ring1-inst1] timer hold-off 300

### timer wtr

Use timer wtr to set the WTR timer for an ERPS instance.

Use undo timer wtr to restore the default.

Syntax

timer wtr wtr-value

undo timer wtr

Default

The WTR timer is 5 minutes for an ERPS instance.

Views

ERPS instance view

Predefined user roles

network-admin

Parameters

wtr-value: Specifies the WTR timer in the range of 1 to 12 minutes and in step of 1.

Usage guidelines

This timer prevents intermittent link failures from impacting the network.

Examples

# Set the WTR timer to 3 minutes for instance 1 of ERPS ring 1.

<Sysname> system-view

[Sysname] erps ring 1

[Sysname-erps-ring1] instance 1

[Sysname-erps-ring1-inst1] timer wtr 3

# Modified feature: Physical type of a combo interface

## Feature change description

In this version and later, the combo enable auto command is supported, which configures a combo interface to autonegotiate its physical type.

## Command changes

### combo enable

Old syntax

combo enable { copper | fiber }

New syntax

combo enable { auto | copper | fiber }

Views

Ethernet interface view

Parameters

auto: Specifies the combo interface to autonegotiate its physical type.

Usage guidelines

When a combo interface acts as an IRF physical interface, you must manually configure the physical type of the combo interface as copper or fiber.

A combo interface in auto mode does not support the duplex half, speed 10, or speed 100 command.

Change description

Before modification:

By default, the copper combo port is activated. You can specify the copper or fiber keyword to activate the copper or fiber combo port as needed.

After modification:

By default, a combo interface autonegotiates its physical type. When a combo autonegotiates its physical type, the actual physical type depends on the connected media:

* When the copper combo port is not connected to a twisted-pair cable and the fiber combo port has a transceiver module installed, the fiber combo port is activated.
* When the copper combo port is connected to a twisted-pair cable and is up:

If you install a transceiver module in the fiber combo port, the copper combo port is still activated before the device is rebooted.

After the device is rebooted, the fiber combo port is activated.

* When the copper combo port is connected to a twisted-pair cable and is down and the fiber combo port has a transceiver module installed, the fiber combo port is activated.
* When the fiber combo port has a transceiver module installed, the fiber combo port is activated even if you connect a twisted-pair cable to the copper combo port.

If you need to specify the physical type of a physical interface according to the network requirements, you can specify the copper or fiber keyword to activate the copper or fiber combo port.

1. Release 3208P12

This release has the following changes:

New feature: PD detection mode

Modified feature: Setting the length of ICMP or ICMPv6 echo requests for the ping operation

# New feature: PD detection mode

## Configuring the PD detection mode

#### About PD detection modes

The device detects PDs in one of the following modes:

* None—The device supplies power to PDs that are correctly connected to the device without causing short circuit.
* Simple—The device supplies power to PDs that comply with basic requirements of 802.3af or 802.3at.
* Strict—The device supplies power to PDs that comply with all requirements of 802.3af or 802.3at.

#### Restrictions and guidelines

Only PSEs with model LSP7POEB and LSP7POED support this configuration. To obtain your PSE model, see the PSE Model field in the output from the display poe pse command.

For this feature to take effect on nonstandard PDs, you must enable detection for nonstandard PDs by using the poe legacy enable command.

#### Procedure

Enter system view.

system-view

Enter PI view.

interface interface-type interface-number

Configure the PD detection mode.

poe detection-mode { none | simple | strict }

By default, the PD detection mode is strict.

## Command reference

### poe detection-mode

Use poe detection-mode to configure the PD detection mode.

Use undo poe detection-mode to restore the default.

Syntax

poe detection-mode { none | simple | strict }

undo poe detection-mode

Default

The PD detection mode is strict.

Views

PI view

Predefined user roles

network-admin

Parameters

none: Enables the device to supply power to PDs that are correctly connected to the device without causing short circuit.

simple: Enables the device to supply power to PDs that comply with basic requirements of 802.3af or 802.3at.

strict: Enables the device to supply power to PDs that comply with all requirements of 802.3af or 802.3at.

Usage guidelines

To configure the detection mode for nonstandard PDs, first execute the poe legacy enable command to enable detection for nonstandard PDs.

Examples

# Configure the simple detection mode for .

<Sysname> system-view

[Sysname] interface

[Sysname-] poe detection-mode simple

# Modified feature: Setting the length of ICMP or ICMPv6 echo requests for the ping operation

## Feature change description

In the ping operation, the value range for the length of ICMP or ICMPv6 echo requests was changed from 20 to 8100 bytes to 20 to 9600 bytes.

## Command changes

### Modified command: ping

Syntax

ping [ ip ] [ -a source-ip | -c count | -f | -h ttl | -i interface-type interface-number | -m interval | -n | -p pad | -q | -r | -s packet-size | -t timeout | -tos tos | -v] \* host

Views

Any view

Parameters

-s packet-size: Specifies the length (in bytes) of ICMP echo requests (excluding the IP packet header and the ICMP packet header). The value range is 20 to 9600, and the default is 56.

Change description

Before modification: The value range for the packet-size argument is 20 to 8100 bytes.

After modification: The value range for the packet-size argument is 20 to 9600 bytes.

### Modified command: ping ipv6

Syntax

ping ipv6 [ -a source-ipv6 | -c count | -i interface-type interface-number | -m interval | -q | -s packet-size | -t timeout | -tc traffic-class | -v ] \* host

Views

Any view

Parameters

-s packet-size: Specifies the length (in bytes) of ICMPv6 echo requests (excluding the IPv6 packet header and the ICMPv6 packet header). The value range is 20 to 9600, and the default is 56.

Change description

Before modification: The value range for the packet-size argument is 20 to 8100 bytes.

After modification: The value range for the packet-size argument is 20 to 9600 bytes.

1. Release 3208P10

This release has the following changes:

* New feature: Automatic obtaining of the login username for temporary user role authorization
* New feature: 802.1X EAP-TLS fragmentation for packets sent to the server
* New feature: Enabling interface consistency check for ARP and MAC address entries
* New feature: 802.1X offline detection
* New feature: Enabling SAVI and setting the entry deletion delay by using commands
* Modified feature: Configuring MAC-based MAC authentication user accounts
* Modified feature: Port security NTK feature

# New feature: Automatic obtaining of the login username for temporary user role authorization

## Automatically obtaining the login username for temporary user role authorization

### About automatic obtaining of the login username for temporary user role authorization

This feature is applicable only to the login from a user line that uses scheme authentication, which requires a username for login. This feature enables the device to automatically obtain the login username when the login user requests a temporary user role authorization from a remote authentication server.

### Restrictions and guidelines

If the user was logged in from a user line that uses password authentication or no authentication, the device cannot obtain the login username. The request for temporary user role authorization from a remote authentication server will fail.

This feature does not take effect on local password authentication for temporary user role authorization.

### Procedure

Enter system view.

system-view

Enable the device to automatically obtain the login username when a login user requests temporary user role authorization from a remote authentication server.

super use-login-username

By default, the device requests a username at the prompt when a login user requests temporary user role authorization from a remote authentication server.

## Command reference

### super use-login-username

Use super use-login-username to enable the device to automatically obtain the login username when a login user requests temporary user role authorization from a remote authentication server.

Use undo super use-login-username to restore the default.

Syntax

super use-login-username

undo super use-login-username

Default

The device requests a username at the prompt when a login user requests temporary user role authorization from a remote authentication server.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command is applicable only to the login from a user line that uses scheme authentication, which requires a username for login.

If the user was logged in from a user line that uses password authentication or no authentication, the device cannot obtain the login username. The request for temporary user role authorization from a remote authentication server will fail.

This command does not take effect on local password authentication for temporary user role authorization.

Examples

# Enable the device to automatically obtain the login username when a login user requests temporary user role authorization from a remote authentication server.

<Sysname> system-view

[Sysname] super use-login-username

# New feature: 802.1X EAP-TLS fragmentation for packets sent to the server

## Setting the maximum length of an EAP-TLS fragment sent to the server

#### About setting the maximum length of an EAP-TLS fragment sent to the server

Some RADIUS servers cannot process oversized packets. If the length of a RADIUS packet exceeds the maximum packet length allowed by the servers, the client will fail the authentication.

The device might send oversized packets to such a RADIUS server when it uses the EAP relay mode and the EAP-TLS authentication method in remote authentication. The device encapsulates the EAP-TLS messages received from a client into the EAP-Message attribute of the RADIUS packets that will be sent to the server.

To avoid authentication failures caused by oversized packets, you can fragment the EAP-TLS messages that will be sent to the server in RADIUS packets.

Set a proper maximum length for the EAP-TLS fragments according to the maximum packet length allowed by the server.

After receiving all EAP-TLS fragments, the server will reassemble the EAP-TLS fragments and obtain the complete authentication information of the client.

For example, the maximum packet length allowed by the server is 1200 bytes and the length of a RADIUS packet (excluding the EAP-Message attribute) is 800 bytes. To make sure the maximum length of a RADIUS packet does not exceed 1200 bytes, you must set the maximum length of an EAP-TLS fragment to a value less than 400 bytes.

#### Restrictions and guidelines

For 802.1X EAP-TLS fragmentation and the maximum fragment length to take effect, you must set the EAP message handling method to EAP relay.

#### Procedure

Enter system view.

system-view

Set the maximum length of an EAP-TLS fragment that will be sent in an authentication packet to the server.

dot1x eap-tls-fragment to-server eap-tls-max-length

By default, EAP-TLS messages are not fragmented by 802.1X EAP-TLS fragmentation.

## Command reference

### dot1x eap-tls-fragment to-server

Use dot1x eap-tls-fragment to-server to set the maximum length of an EAP-TLS fragment that will be sent in an authentication packet to the server.

Use undo dot1x eap-tls-fragment to-server to restore the default.

Syntax

dot1x eap-tls-fragment to-server eap-tls-max-length

undo dot1x eap-tls-fragment to-server

Default

EAP-TLS messages are not fragmented by 802.1X EAP-TLS fragmentation.

Views

System view

Predefined user roles

network-admin

Parameters

eap-tls-max-length: Sets the maximum length of an EAP-TLS fragment in bytes. The value range is 100 to 1500.

Usage guidelines

|  |  |
| --- | --- |
| 说明: IMPORTANT | IMPORTANT:  For this command to take effect, you must set the EAP message handling method to EAP relay. |

Some RADIUS servers cannot process oversized packets. If the length of a RADIUS packet exceeds the maximum packet length allowed by the servers, the client will fail the authentication.

The device might send oversized packets to such a RADIUS server when it uses the EAP relay mode and the EAP-TLS authentication method in remote authentication. The device encapsulates the EAP-TLS messages received from a client into the EAP-Message attribute of the RADIUS packets that will be sent to the server.

To avoid authentication failures caused by oversized packets, you can fragment the EAP-TLS messages that will be sent to the server in RADIUS packets.

Use this command to set a proper maximum length for the EAP-TLS fragments according to the maximum packet length allowed by the server.

After receiving all EAP-TLS fragments, the server will reassemble the EAP-TLS fragments and obtain the complete authentication information of the client.

For example, the maximum packet length allowed by the server is 1200 bytes and the length of a RADIUS packet (excluding the EAP-Message attribute) is 800 bytes. To make sure the maximum length of a RADIUS packet does not exceed 1200 bytes, you must set the maximum length of an EAP-TLS fragment to a value less than 400 bytes.

Examples

# Set the maximum length to 400 bytes for the EAP-TLS fragments that will be sent in packets to the server.

<Sysname> system-view

[Sysname] dot1x eap-tls-fragment to-server 400

Related commands

dot1x authentication-method

# New feature: Enabling interface consistency check for ARP and MAC address entries

## Enabling interface consistency check for ARP and MAC address entries

#### About interface consistency check for ARP and MAC address entries

In an instable network, the receiving interface for packets from a user might change. The interface in the MAC address entry can be updated immediately while the interface in the ARP entry cannot. In this case, the packets matching the ARP entry will be sent out of an incorrect interface. To solve this problem, you can use this feature to periodically check the interface consistency for the ARP and MAC address entry of a user. If the interfaces are not the same, ARP sends ARP requests in the VLAN of the ARP entry and updates the entry with the ARP reply receiving interface.

#### Procedure

Enter system view.

system-view

Enabling interface consistency check for ARP and MAC address entries.

arp mac-interface-consistency check enable

By default, enabling interface consistency check for ARP and MAC address entries is disabled.

## Command reference

### arp mac-interface-consistency check enable

Use arp mac-interface-consistency check enable to enable interface consistency check for ARP and MAC address entries.

Use undo arp mac-interface-consistency check enable to disable this feature.

Syntax

arp mac-interface-consistency check enable

undo arp mac-interface-consistency check enable

Default

Enabling interface consistency check for ARP and MAC address entries is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

In an instable network, the receiving interface for packets from a user might change. The interface in the MAC address entry can be updated immediately while the interface in the ARP entry cannot. In this case, the packets matching the ARP entry will be sent out of an incorrect interface. To solve this problem, you can use this feature to periodically check the interface consistency for the ARP and MAC address entry of a user. If the interfaces are not the same, ARP sends ARP requests in the VLAN of the ARP entry and updates the entry with the ARP reply receiving interface.

Use display mac-address to display MAC address entries.

Examples

# Enable interface consistency check for ARP and MAC address entries.

<Sysname> system-view

[Sysname] arp mac-interface-consistency check enable

Related commands

display mac-address (Layer 2—LAN Switching Command Reference)

# New feature: 802.1X offline detection

## Configuring 802.1X offline detection

#### About 802.1X offline detection

The 802.1X offline detection feature monitors the online status of 802.1X users. This feature uses an offline detect timer to set the interval that the device waits for traffic from a user before the device determines that the user is idle. If the device has not received traffic from a user before the timer expires, the device logs off that user and requests the accounting server to stop accounting for the user.

#### Restrictions and guidelines

The 802.1X offline detection feature takes effect only on a port that performs MAC-based access control. If you change the port access mode to port-based, the 802.1X offline detection feature cannot take effect.

For this feature to operate as expected, do not set the offline detect timer to the same value as either of the following timers:

* Handshake timer (set by using the dot1x timer handshake-period command).
* Periodic reauthentication timer (set by using the dot1x timer reauth-period command).

#### Procedure

Enter system view.

system-view

Set the 802.1X offline detect timer.

dot1x timer offline-detect offline-detect-value

By default, the 802.1X offline detect timer is 300 seconds.

Enter interface view.

interface interface-type interface-number

Enable 802.1X offline detection.

dot1x offline-detect enable

By default, 802.1X offline detection is disabled.

## Command reference

### dot1x offline-detect enable

Use dot1x offline-detect enable to enable 802.1X offline detection on a port.

Use undo dot1x offline-detect enable to disable 802.1X offline detection.

Syntax

dot1x offline-detect enable

undo dot1x offline-detect enable

Default

802.1X offline detection is disabled on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

The 802.1X offline detection feature monitors the online status of 802.1X users. This feature uses an offline detect timer to set the interval that the device waits for traffic from a user before the device determines that the user is idle. If the device has not received traffic from a user before the timer expires, the device logs off that user and requests the accounting server to stop accounting for the user.

To have 802.1X offline detection take effect, you must configure the port to perform MAC-based access control. If you change the port access mode to port-based, the 802.1X offline detection feature cannot take effect.

To set the offline detect timer, use the dot1x timer command.

Examples

# Disable 802.1X offline detection on GigabitEthernet 1/0/1.

<Sysname> system-view

[Sysname] interface gigabitethernet 1/0/1

[Sysname-GigabitEthernet1/0/1] undo dot1x offline-detect enable

Related commands

display dot1x

dot1x port-method

dot1x timer

### dot1x timer offline-detect

Use dot1x timer offline-detect to set the 802.1X offline detect timer.

Use undo dot1x timer offline-detect to restore the default.

Syntax

dot1x timer offline-detect offline-detect-value

undo dot1x timer offline-detect

Default

The 802.1X offline detect timer is 300 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

offline-detect offline-detect-value: Sets the offline detect timer in seconds. The value range for the offline-detect-value argument is 60 to 2147483647.

Usage guidelines

The offline detect timer sets the interval that the device waits for traffic from a user before the device determines that the user is idle. If the device has not received traffic from a user before the timer expires, the device logs off that user and requests the accounting server to stop accounting for the user. This timer takes effect only when the 802.1X offline detection feature is enabled.

Examples

# Set the 802.1X offline detect timer to 150 seconds.

<Sysname> system-view

[Sysname] dot1x timer offline-detect 150

Related commands

display dot1x

# New feature: Enabling SAVI and setting the entry deletion delay by using commands

The ipv6 savi strict and ipv6 savi down-delay commands were added. You can use these commands to enable SAVI and set the entry deletion delay.

## About SAVI

Source Address Validation Improvement (SAVI) checks the validity of the source addresses of global unicast IPv6 packets. It implements the validity check by using the ND snooping, DHCPv6 snooping, ND attack detection, and IP source guard features. SAVI checks only global unicast addresses and forwards the packets that pass the validity check. Packets sourced from an invalid address are dropped.

## SAVI application scenarios

#### DHCPv6-only

The hosts connected to the SAVI-enabled device obtain addresses only through DHCPv6. In this scenario, SAVI drops all RA and RR messages. DHCPv6 messages, ND messages (RA and RR messages excluded), and IPv6 data packets are checked based on DHCPv6 snooping entries and static IPv6 source guard binding entries.

#### SLAAC-only

The hosts connected to the SAVI-enabled device obtain addresses only through Stateless Address Autoconfiguration (SLAAC). In this scenario, SAVI drops all DHCPv6 messages. Only ND messages and IPv6 data packets are checked based on DHCPv6 snooping entries and static IPv6 source guard binding entries.

#### DHCPv6+SLAAC

The hosts connected to the SAVI-enabled device obtain addresses through DHCPv6 and SLAAC. In this scenario, SAVI checks all DHCPv6 messages, ND messages, and IPv6 data packets based on DHCPv6 snooping entries, ND snooping entries, and static IPv6 source guard binding entries.

## SAVI tasks at a glance

To configure SAVI, perform the following tasks:

Enabling SAVI

Configuring IPv6 source guard

Configuring DHCPv6 snooping

Configuring ND snooping and ND attack detection

(Optional.) Setting the entry deletion delay

## Enabling SAVI

Enter system view.

system-view

Enable SAVI.

ipv6 savi strict

By default, SAVI is disabled.

## Configuring IPv6 source guard

Enable IPv6 source guard on an interface.

(Optional.) Configure static IPv6SG bindings.

For more information about IPv6 source guard configuration, see "Configuring IP source guard."

## Configuring DHCPv6 snooping

#### Restrictions and guidelines

Enable only DHCPv6 snooping for the SLAAC-only scenario.

#### Procedure

Enable DHCPv6 snooping.

Specify DHCPv6 snooping trusted ports.

Enable recording client information in DHCPv6 snooping entries.

For more information about DHCPv6 snooping configuration, see Layer 3—IP Services Configuration Guide.

## Configuring ND snooping and ND attack detection

#### Restrictions and guidelines

Enable only ND attack detection for the DHCPv6-only scenario.

#### Procedure

Enable ND snooping for global unicast addresses.

For more information about ND snooping, see IPv6 basics in Layer 3—IP Services Configuration Guide.

Enable ND attack detection.

For more information about ND attack detection, see "Configuring ND attack defense."

Specify ND trusted ports.

For more information about ND trusted ports, see "Configuring ND attack defense."

## Setting the entry deletion delay

#### About the entry deletion delay

The entry deletion delay is the period of time that the device waits before deleting the DHCPv6 snooping entries and ND snooping entries for a down port.

#### Procedure

Enter system view.

system-view

Set the entry deletion delay.

ipv6 savi down-delay delay-time

By default, the entry deletion delay is 30 seconds.

## SAVI configuration examples

### Example: Configuring DHCPv6-only SAVI

#### Network configuration

As shown in Figure 1, configure SAVI on the switch to meet the following requirements:

* Clients obtain IPv6 addresses only through DHCPv6.
* RA and RR messages are dropped on through in VLAN 2.
* SAVI checks the source addresses of DHCPv6 messages, ND messages (RA and RR messages excluded), and IPv6 data packets on and .

Network diagram



#### Procedure

# Enable SAVI.

<Switch> system-view

[Switch] ipv6 savi strict

# Assign through to VLAN 2.

[Switch] vlan 2

[Switch-vlan2] port

[Switch-vlan2] quit

# Enable DHCPv6 snooping.

[Switch] ipv6 dhcp snooping enable

# Configure as a DHCPv6 snooping trusted port.

[Switch] interface

[Switch-] ipv6 dhcp snooping trust

[Switch-] quit

# Enable recording DHCPv6 snooping entries on and .

[Switch] interface

[Switch-] ipv6 dhcp snooping binding record

[Switch-] quit

[Switch] interface

[Switch-] ipv6 dhcp snooping binding record

[Switch-] quit

# Enable ND attack detection.

[Switch] vlan 2

[Switch-vlan2] ipv6 nd detection enable

[Switch-vlan2] quit

# Enable IPv6 source guard on and .

[Switch] interface

[Switch-] ipv6 verify source ip-address mac-address

[Switch-] quit

[Switch] interface

[Switch-] ipv6 verify source ip-address mac-address

[Switch-] quit

### Example: Configuring SLAAC-only SAVI

#### Network configuration

As shown in Figure 2, configure SAVI on Switch B to meet the following requirements:

* Hosts obtain IPv6 addresses only through SLAAC.
* DHCPv6 messages are dropped on through in VLAN 2.
* SAVI checks the source addresses of ND messages and IPv6 data packets on and .

Network diagram



#### Procedure

# Enable SAVI.

<SwitchB> system-view

[SwitchB] ipv6 savi strict

# Assign through to VLAN 2.

[SwitchB] vlan 2

[SwitchB-vlan2] port

[SwitchB-vlan2] quit

# Enable ND snooping for global unicast addresses in VLAN 2.

[SwitchB] vlan 2

[SwitchB-vlan2] ipv6 nd snooping enable global

# Enable ND attack detection for VLAN 2.

[SwitchB-vlan2] ipv6 nd detection enable

[SwitchB-vlan2] quit

# Enable DHCPv6 snooping.

[SwitchB] ipv6 dhcp snooping enable

# Configure as an ND trusted port.

[SwitchB] interface

[SwitchB-] ipv6 nd detection trust

[SwitchB-] quit

# Enable IPv6 source guard on and .

[SwitchB] interface

[SwitchB-] ip verify source ip-address mac-address

[SwitchB-] quit

[SwitchB] interface

[SwitchB-] ip verify source ip-address mac-address

[SwitchB-] quit

### Example: Configuring DHCPv6+SLAAC SAVI

#### Network configuration

As shown in Figure 3, configure SAVI on Switch B to meet the following requirements:

* Hosts obtain IP addresses through DHCPv6 or SLAAC.
* SAVI checks the source addresses of DHCPv6 messages, ND messages, and IPv6 data packets on through .

Network diagram



#### Procedure

# Enable SAVI.

<SwitchB> system-view

[SwitchB] ipv6 savi strict

# Assign through to VLAN 2.

[SwitchB] vlan 2

[SwitchB-vlan2] port

# Enable DHCPv6 snooping.

[SwitchB] ipv6 dhcp snooping enable

# Enable recording DHCPv6 snooping entries on through .

[SwitchB] interface

[SwitchB-] ipv6 dhcp snooping binding record

[SwitchB-] quit

[SwitchB] interface

[SwitchB-] ipv6 dhcp snooping binding record

[SwitchB-] quit

[SwitchB] interface

[SwitchB-] ipv6 dhcp snooping binding record

[SwitchB-] quit

# Configure as a DHCPv6 snooping trusted port.

[SwitchB] interface

[SwitchB-] ipv6 dhcp snooping trust

[SwitchB-] quit

# Enable ND snooping for global unicast addresses in VLAN 2.

[SwitchB] vlan 2

[SwitchB-vlan2] ipv6 nd snooping enable global

# Enable ND attack detection for VLAN 2.

[SwitchB-vlan2] ipv6 nd detection enable

[SwitchB-vlan2] quit

# Configure as an ND trusted port.

[SwitchB] interface

[SwitchB-] ipv6 nd detection trust

[SwitchB-] quit

# Enable IPv6 source guard on through .

[SwitchB] interface

[SwitchB-] ip verify source ipv6 ip-address mac-address

[SwitchB-] quit

[SwitchB] interface

[SwitchB-] ip verify source ipv6 ip-address mac-address

[SwitchB-] quit

[SwitchB] interface

[SwitchB-] ip verify source ipv6 ip-address mac-address

## SAVI commands

### ipv6 savi down-delay

Use ipv6 savi down-delay to set the entry deletion delay.

Use undo ipv6 savi down-delay to restore the default.

Syntax

ipv6 savi down-delay delay-time

undo ipv6 savi down-delay

Default

The entry deletion delay is 30 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

delay-time: Specifies the entry deletion delay in the range of 0 to 21474836 seconds.

Usage guidelines

The entry deletion delay is the period of time that the device waits before deleting the DHCPv6 snooping entries and ND snooping entries for a down port.

Examples

# Set the entry deletion delay to 100 seconds.

<Sysname> system-view

[Sysname] ipv6 savi down-delay 100

### ipv6 savi strict

Use ipv6 savi strict to enable Source Address Validation Improvement (SAVI).

Use undo ipv6 savi strict to disable SAVI.

Syntax

ipv6 savi strict

undo ipv6 savi strict

Default

SAVI is disabled.

Views

System view

Predefined user roles

network-admin

Examples

# Enable SAVI.

<Sysname> system-view

[Sysname] ipv6 savi strict

Related commands

ipv6 verify source

# Modified feature: Configuring MAC-based MAC authentication user accounts

## Feature change description

Support for password configuration was added to MAC-based MAC authentication user accounts.

## Command changes

### Modified command: mac-authentication user-name-format

Old syntax

mac-authentication user-name-format { fixed [ account name ] [ password { cipher | simple } string ] | mac-address [ { with-hyphen | without-hyphen } [ lowercase | uppercase ] ] }

New syntax

mac-authentication user-name-format { fixed [ account name ] [ password { cipher | simple } string ] | mac-address [ { with-hyphen | without-hyphen } [ lowercase | uppercase ] ] [ password { cipher | simple } string ] }

Views

System view

Change description

Before modification: You cannot specify a password for MAC-based MAC authentication user accounts. The MAC address of each user is used as the password.

After modification: You can specify a password for all MAC-based MAC authentication user accounts by using the password { cipher | simple } string option. If you do not specify a password, each user uses its own MAC address as the password.

* password: Specifies the password for MAC-based MAC authentication user accounts.
* cipher: Specifies a password in encrypted form.
* simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.
* string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

# Modified feature: Port security NTK feature

## Feature change description

In this release, the ntkauto mode was added to the need to known (NTK) feature of port security.

## Command changes

### Modified command: port-security ntk-mode

Old syntax

port-security ntk-mode { ntk-withbroadcasts | ntk-withmulticasts | ntkonly }

New syntax

port-security ntk-mode { ntk-withbroadcasts | ntk-withmulticasts | ntkauto | ntkonly }

Views

Layer 2 Ethernet interface view

Change description

Before modification: The ntkauto keyword was not added to this command.

After modification: The ntkauto keyword was not added to this command. This keyword specifies the ntkauto mode. A port in ntkauto mode forwards broadcast frames, multicast frames, and unicast frames with authenticated destination MAC addresses only when the port has online users.

1. Release 3208P08

This release has the following changes:

New feature: Shutting down an interface by OpenFlow

# New feature: Shutting down an interface by OpenFlow

## Shut down an interface by OpenFlow.

#### About interface shutdown

After an interface is shut down by OpenFlow, the Current state field displays OFP DOWN in the display interface command output.

You can use the undo openflow shutdown command to bring up an interface shut down by OpenFlow. The interface can also be brought up by port modification messages from controllers.

#### Procedure

Enter system view.

system-view

Enter interface view.

interface interface-type interface-number

Shut down an interface by OpenFlow.

openflow shutdown

By default, an interface is not shut down by OpenFlow.

## Command reference

### openflow shutdown

Use openflow shutdown to shut down an interface by OpenFlow.

Use undo openflow shutdown to restore the default.

Syntax

openflow shutdown

undo openflow shutdown

Default

An interface is not shut down by OpenFlow.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

After an interface is shut down by OpenFlow, the Current state field displays OFP DOWN in the display interface command output.

To bring up an interface shut down by OpenFlow, use either of the following methods:

* Use the undo openflow shutdown command on the interface.
* Use the controller to send port modification messages to the interface.

Examples

# Shut down by OpenFlow.

<Sysname> system-view

[Sysname] interface

[Sysname-] openflow shutdown

1. Release 3208P03

This release has the following changes:

New feature: VRRP

# New feature: VRRP

VRRP does not take effect on member ports of aggregation groups.

## About VRRP

Typically, you can configure a default gateway for every host on a LAN. All packets destined for other networks are sent through the default gateway. As shown in Figure 1, when the default gateway fails, no hosts can communicate with external networks.

LAN networking



Using a default gateway facilitates your configuration but requires high availability. Using more egress gateways improves link availability but introduces the problem of routing among the egresses.

Virtual Router Redundancy Protocol (VRRP) is designed to address this issue. VRRP adds a group of network gateways to a VRRP group called a virtual router. The VRRP group has one master and multiple backups, and provides a virtual IP address. The hosts on the subnet use the virtual IP address as their default network gateway to communicate with external networks.

VRRP avoids single points of failure and simplifies the configuration on hosts. When the master in the VRRP group on a multicast or broadcast LAN (for example, an Ethernet network) fails, another router in the VRRP group takes over. The switchover is complete without causing dynamic route recalculation, route re-discovery, gateway reconfiguration on the hosts, or traffic interruption.

VRRP operates in either of the following modes:

* Standard mode—Implemented based on RFCs. For more information, see "VRRP standard mode."
* Load balancing mode—Extends the VRRP standard mode to distribute load across VRRP group members. For more information, see "VRRP load balancing mode."

VRRP has two versions: VRRPv2 and VRRPv3. VRRPv2 supports IPv4 VRRP. VRRPv3 supports IPv4 VRRP and IPv6 VRRP.

## VRRP standard mode

### VRRP networking

As shown in Figure 2, Router A, Router B, and Router C form a virtual router, which has its own IP address. Hosts on the subnet use the virtual router as the default gateway.

The router with the highest priority among the three routers is elected as the master, and the other two are backups. Only the master in the VRRP group can provide gateway service. When the master fails, the backup routers elect a new master to take over for nonstop gateway service.

VRRP networking



### Virtual IP address and IP address owner

The virtual IP address of the virtual router can be either of the following IP addresses:

* Unused IP address on the subnet where the VRRP group resides.
* IP address of an interface on a router in the VRRP group.

In the latter case, the router is called the IP address owner. A VRRP group can have only one IP address owner.

### Router priority in a VRRP group

VRRP determines the role (master or backup) of each router in a VRRP group by priority. A router with higher priority is more likely to become the master.

A VRRP priority can be in the range of 0 to 255, and a greater number represents a higher priority. Priorities 1 to 254 are configurable. Priority 0 is reserved for special uses, and priority 255 is for the IP address owner. The IP address owner in a VRRP group always has a running priority of 255 and acts as the master as long as it operates correctly.

### Preemption

A router in a VRRP group operates in either non-preemptive mode or preemptive mode.

* Non-preemptive mode—The master router acts as the master as long as it operates correctly, even if a backup router is later assigned a higher priority. Non-preemptive mode helps avoid frequent switchover between the master and backup routers.
* Preemptive mode—A backup starts a new master election and takes over as master when it detects that it has a higher priority than the current master. Preemptive mode ensures that the router with the highest priority in a VRRP group always acts as the master.

### Authentication method

To avoid attacks from unauthorized users, VRRP member routers add authentication keys in VRRP packets to authenticate one another. VRRP provides the following authentication methods:

* Simple authentication

The sender fills an authentication key into the VRRP packet, and the receiver compares the received authentication key with its local authentication key. If the two authentication keys match, the received VRRP packet is legitimate. Otherwise, the received packet is illegitimate and gets discarded.

* MD5 authentication

The sender computes a digest for the VRRP packet by using the authentication key and MD5 algorithm, and saves the result to the packet. The receiver performs the same operation with the authentication key and MD5 algorithm, and compares the result with the content in the authentication header. If the results match, the received VRRP packet is legitimate. Otherwise, the received packet is illegitimate and gets discarded.

On a secure network, you can choose to not authenticate VRRP packets.

|  | NOTE:  IPv4 VRRPv3 and IPv6 VRRPv3 do not support VRRP packet authentication. |
| --- | --- |

### VRRP timers

#### Skew\_Time

Skew\_Time helps avoid the situation that multiple backups in a VRRP group become the master when the master in the VRRP group fails.

Skew\_Time is not configurable; its value depends on the VRRP version.

* In VRRPv2 (described in RFC 3768), Skew\_Time is (256 – Router priority)/256.
* In VRRPv3 (described in RFC 5798), Skew\_Time is ((256 – Router priority) × VRRP advertisement interval)/256.

#### VRRP advertisement interval

The master in a VRRP group periodically sends VRRP advertisements to declare its presence.

You can configure the interval at which the master sends VRRP advertisements. If a backup does not receive any VRRP advertisement when the timer (3 × VRRP advertisement interval + Skew\_Time) expires, it takes over as the master.

#### VRRP preemption delay timer

You can configure the VRRP preemption delay timer for the following purposes:

* Avoid frequent state changes among members in a VRRP group.
* Provide the backups with enough time to collect information (such as routing information).

In preempt mode, a backup does not immediately become the master after it receives an advertisement with lower priority than the local priority. Instead, it waits for a period of time (preemption delay time + Skew\_Time) before taking over as the master.

### Master election

Routers in a VRRP group determine their roles by priority. When a router joins a VRRP group, it has a backup role. The router role changes according to the following situations:

* If the backup does not receive any VRRP advertisement when the timer (3 × advertisement interval + Skew\_Time) expires, it becomes the master.
* If the backup receives a VRRP advertisement with the same or greater priority within the timer (3 × advertisement interval + Skew\_Time), it remains a backup.
* If the backup receives a VRRP advertisement with a smaller priority within the timer (3 × advertisement interval + Skew\_Time), the following results apply:
  + It remains a backup when operating in non-preemptive mode.
  + It becomes the master when operating in preemptive mode.

The elected master starts a VRRP advertisement interval to periodically send VRRP advertisements to notify the backups that it is operating correctly. Each of the backups starts a timer to wait for advertisements from the master.

When multiple routers in a VRRP group declare that they are the master because of network problems, the one with the highest priority becomes the master. If two routers have the same priority, the one with the highest IP address becomes the master.

### VRRP tracking

The VRRP tracking function uses network quality analyzer (NQA) or bidirectional forwarding detection (BFD) to monitor the state of the master or the upstream link. The collaboration between VRRP and NQA or BFD through a track entry implements the following functions:

* Monitors the upstream link and changes the priority of the router according to the state of the link. If the upstream link fails, the hosts on the subnet cannot access external networks through the router and the state of the track entry becomes Negative. The priority of the master decreases by a specified value, and a router with a higher priority in the VRRP group becomes the master. The switchover ensures uninterrupted communication between the hosts on the subnet and external networks.
* Monitors the state of the master on the backups. When the master fails, a backup immediately takes over to ensure uninterrupted communication.

When the track entry changes from Negative to Positive or Notready, the router automatically restores its priority. For more information about track entries, see "Configuring Track."

To enable VRRP tracking, configure the routers in the VRRP group to operate in preemptive mode first. This configuration ensures that only the router with the highest priority operates as the master.

### VRRP application

#### Master/backup

In master/backup mode, only the master forwards packets, as shown in Figure 3. When the master fails, a new master is elected from among the backups. This mode requires only one VRRP group, and each router in the group has a different priority. The one with the highest priority becomes the master.

VRRP in master/backup mode



Assume that Router A is acting as the master to forward packets to external networks, and Router B and Router C are backups in listening state. When Router A fails, Router B and Router C elect a new master to forward packets for hosts on the subnet.

#### Load sharing

A router can join multiple VRRP groups. With different priorities in different VRRP groups, the router can act as the master in one VRRP group and a backup in another.

In load sharing mode, multiple VRRP groups provide gateway services. This mode requires a minimum of two VRRP groups, and each group has one master and multiple backups. The master roles in the VRRP groups are assumed by different routers, as shown in Figure 4.

Load sharing of VRRP



A router can be in multiple VRRP groups and have a different priority in each group.

As shown in Figure 4, the following VRRP groups exist:

* VRRP group 1—Router A is the master. Router B and Router C are the backups.
* VRRP group 2—Router B is the master. Router A and Router C are the backups.
* VRRP group 3—Router C is the master. Router A and Router B are the backups.

To implement load sharing among Router A, Router B, and Router C, perform the following tasks:

* Configure the virtual IP addresses of VRRP group 1, 2, and 3 as default gateway IP addresses for hosts on the subnet.
* Assign the highest priority to Router A, B, and C in VRRP group 1, 2, and 3, respectively.

## VRRP load balancing mode

In a standard-mode VRRP group, only the master can forward packets and backups are in listening state. You can create multiple VRRP groups to share traffic, but you must configure different gateways for hosts on the subnet.

In load balancing mode, a VRRP group maps its virtual IP address to multiple virtual MAC addresses, assigning one virtual MAC address to each member router. Every router in this VRRP group can forward traffic and respond to IPv4 ARP requests or IPv6 ND requests from hosts. Because their virtual MAC addresses are different, traffic from hosts is distributed across the VRRP group members. Load balancing mode simplifies configuration and improves forwarding efficiency.

VRRP load balancing mode uses the same master election, preemption, and tracking mechanisms as the standard mode. New mechanisms have been introduced to VRRP load balancing mode, as described in the following sections.

### Virtual MAC address assignment

In load balancing mode, the master assigns virtual MAC addresses to routers in the VRRP group. The master uses different MAC addresses to respond to ARP requests or ND requests from different hosts. The backup routers, however, do not answer ARP requests or ND requests from hosts.

In an IPv4 network, a load balanced VRRP group works as follows:

The master assigns virtual MAC addresses to all member routers, including itself. This example assumes that the virtual IP address of the VRRP group is 10.1.1.1/24, Router A is the master, and Router B is the backup. Router A assigns 000f-e2ff-0011 for itself and 000f-e2ff-0012 for Router B. See Figure 5.

Virtual MAC address assignment



When an ARP request arrives, the master (Router A) selects a virtual MAC address based on the load balancing algorithm to answer the ARP request. In this example, Router A returns the virtual MAC address of itself in response to the ARP request from Host A. Router A returns the virtual MAC address of Router B in response to the ARP request from Host B. See Figure 6.

Answering ARP requests



Each host sends packets to the returned MAC address. As shown in Figure 7, Host A sends packets to Router A and Host B sends packets to Router B.

Sending packets to different routers for forwarding



In the ARP reply sent by the master, the source MAC address in the Ethernet header is different from the sender MAC address in the message body. For the Layer 2 device to forward the ARP packet, follow these configuration guidelines on the Layer 2 device:

* Do not enable ARP packet source MAC address consistency check.
* Do not specify the src-mac keyword when you enable ARP packet validity check for ARP detection.

For more information about ARP packet source MAC address consistency check and ARP detection, see Security Configuration Guide.

### Virtual forwarder

#### Virtual forwarder creation

Virtual MAC addresses enable traffic distribution across routers in a VRRP group. To enable routers in the VRRP group to forward packets, VFs must be created on them. Each VF is associated with a virtual MAC address in the VRRP group and forwards packets that are sent to this virtual MAC address.

VFs are created on routers in a VRRP group, as follows:

The master assigns virtual MAC addresses to all routers in the VRRP group. Each member router creates a VF for this MAC address and becomes the owner of this VF.

Each VF owner advertises its VF information to the other member routers.

After receiving the VF advertisement, each of the other routers creates the advertised VF.

Eventually, every member router maintains one VF for each virtual MAC address in the VRRP group.

#### VF weight and priority

The weight of a VF indicates the forwarding capability of a VF. A higher weight means higher forwarding capability. When the weight is lower than the lower limit of failure, the VF cannot forward packets.

The priority of a VF determines the VF state. Among the VFs created on different member routers for the same virtual MAC address, the VF with the highest priority is in active state. This VF, known as the active virtual forwarder (AVF), forwards packets. All other VFs listen to the state of the AVF and are known as the listening virtual forwarders (LVFs). VF priority is in the range of 0 to 255, where 255 is reserved for the VF owner. When the weight of a VF owner is higher than or equal to the lower limit of failure, the priority of the VF owner is 255.

The priority of a VF is calculated based on its weight.

* If the VF weight is higher than or equal to the lower limit of failure, the following VF priorities apply:
  + On a VF owner, the VF priority is 255.
  + On a non-VF owner, the VF priority is calculated as weight/(number of local AVFs + 1).
* If the VF weight is lower than the lower limit of failure, the VF priority is 0.

#### VF backup

The VFs corresponding to a virtual MAC address on different routers in the VRRP group back up one another.

VF information



Figure 8 shows the VF table on each router in the VRRP group and how the VFs back up one another. The master, Router A, assigns virtual MAC addresses 000f-e2ff-0011, 000f-e2ff-0012, and 000f-e2ff-0013 to itself, Router B, and Router C, respectively. Each router creates VF 1, VF 2, and VF 3 for virtual MAC addresses 000f-e2ff-0011, 000f-e2ff-0012, and 000f-e2ff-0013, respectively. The VFs for the same virtual MAC address on different routers back up one another. For example, the VF 1 instances on Router A, Router B, and Router C back up one another.

* The VF 1 instance on Router A (the VF 1 owner) has priority 255. It acts as the AVF to forward packets sent to virtual MAC address 000f-e2ff-0011.
* The VF 1 instances on Router B and Router C have a priority of 255/(1 + 1), or 127. Because their priorities are lower than the priority of the VF 1 instance on Router A, they act as LVFs. These LVFs listen to the state of the VF 1 instance on Router A.
* When the VF 1 instance on Router A fails, the VF 1 instances on Router B and Router C elect the one with higher priority as the new AVF. This AVF forwards packets destined for virtual MAC address 000f-e2ff-0011. If the two LVFs' priorities are the same, the LVF with a greater device MAC address becomes the new AVF.

A VF always operates in preemptive mode. When an LVF finds its priority value higher than the one advertised by the AVF, the LVF declares itself as the AVF.

#### VF timers

When the AVF on a router fails, the new AVF on another router creates the following timers for the failed AVF:

* Redirect timer—Before this timer expires, the master still uses the virtual MAC address corresponding to the failed AVF to respond to ARP/ND requests from hosts. The VF owner can share traffic load if the VF owner resumes normal operation within this time. When this timer expires, the master stops using the virtual MAC address corresponding to the failed AVF to respond to ARP/ND requests from hosts.
* Timeout timer—The duration after which the new AVF takes over responsibilities of the failed VF owner. Before this timer expires, all routers in the VRRP group keep the VFs that correspond to the failed AVF. The new AVF forwards packets destined for the virtual MAC address of the failed AVF. When this timer expires, all routers in the VRRP group remove the VFs that correspond to the failed AVF, including the new AVF. Packets destined for the virtual MAC address of the failed AVF are not forwarded any longer.

#### VF tracking

An AVF forwards packets destined for the MAC address of the AVF. If the AVF's upstream link fails but no LVF takes over, the hosts that use the AVF's MAC address as their gateway MAC address cannot access the external network.

The VF tracking function can solve this problem. You can use NQA or BFD to monitor the upstream link state of the VF owner, and associate the VFs with NQA or BFD through the tracking function. This enables the collaboration between VRRP and NQA or BFD through the Track module. When the upstream link fails, the state of the track entry changes to Negative. The weights of the VFs (including the AVF) on the router decrease by a specific value. The corresponding LVF with a higher priority on another router becomes the AVF and forwards packets.

## Protocols and standards

* RFC 3768, Virtual Router Redundancy Protocol (VRRP)
* RFC 5798, Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6

## Configuring IPv4 VRRP

### Restrictions and guidelines: IPv4 VRRP configuration

* IPv4 VRRP does not take effect on member ports of aggregation groups.
* Configuration on the routers in an IPv4 VRRP group must be consistent.

### IPv4 VRRP tasks at a glance

To configure IPv4 VRRP, perform the following tasks:

Specifying an IPv4 VRRP operating mode

(Optional.) Specifying the IPv4 VRRP version

Configuring an IPv4 VRRP group

(Optional.) Configuring IPv4 VRRP packet attributes

(Optional.) Configuring VF tracking

This configuration takes effect only in VRRP load balancing mode.

(Optional.) Setting the packet sending mode for IPv4 VRRPv3

(Optional.) Enabling periodic sending of gratuitous ARP packets for IPv4 VRRP

(Optional.) Configuring a subordinate IPv4 VRRP group to follow a master IPv4 VRRP group

(Optional.) Enabling SNMP notifications for VRRP

### Specifying an IPv4 VRRP operating mode

#### Restrictions and guidelines

After an IPv4 VRRP operating mode is configured on a router, all IPv4 VRRP groups on the router operate in the specified operating mode.

#### Procedure

Enter system view.

system-view

Specify an IPv4 VRRP operating mode.

* + Specify the standard mode.
  + undo vrrp mode
  + Specify the load balancing mode.
  + vrrp mode load-balance [ version-8 ]

By default, VRRP operates in standard mode.

### Specifying the IPv4 VRRP version

#### About IPv4 VRRP versions

IPv4 VRRP can use VRRPv2 and VRRPv3.

#### Restrictions and guidelines

For an IPv4 VRRP group to operate correctly, make sure the same VRRP version is used on all routers in the IPv4 VRRP group.

#### Procedure

Enter system view.

system-view

Enter interface view.

interface interface-type interface-number

Specify the version of VRRP.

vrrp version version-number

By default, VRRPv3 is used.

### Configuring an IPv4 VRRP group

#### About IPv4 VRRP group

A VRRP group can operate correctly after you create it and assign a minimum of one virtual IP address to it. You can configure multiple virtual IP addresses for the VRRP group on an interface that connects to multiple subnets for router backup on different subnets.

If you disable an IPv4 VRRP group, the VRRP group enters initialized state, and the existing configuration on the VRRP group remains unchanged. You can modify the configuration of the VRRP group. The modification takes effect when you enable the VRRP group again.

#### Restrictions and guidelines

| Item | Remarks |
| --- | --- |
| VLAN interface | Do not create a VRRP group on the VLAN interface of a super VLAN because network performance might be adversely affected. For information about the super VLAN feature, see Layer 2—LAN Switching Configuration Guide. |
| Maximum number of VRRP groups and virtual IP addresses | In VRRP load balancing mode, the device supports a maximum of MaxVRNum/N VRRP groups. MaxVRNum refers to the maximum number of VRRP groups supported by the device in VRRP standard mode. N refers to the number of devices in the VRRP group. |
| Virtual IP address | When VRRP is operating in standard mode, the virtual IP address of a VRRP group can be either of the following addresses:   * + - * Unused IP address on the subnet where the VRRP group resides.       * IP address of an interface on a router in the VRRP group.   In load balancing mode, the virtual IP address of a VRRP group can be any unassigned IP address of the subnet where the VRRP group resides. It cannot be the IP address of any interfaces in the VRRP group. No IP address owner can exist in a VRRP group.  An IPv4 VRRP group without virtual IP addresses configured can exist on a device provided that other settings (for example, priority and preemption mode) are available. Such a VRRP group stays in inactive state and does not function.  For hosts in the subnet to access external networks, as a best practice, configure the following addresses in the same subnet:   * + - * Virtual IP address of an IPv4 VRRP group.       * Downlink interface IP addresses of the VRRP group members. |
| IP address owner | On an IP address owner, as a best practice, do not use the network command to enable OSPF on the interface owning the virtual IP address of the VRRP group. For more information about the network command, see Layer 3—IP Routing Command Reference.  Removal of the VRRP group on the IP address owner causes IP address collision. To avoid the collision, change the IP address of the interface on the IP address owner before you remove the VRRP group from the interface.  The running priority of an IP address owner is always 255, and you do not need to configure it. An IP address owner always operates in preemptive mode.  If you configure the vrrp vrid track priority reduced or vrrp vrid track switchover command on an IP address owner, the configuration does not take effect until the router becomes a non-IP address owner. |
| VRRP association with a track entry | When the track entry changes from Negative to Positive or Notready, the router automatically restores its priority or the failed master router becomes the master again. |

#### Creating a VRRP group and assigning a virtual IP address

Enter system view.

system-view

Enter interface view.

interface interface-type interface-number

Create a VRRP group and assign a virtual IP address.

vrrp vrid virtual-router-id virtual-ip virtual-address

#### Configuring an IPv4 VRRP group

Enter system view.

system-view

Enter interface view.

interface interface-type interface-number

Set the priority of the router in the VRRP group.

vrrp vrid virtual-router-id priority priority-value

The default setting is 100.

Enable the preemptive mode for the router in a VRRP group and set the preemption delay time.

vrrp vrid virtual-router-id preempt-mode [ delay delay-value ]

By default, the router in a VRRP group operates in preemptive mode and the preemption delay time is 0 centiseconds, which means an immediate preemption.

Associate a VRRP group with a track entry.

vrrp vrid virtual-router-id track track-entry-number { forwarder-switchover member-ip ip-address | priority reduced [ priority-reduced ] | switchover | weight reduced [ weight-reduced ] }

By default, a VRRP group is not associated with any track entries.

#### Disabling an IPv4 VRRP group

Enter system view.

system-view

Enter interface view.

interface interface-type interface-number

Disable a VRRP group.

vrrp vrid virtual-router-id shutdown

### Configuring IPv4 VRRP packet attributes

#### Restrictions and guidelines

* You can configure different authentication modes and authentication keys for VRRP groups on an interface. However, members of the same VRRP group must use the same authentication mode and authentication key.
* In VRRPv2, all routers in a VRRP group must have the same VRRP advertisement interval.
* In VRRPv3, authentication mode and authentication key settings do not take effect.
* In VRRPv3, routers in an IPv4 VRRP group can have different intervals for sending VRRP advertisements. The master in the VRRP group sends VRRP advertisements at specified intervals, and carries the interval in the advertisements. After a backup receives the advertisement, it records the interval in the advertisement. If the backup does not receive a VRRP advertisement before the timer (3 x recorded interval + Skew\_Time) expires, it regards the master as failed and takes over.

#### Procedure

Enter system view.

system-view

Enter interface view.

interface interface-type interface-number

Configure the authentication mode and authentication key for an IPv4 VRRP group to send and receive VRRP packets.

vrrp vrid virtual-router-id authentication-mode { md5 | simple } { cipher | plain } string

By default, authentication is disabled.

Set the interval at which the master in an IPv4 VRRP group sends VRRP advertisements.

vrrp vrid virtual-router-id timer advertise adver-interval

The default setting is 100 centiseconds.

As a best practice to maintain system stability, set the VRRP advertisement interval to be greater than 100 centiseconds.

Specify the source interface for receiving and sending VRRP packets.

vrrp vrid virtual-router-id source-interface interface-type interface-number

By default, the source interface for receiving and sending VRRP packets is not specified. The interface where the VRRP group resides sends and receives VRRP packets.

Enable TTL check for IPv4 VRRP packets.

vrrp check-ttl enable

By default, TTL check for IPv4 VRRP packets is enabled.

Return to system view.

quit

Set a DSCP value for VRRP packets.

vrrp dscp dscp-value

By default, the DSCP value for VRRP packets is 48.

The DSCP value identifies the packet priority during transmission.

### Configuring VF tracking

#### About VF tracking

You can configure VF tracking in both standard mode and load balancing mode, but the function takes effect only in load balancing mode.

In load balancing mode, you can establish the collaboration between the VFs and NQA or BFD through the tracking function. When the state of the track entry transits to Negative, the weights of all VFs in the VRRP group on the router decrease by a specific value. When the state of the track entry transits to Positive or Notready, the original weight values of the VFs restore.

#### Restrictions and guidelines

* By default, the weight of a VF is 255, and its lower limit of failure is 10.
* When the weight of a VF owner is higher than or equal to the lower limit of failure, its priority is always 255. The priority does not change with the weight. When the upstream link of the VF owner fails, an LVF must take over as the AVF. The switchover happens when the weight of the VF owner drops below the lower limit of failure. This requires that the reduced weight for the VF owner be higher than 245.

#### Procedure

Enter system view.

system-view

Enter interface view.

interface interface-type interface-number

Configure the VFs in a VRRP group to monitor a track entry.

vrrp vrid virtual-router-id track track-entry-number { forwarder-switchover member-ip ip-address | priority reduced [ priority-reduced ] | switchover | weight reduced [ weight-reduced ] }

By default, no track entry is specified.

### Setting the packet sending mode for IPv4 VRRPv3

#### About the packet sending mode for IPv4 VRRPv3

A router configured with VRRPv3 can process incoming VRRPv2 packets, but a router configured with VRRPv2 cannot process incoming VRRPv3 packets. When the VRRP version of the routers in a VRRP group is changed from VRRPv2 to VRRPv3, multiple masters might be elected in the VRRP group. To resolve the problem, you can set the packet sending mode for IPv4 VRRPv3. This task enables a router configured with VRRPv3 to send VRRPv2 packets and communicate with routers configured with VRRPv2.

#### Restrictions and guidelines

* The packet sending mode for IPv4 VRRPv3 takes effect only on outgoing VRRP packets. A router configured with VRRPv3 can process incoming VRRPv2 and VRRPv3 packets.
* If you set the packet sending mode for IPv4 VRRPv3 and configure VRRP packet authentication, authentication information will be carried in outgoing VRRPv2 packets but not in outgoing VRRPv3 packets.
* The VRRP advertisement interval is set in centiseconds by using the vrrp vrid timer advertise command. The VRRP advertisement interval carried in VRRPv2 packets sent from routers configured with VRRPv3 might be different from the configured value. For information about the VRRP advertisement interval, see the vrrp vrid timer advertise command in High Availability Command Reference.

#### Procedure

Enter system view.

system-view

Enter interface view.

interface interface-type interface-number

Set the packet sending mode for IPv4 VRRPv3.

vrrp vrid virtual-router-id vrrpv3-send-packet { v2-only | v2v3-both }

By default, a router configured with VRRPv3 sends only VRRPv3 packets.

### Enabling periodic sending of gratuitous ARP packets for IPv4 VRRP

#### About periodic sending of gratuitous ARP packets for IPv4 VRRP

This feature enables the master router in a VRRP group to periodically send gratuitous ARP packets. Then the downstream devices can update the MAC address entry for the virtual MAC address of the VRRP group in a timely manner.

#### Restrictions and guidelines

* This feature takes effect only in VRRP standard mode.
* If you change the sending interval for gratuitous ARP packets, the configuration takes effect at the next sending interval.
* The master sends the first gratuitous ARP packet at a random time in the second half of the set interval after you execute the vrrp send-gratuitous-arp command. This prevents too many gratuitous ARP packets from being sent at the same time.
* The sending interval for gratuitous ARP packets might be much longer than the set interval when the following conditions are met:
  + Multiple VRRP groups exist on the device.
  + A short sending interval is set.

#### Procedure

Enter system view.

system-view

Enable periodic sending of gratuitous ARP packets for IPv4 VRRP.

vrrp send-gratuitous-arp [ interval interval ]

By default, periodic sending of gratuitous ARP packets is disabled for IPv4 VRRP.

### Configuring a subordinate IPv4 VRRP group to follow a master IPv4 VRRP group

#### About master and subordinate IPv4 VRRP groups

Each VRRP group determines the device role (master or backup) by exchanging VRRP packets among member devices, which might consume excessive bandwidth and CPU resources. To reduce the number of VRRP packets in the network, you can configure a subordinate VRRP group to follow a master VRRP group.

A master VRRP group determines the device role through exchanging VRRP packets among member devices. A VRRP group that follows a master group, called a subordinate VRRP group, does not exchange VRRP packets among its member devices. The state of the subordinate VRRP group follows the state of the master group.

#### Restrictions and guidelines

* To ensure the master router election, configure the settings such as the router priority, preemptive mode, and tracking function for the master IPv4 VRRP group. The settings are not required for subordinate IPv4 VRRP groups.
* You can configure a subordinate VRRP group to follow a master VRRP group in both VRRP standard and load balancing modes. The configuration takes effect only in VRRP standard mode.
* An IPv4 VRRP group cannot be both a master group and a subordinate group.
* An IPv4 VRRP group stays in Inactive state if it is configured to follow a nonexistent master group.
* If an IPv4 VRRP group in Inactive or Initialize state follows a master group that is not in Inactive state, the state of the VRRP group does not change.
* A subordinate IPv4 VRRP group does not exchange VRRP packets, which might cause the MAC address entry for its virtual MAC address not to be updated on downstream devices. As a best practice, enable periodic sending of gratuitous ARP packets for IPv4 VRRP by using the vrrp send-gratuitous-arp command.

#### Procedure

Enter system view.

system-view

Enter interface view.

interface interface-type interface-number

Configure an IPv4 VRRP group as a master group and assign a name to it.

vrrp vrid virtual-router-id name name

By default, an IPv4 VRRP group does not act as a master group.

Return to system view.

quit

Enter interface view.

interface interface-type interface-number

Configure an IPv4 VRRP group to follow a master group.

vrrp vrid virtual-router-id follow name

By default, an IPv4 VRRP group does not follow a master VRRP group.

### Enabling SNMP notifications for VRRP

#### About SNMP notifications for VRRP

To report critical VRRP events to an NMS, enable SNMP notifications for VRRP. For VRRP event notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

#### Procedure

Enter system view.

system-view

Enable SNMP notifications for VRRP.

snmp-agent trap enable vrrp [ auth-failure | new-master ]

By default, SNMP notifications for VRRP are enabled.

### Display and maintenance commands for IPv4 VRRP

Execute display commands in any view and the reset command in user view.

| Task | Command |
| --- | --- |
| Display states of IPv4 VRRP groups. | display vrrp [ interface interface-type interface-number [ vrid virtual-router-id ] ] [ verbose ] |
| Display master-to-subordinate IPv4 VRRP group bindings. | display vrrp binding [ interface interface-type interface-number [ vrid virtual-router-id ] | name name ] |
| Display statistics for IPv4 VRRP groups. | display vrrp statistics [ interface interface-type interface-number [ vrid virtual-router-id ] ] |
| Clear statistics for IPv4 VRRP groups. | reset vrrp statistics [ interface interface-type interface-number [ vrid virtual-router-id ] ] |

## Configuring IPv6 VRRP

### Restrictions and guidelines: IPv6 VRRP configuration

* IPv6 VRRP does not take effect on member ports of aggregation groups.
* Configuration on the routers in an IPv6 VRRP group must be consistent.

### IPv6 VRRP tasks at a glance

To configure IPv6 VRRP, perform the following tasks:

Specifying an IPv6 VRRP operating mode

Configuring an IPv6 VRRP group

(Optional.) Configuring VF tracking

This configuration takes effect only in VRRP load balancing mode.

(Optional.) Configuring IPv6 VRRP packet attributes

(Optional.) Enabling periodic sending of ND packets for IPv6 VRRP

(Optional.) Configuring a subordinate IPv6 VRRP group to follow a master IPv6 VRRP group

### Specifying an IPv6 VRRP operating mode

#### Restrictions and guidelines

After the IPv6 VRRP operating mode is specified on a router, all IPv6 VRRP groups on the router operate in the specified operating mode.

#### Procedure

Enter system view.

system-view

Specify an IPv6 VRRP operating mode.

* + Specify the standard mode.
  + undo vrrp ipv6 mode
  + Specify the load balancing mode.
  + vrrp ipv6 mode load-balance

By default, VRRP operates in standard mode.

### Configuring an IPv6 VRRP group

#### About IPv6 VRRP group

A VRRP group can work correctly after you create it and assign a minimum of one virtual IPv6 address for it. You can configure multiple virtual IPv6 addresses for the VRRP group on an interface that connects to multiple subnets for router backup.

If you disable an IPv6 VRRP group, the VRRP group enters initialized state, and the existing configuration on the VRRP group remains unchanged. You can modify the configuration of the VRRP group. The modification takes effect when you enable the VRRP group again.

#### Restrictions and guidelines

| Item | Remarks |
| --- | --- |
| VLAN interface | Do not create VRRP groups on the VLAN interface of a super VLAN. Otherwise, network performance might be adversely affected. For information about the super VLAN feature, see Layer 2—LAN Switching Configuration Guide. |
| Maximum number of VRRP groups and virtual IPv6 addresses | In VRRP load balancing mode, the device supports a maximum of MaxVRNum/N VRRP groups. MaxVRNum refers to the maximum number of VRRP groups supported by the device in VRRP standard mode. N refers to the number of devices in the VRRP group. |
| Virtual IPv6 address | In load balancing mode, the virtual IPv6 address of a VRRP group cannot be the same as the IPv6 address of any interfaces in the VRRP group. No IP address owner can exist in a VRRP group.  An IPv6 VRRP group without virtual IPv6 addresses configured can exist on a device provided that other settings (for example, priority and preemption mode) are available. Such a VRRP group stays in inactive state and does not function.  For hosts in the subnet to access external networks, as a best practice, configure the following addresses in the same subnet:   * + - * Virtual IPv6 address of an IPv6 VRRP group.       * Downlink interface IPv6 addresses of the VRRP group members. |
| IP address owner | On an IP address owner, as a best practice, do not use the ospfv3 area command to enable OSPF on the interface owning the virtual IPv6 address of the VRRP group. For more information about the ospfv3 area command, see Layer 3—IP Routing Command Reference.  Removal of the VRRP group on the IP address owner causes IP address collision. To avoid the collision, change the IPv6 address of the interface on the IP address owner before you remove the VRRP group from the interface.  The running priority of an IP address owner is always 255, and you do not need to configure it. An IP address owner always operates in preemptive mode.  If you configure the vrrp ipv6 vrid track priority reduced or vrrp ipv6 vrid track switchover command on an IP address owner, the configuration does not take effect until the router becomes a non-IP address owner. |
| VRRP association with a track entry | When the track entry changes from Negative to Positive or Notready, the router automatically restores its priority or the failed master router becomes the master again. |

#### Creating a VRRP group and assign a virtual IPv6 address

Enter system view.

system-view

Enter interface view.

interface interface-type interface-number

Create a VRRP group and assign a virtual IPv6 address, which is a link-local address.

vrrp ipv6 vrid virtual-router-id virtual-ip virtual-address link-local

The first virtual IPv6 address that you assign to an IPv6 VRRP group must be a link-local address. It must be the last address you remove. Only one link-local address is allowed in a VRRP group.

#### Configuring an IPv6 VRRP group

Enter system view.

system-view

Enter interface view.

interface interface-type interface-number

Assign a virtual IPv6 address, which is a global unicast address.

vrrp ipv6 vrid virtual-router-id virtual-ip virtual-address

By default, no global unicast address is assigned to an IPv6 VRRP group.

Set the priority of the router in the VRRP group.

vrrp ipv6 vrid virtual-router-id priority priority-value

The default setting is 100.

Enable the preemptive mode for the router in a VRRP group and set the preemption delay time.

vrrp ipv6 vrid virtual-router-id preempt-mode [ delay delay-value ]

By default, the router in a VRRP group operates in preemptive mode and the preemption delay time is 0 centiseconds, which means an immediate preemption.

Associate a VRRP group with a track entry.

vrrp ipv6 vrid virtual-router-id track track-entry-number { forwarder-switchover member-ip ipv6-address | priority reduced [ priority-reduced ] | switchover | weight reduced [ weight-reduced ] }

By default, a VRRP group is not associated with any track entries.

#### Disabling an IPv6 VRRP group

Enter system view.

system-view

Enter interface view.

interface interface-type interface-number

Disable an IPv6 VRRP group.

vrrp ipv6 vrid virtual-router-id shutdown

By default, an IPv6 VRRP group is enabled.

### Configuring VF tracking

#### About VF tracking

You can configure VF tracking in both standard mode and load balancing mode, but the function takes effect only in load balancing mode.

In load balancing mode, you can configure the VFs in a VRRP group to monitor a track entry. When the state of the track entry transits to Negative, the weights of all VFs in the VRRP group on the router decrease by a specific value. When the state of the track entry transits to Positive or Notready, the original weights of the VFs restore.

#### Restrictions and guidelines

* By default, the weight of a VF is 255, and its lower limit of failure is 10.
* When the weight of a VF owner is higher than or equal to the lower limit of failure, its priority is always 255. The priority does not change with the weight. When the upstream link of the VF owner fails, an LVF must take over as the AVF. The switchover happens when the weight of the VF owner drops below the lower limit of failure. This requires that the reduced weight for the VF owner be higher than 245.

#### Procedure

Enter system view.

system-view

Enter interface view.

interface interface-type interface-number

Configure the VFs in a VRRP group to monitor a track entry.

vrrp ipv6 vrid virtual-router-id track track-entry-number { forwarder-switchover member-ip ipv6-address | priority reduced [ priority-reduced ] | switchover | weight reduced [ weight-reduced ] }

By default, no track entry is specified.

### Configuring IPv6 VRRP packet attributes

#### Restrictions and guidelines

* The routers in an IPv6 VRRP group can have different intervals for sending VRRP advertisements. The master in the VRRP group sends VRRP advertisements at the specified interval and carries the interval attribute in the advertisements. After a backup receives the advertisement, it records the interval in the advertisement. If the backup does not receive a VRRP advertisement before the timer (3 x recorded interval + Skew\_Time) expires, it regards the master as failed and takes over.
* A high volume of network traffic might cause a backup to fail to receive VRRP advertisements from the master within the specified time. As a result, an unexpected master switchover occurs. To solve this problem, configure a larger interval.

#### Procedure

Enter system view.

system-view

Enter interface view.

interface interface-type interface-number

Set the IPv6 VRRP advertisement interval.

vrrp ipv6 vrid virtual-router-id timer advertise adver-interval

The default setting is 100 centiseconds.

As a best practice to maintain system stability, set the VRRP advertisement interval to be greater than 100 centiseconds.

Return to system view.

quit

Set a DSCP value for IPv6 VRRP packets.

vrrp ipv6 dscp dscp-value

By default, the DSCP value for IPv6 VRRP packets is 56.

The DSCP value identifies the packet priority during transmission.

### Enabling periodic sending of ND packets for IPv6 VRRP

#### About periodic sending of ND packets for IPv6 VRRP

This feature enables the master router in an IPv6 VRRP group to periodically send ND packets. Then the downstream devices can update the MAC address entry for the virtual MAC address of the IPv6 VRRP group in a timely manner.

#### Restrictions and guidelines

* This feature takes effect only in VRRP standard mode.
* If you change the sending interval for ND packets, the configuration takes effect at the next sending interval.
* The master sends the first ND packet at a random time in the second half of the set interval after you execute the vrrp ipv6 send-nd command. This prevents too many ND packets from being sent at the same time.
* The sending interval for ND packets might be much longer than the set interval when the following conditions are met:
  + Multiple IPv6 VRRP groups exist on the device.
  + A short sending interval is set.

#### Procedure

Enter system view.

system-view

Enable periodic sending of ND packets for IPv6 VRRP.

vrrp ipv6 send-nd [ interval interval ]

By default, periodic sending of ND packets is disabled for IPv6 VRRP.

### Configuring a subordinate IPv6 VRRP group to follow a master IPv6 VRRP group

#### About master and subordinate IPv6 VRRP groups

Each IPv6 VRRP group determines the device role (master or backup) by exchanging VRRP packets among member devices, which might consume excessive bandwidth and CPU resources. To reduce the number of VRRP packets in the network, you can configure a subordinate IPv6 VRRP group to follow a master IPv6 VRRP group.

A master IPv6 VRRP group determines the device role through exchanging VRRP packets among member devices. An IPv6 VRRP group that follows a master group, called a subordinate VRRP group, does not exchange VRRP packets among its member devices. The state of the subordinate VRRP group follows the state of the master group.

#### Restrictions and guidelines

* To ensure the master router election, configure the settings such as the router priority, preemptive mode, and tracking function for the master IPv6 VRRP group. The settings are not required for subordinate IPv6 VRRP groups.
* You can configure a subordinate IPv6 VRRP group to follow a master IPv6 VRRP group in both VRRP standard and load balancing modes. The configuration takes effect only in VRRP standard mode.
* An IPv6 VRRP group cannot be both a master group and a subordinate group.
* An IPv6 VRRP group stays in Inactive state if it is configured to follow a nonexistent master IPv6 VRRP group.
* If an IPv6 VRRP group in Inactive or Initialize state follows a master group that is not in Inactive state, the state of the VRRP group does not change.
* A subordinate IPv6 VRRP group does not exchange VRRP packets, which might cause the MAC address entry for its virtual MAC address not to be updated on downstream devices. As a best practice, enable periodic sending of ND packets for IPv6 VRRP by using the vrrp ipv6 send-nd command.

#### Procedure

Enter system view.

system-view

Enter interface view.

interface interface-type interface-number

Configure an IPv6 VRRP group as a master group and assign a name to it.

vrrp ipv6 vrid virtual-router-id name name

By default, an IPv6 VRRP group does not act as a master group.

Return to system view.

quit

Enter interface view.

interface interface-type interface-number

Configure an IPv6 VRRP group to follow a master group.

vrrp ipv6 vrid virtual-router-id follow name

By default, an IPv6 VRRP group does not follow a master VRRP group.

### Display and maintenance commands for IPv6 VRRP

Execute display commands in any view and the reset command in user view.

| Task | Command |
| --- | --- |
| Display the states of IPv6 VRRP groups. | display vrrp ipv6 [ interface interface-type interface-number [ vrid virtual-router-id ] ] [ verbose ] |
| Display master-to-subordinate IPv6 VRRP group bindings. | display vrrp ipv6 binding [ interface interface-type interface-number [ vrid virtual-router-id ] | name name ] |
| Display statistics for IPv6 VRRP groups. | display vrrp ipv6 statistics [ interface interface-type interface-number [ vrid virtual-router-id ] ] |
| Clear statistics for IPv6 VRRP groups. | reset vrrp ipv6 statistics [ interface interface-type interface-number [ vrid virtual-router-id ] ] |

## IPv4 VRRP configuration examples

### Example: Configuring a single VRRP group

#### Network configuration

As shown in Figure 9, Switch A and Switch B form a VRRP group. They use the virtual IP address 10.1.1.111/24 to provide gateway service for the subnet where Host A resides.

Switch A operates as the master to forward packets from Host A to Host B. When Switch A fails, Switch B takes over to forward packets for Host A.

Network diagram



‌

#### Procedure

Configure Switch A:

# Configure VLAN 2.

<SwitchA> system-view

[SwitchA] vlan 2

[SwitchA-vlan2] port

[SwitchA-vlan2] quit

[SwitchA] interface vlan-interface 2

[SwitchA-Vlan-interface2] ip address 10.1.1.1 255.255.255.0

# Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to 10.1.1.111.

[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.111

# Assign Switch A a higher priority than Switch B in VRRP group 1, so Switch A can become the master.

[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110

# Configure Switch A to operate in preemptive mode, so it can become the master whenever it operates correctly. Set the preemption delay to 5000 centiseconds to avoid frequent status switchover.

[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000

Configure Switch B:

# Configure VLAN 2.

<SwitchB> system-view

[SwitchB] vlan 2

[SwitchB-Vlan2] port

[SwitchB-vlan2] quit

[SwitchB] interface vlan-interface 2

[SwitchB-Vlan-interface2] ip address 10.1.1.2 255.255.255.0

# Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to 10.1.1.111.

[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.111

# Set the priority of Router B to 100 in VRRP group 1.

[SwitchB-Vlan-interface2] vrrp vrid 1 priority 100

# Configure Switch B to operate in preemptive mode, and set the preemption delay to 5000 centiseconds.

[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000

#### Verifying the configuration

# Ping Host B from Host A. (Details not shown.)

# Display detailed information about VRRP group 1 on Switch A.

[SwitchA-Vlan-interface2] display vrrp verbose

IPv4 Virtual Router Information:

Running Mode : Standard

Total number of virtual routers : 1

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Master

Config Pri : 110 Running Pri : 110

Preempt Mode : Yes Delay Time : 5000

Auth Type : None

Virtual IP : 10.1.1.111

Virtual MAC : 0000-5e00-0101

Master IP : 10.1.1.1

# Display detailed information about VRRP group 1 on Switch B.

[SwitchB-Vlan-interface2] display vrrp verbose

IPv4 Virtual Router Information:

Running Mode : Standard

Total number of virtual routers : 1

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Backup

Config Pri : 100 Running Pri : 100

Preempt Mode : Yes Delay Time : 5000

Become Master : 401ms left

Auth Type : None

Virtual IP : 10.1.1.111

Master IP : 10.1.1.1

The output shows that Switch A is operating as the master in VRRP group 1 to forward packets from Host A to Host B.

# Disconnect the link between Host A and Switch A, and verify that Host A can still ping Host B. (Details not shown.)

# Display detailed information about VRRP group 1 on Switch B.

[SwitchB-Vlan-interface2] display vrrp verbose

IPv4 Virtual Router Information:

Running Mode : Standard

Total number of virtual routers : 1

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Master

Config Pri : 100 Running Pri : 100

Preempt Mode : Yes Delay Time : 5000

Auth Type : None

Virtual IP : 10.1.1.111

Virtual MAC : 0000-5e00-0101

Master IP : 10.1.1.2

The output shows that when Switch A fails, Switch B takes over to forward packets from Host A to Host B.

# Recover the link between Host A and Switch A, and display detailed information about VRRP group 1 on Switch A.

[SwitchA-Vlan-interface2] display vrrp verbose

IPv4 Virtual Router Information:

Running Mode : Standard

Total number of virtual routers : 1

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Master

Config Pri : 110 Running Pri : 110

Preempt Mode : Yes Delay Time : 5000

Auth Type : None

Virtual IP : 10.1.1.111

Virtual MAC : 0000-5e00-0101

Master IP : 10.1.1.1

The output shows that after Switch A resumes normal operation, it becomes the master to forward packets from Host A to Host B.

### Example: Configuring multiple VRRP groups

#### Network configuration

As shown in Figure 10, Switch A and Switch B form two VRRP groups. VRRP group 1 uses the virtual IP address 10.1.1.100/25 to provide gateway service for hosts in VLAN 2, and VRRP group 2 uses the virtual IP address 10.1.1.200/25 to provide gateway service for hosts in VLAN 3.

Assign a higher priority to Switch A than Switch B in VRRP group 1, but a lower priority in VRRP group 2. Traffic from VLAN 2 and VLAN 3 can then be distributed between the two switches. When one of the switches fails, the healthy switch provides gateway service for both VLANs.

Network diagram



‌

#### Procedure

Configure Switch A:

# Configure VLAN 2.

<SwitchA> system-view

[SwitchA] vlan 2

[SwitchA-vlan2] port

[SwitchA-vlan2] quit

[SwitchA] interface vlan-interface 2

[SwitchA-Vlan-interface2] ip address 10.1.1.1 255.255.255.128

# Create VRRP group 1, and set its virtual IP address to 10.1.1.100.

[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.100

# Assign Switch A a higher priority than Switch B in VRRP group 1, so Switch A can become the master in the group.

[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110

[SwitchA-Vlan-interface2] quit

# Configure VLAN 3.

[SwitchA] vlan 3

[SwitchA-vlan3] port

[SwitchA-vlan3] quit

[SwitchA] interface vlan-interface 3

[SwitchA-Vlan-interface3] ip address 10.1.1.130 255.255.255.128

# Create VRRP group 2, and set its virtual IP address to 10.1.1.200.

[SwitchA-Vlan-interface3] vrrp vrid 2 virtual-ip 10.1.1.200

Configure Switch B:

# Configure VLAN 2.

<SwitchB> system-view

[SwitchB] vlan 2

[SwitchB-vlan2] port

[SwitchB-vlan2] quit

[SwitchB] interface vlan-interface 2

[SwitchB-Vlan-interface2] ip address 10.1.1.2 255.255.255.128

# Create VRRP group 1, and set its virtual IP address to 10.1.1.100.

[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.100

[SwitchB-Vlan-interface2] quit

# Configure VLAN 3.

[SwitchB] vlan 3

[SwitchB-vlan3] port

[SwitchB-vlan3] quit

[SwitchB] interface vlan-interface 3

[SwitchB-Vlan-interface3] ip address 10.1.1.131 255.255.255.128

# Create VRRP group 2, and set its virtual IP address to 10.1.1.200.

[SwitchB-Vlan-interface3] vrrp vrid 2 virtual-ip 10.1.1.200

# Assign Switch B a higher priority than Switch A in VRRP group 2, so Switch B can become the master in the group.

[SwitchB-Vlan-interface3] vrrp vrid 2 priority 110

#### Verifying the configuration

# Display detailed information about the VRRP groups on Switch A.

[SwitchA-Vlan-interface3] display vrrp verbose

IPv4 Virtual Router Information:

Running Mode : Standard

Total number of virtual routers : 2

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Master

Config Pri : 110 Running Pri : 110

Preempt Mode : Yes Delay Time : 0

Auth Type : None

Virtual IP : 10.1.1.100

Virtual MAC : 0000-5e00-0101

Master IP : 10.1.1.1

Interface Vlan-interface3

VRID : 2 Adver Timer : 100

Admin Status : Up State : Backup

Config Pri : 100 Running Pri : 100

Preempt Mode : Yes Delay Time : 0

Become Master : 203ms left

Auth Type : None

Virtual IP : 10.1.1.200

Master IP : 10.1.1.131

# Display detailed information about the VRRP groups on Switch B.

[SwitchB-Vlan-interface3] display vrrp verbose

IPv4 Virtual Router Information:

Running Mode : Standard

Total number of virtual routers : 2

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Backup

Config Pri : 100 Running Pri : 100

Preempt Mode : Yes Delay Time : 0

Become Master : 211ms left

Auth Type : None

Virtual IP : 10.1.1.100

Master IP : 10.1.1.1

Interface Vlan-interface3

VRID : 2 Adver Timer : 100

Admin Status : Up State : Master

Config Pri : 110 Running Pri : 110

Preempt Mode : Yes Delay Time : 0

Auth Type : None

Virtual IP : 10.1.1.200

Virtual MAC : 0000-5e00-0102

Master IP : 10.1.1.131

The output shows the following information:

* Switch A is operating as the master in VRRP group 1 to forward Internet traffic for hosts that use the default gateway 10.1.1.100/25.
* Switch B is operating as the master in VRRP group 2 to forward Internet traffic for hosts that use the default gateway 10.1.1.200/25.

### Example: Configuring VRRP load balancing

#### Network configuration

As shown in Figure 11, Switch A, Switch B, and Switch C form a load-balanced VRRP group. They use the virtual IP address 10.1.1.1/24 to provide gateway service for subnet 10.1.1.0/24.

Configure VFs on Switch A, Switch B, and Switch C to monitor their respective VLAN-interface 3. When the interface on any one of them fails, the weights of the VFs on the problematic switch decrease so another AVF can take over.

Network diagram



‌

#### Procedure

Configure Switch A:

# Configure VLAN 2.

<SwitchA> system-view

[SwitchA] vlan 2

[SwitchA-vlan2] port

[SwitchA-vlan2] quit

# Configure VRRP to operate in load balancing mode.

[SwitchA] vrrp mode load-balance

# Create VRRP group 1, and set its virtual IP address to 10.1.1.1.

[SwitchA] interface vlan-interface 2

[SwitchA-Vlan-interface2] ip address 10.1.1.2 24

[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1

# Assign Switch A the highest priority in VRRP group 1, so Switch A can become the master.

[SwitchA-Vlan-interface2] vrrp vrid 1 priority 120

# Configure Switch A to operate in preemptive mode, so it can become the master whenever it operates correctly. Set the preemption delay to 5000 centiseconds to avoid frequent status switchover.

[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000

[SwitchA-Vlan-interface2] quit

# Create track entry 1 to monitor the upstream link status of VLAN-interface 3. When the upstream link fails, the track entry transits to Negative.

[SwitchA] track 1 interface vlan-interface 3

# Configure the VFs in VRRP group 1 to monitor track entry 1, and decrease their weights by 250 when the track entry transits to Negative.

[SwitchA] interface vlan-interface 2

[SwitchA-Vlan-interface2] vrrp vrid 1 track 1 weight reduced 250

Configure Switch B:

# Configure VLAN 2.

<SwitchB> system-view

[SwitchB] vlan 2

[SwitchB-vlan2] port

[SwitchB-vlan2] quit

# Configure VRRP to operate in load balancing mode.

[SwitchB] vrrp mode load-balance

# Create VRRP group 1, and set its virtual IP address to 10.1.1.1.

[SwitchB] interface vlan-interface 2

[SwitchB-Vlan-interface2] ip address 10.1.1.3 24

[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1

# Assign Switch B a higher priority than Switch C in VRRP group 1, so Switch B can become the master when Switch A fails.

[SwitchB-Vlan-interface2] vrrp vrid 1 priority 110

# Configure Switch B to operate in preemptive mode, and set the preemption delay to 5000 centiseconds.

[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000

[SwitchB-Vlan-interface2] quit

# Create track entry 1 to monitor the upstream link status of VLAN-interface 3. When the upstream link fails, the track entry transits to Negative.

[SwitchB] track 1 interface vlan-interface 3

# Configure the VFs in VRRP group 1 to monitor track entry 1, and decrease their weights by 250 when the track entry transits to Negative.

[SwitchB] interface vlan-interface 2

[SwitchB-Vlan-interface2] vrrp vrid 1 track 1 weight reduced 250

Configure Switch C:

# Configure VLAN 2.

<SwitchC> system-view

[SwitchC] vlan 2

[SwitchC-vlan2] port

[SwitchC-vlan2] quit

# Configure VRRP to operate in load balancing mode.

[SwitchC] vrrp mode load-balance

# Create VRRP group 1, and set its virtual IP address to 10.1.1.1.

[SwitchC] interface vlan-interface 2

[SwitchC-Vlan-interface2] ip address 10.1.1.4 24

[SwitchC-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1

# Configure Switch C to operate in preemptive mode, and set the preemption delay to 5000 centiseconds.

[SwitchC-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000

[SwitchC-Vlan-interface2] quit

# Create track entry 1 to monitor the upstream link status of VLAN-interface 3. When the upstream link fails, the track entry transits to Negative.

[SwitchC] track 1 interface vlan-interface 3

# Configure the VFs in VRRP group 1 to monitor track entry 1, and decrease their weights by 250 when the track entry transits to Negative.

[SwitchC] interface vlan-interface 2

[SwitchC-Vlan-interface2] vrrp vrid 1 track 1 weight reduced 250

#### Verifying the configuration

# Verify that Host A can ping the external network. (Details not shown.)

# Display detailed information about VRRP group 1 on Switch A.

[SwitchA-Vlan-interface2] display vrrp verbose

IPv4 Virtual Router Information:

Running Mode : Load Balance

Total number of virtual routers : 1

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Master

Config Pri : 120 Running Pri : 120

Preempt Mode : Yes Delay Time : 5000

Auth Type : None

Virtual IP : 10.1.1.1

Member IP List : 10.1.1.2 (Local, Master)

10.1.1.3 (Backup)

10.1.1.4 (Backup)

Forwarder Information: 3 Forwarders 1 Active

Config Weight : 255

Running Weight : 255

Forwarder 01

State : Active

Virtual MAC : 000f-e2ff-0011 (Owner)

Owner ID : 0000-5e01-1101

Priority : 255

Active : local

Forwarder 02

State : Listening

Virtual MAC : 000f-e2ff-0012 (Learnt)

Owner ID : 0000-5e01-1103

Priority : 127

Active : 10.1.1.3

Forwarder 03

State : Listening

Virtual MAC : 000f-e2ff-0013 (Learnt)

Owner ID : 0000-5e01-1105

Priority : 127

Active : 10.1.1.4

Forwarder Weight Track Information:

Track Object : 1 State : Positive Weight Reduced : 250

# Display detailed information about VRRP group 1 on Switch B.

[SwitchB-Vlan-interface2] display vrrp verbose

IPv4 Virtual Router Information:

Running Mode : Load Balance

Total number of virtual routers : 1

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Backup

Config Pri : 110 Running Pri : 110

Preempt Mode : Yes Delay Time : 5000

Become Master : 410ms left

Auth Type : None

Virtual IP : 10.1.1.1

Member IP List : 10.1.1.3 (Local, Backup)

10.1.1.2 (Master)

10.1.1.4 (Backup)

Forwarder Information: 3 Forwarders 1 Active

Config Weight : 255

Running Weight : 255

Forwarder 01

State : Listening

Virtual MAC : 000f-e2ff-0011 (Learnt)

Owner ID : 0000-5e01-1101

Priority : 127

Active : 10.1.1.2

Forwarder 02

State : Active

Virtual MAC : 000f-e2ff-0012 (Owner)

Owner ID : 0000-5e01-1103

Priority : 255

Active : local

Forwarder 03

State : Listening

Virtual MAC : 000f-e2ff-0013 (Learnt)

Owner ID : 0000-5e01-1105

Priority : 127

Active : 10.1.1.4

Forwarder Weight Track Information:

Track Object : 1 State : Positive Weight Reduced : 250

# Display detailed information about VRRP group 1 on Switch C.

[SwitchC-Vlan-interface2] display vrrp verbose

IPv4 Virtual Router Information:

Running Mode : Load Balance

Total number of virtual routers : 1

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Backup

Config Pri : 100 Running Pri : 100

Preempt Mode : Yes Delay Time : 5000

Become Master : 401ms left

Auth Type : None

Virtual IP : 10.1.1.1

Member IP List : 10.1.1.4 (Local, Backup)

10.1.1.2 (Master)

10.1.1.3 (Backup)

Forwarder Information: 3 Forwarders 1 Active

Config Weight : 255

Running Weight : 255

Forwarder 01

State : Listening

Virtual MAC : 000f-e2ff-0011 (Learnt)

Owner ID : 0000-5e01-1101

Priority : 127

Active : 10.1.1.2

Forwarder 02

State : Listening

Virtual MAC : 000f-e2ff-0012 (Learnt)

Owner ID : 0000-5e01-1103

Priority : 127

Active : 10.1.1.3

Forwarder 03

State : Active

Virtual MAC : 000f-e2ff-0013 (Owner)

Owner ID : 0000-5e01-1105

Priority : 255

Active : local

Forwarder Weight Track Information:

Track Object : 1 State : Positive Weight Reduced : 250

The output shows that Switch A is the master in VRRP group 1, and each of the three switches has one AVF and two LVFs.

# Disconnect the link of VLAN-interface 3 on Switch A, and display detailed information about VRRP group 1 on Switch A.

[SwitchA-Vlan-interface2] display vrrp verbose

IPv4 Virtual Router Information:

Running Mode : Load Balance

Total number of virtual routers : 1

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Master

Config Pri : 120 Running Pri : 120

Preempt Mode : Yes Delay Time : 5000

Auth Type : None

Virtual IP : 10.1.1.1

Member IP List : 10.1.1.2 (Local, Master)

10.1.1.3 (Backup)

10.1.1.4 (Backup)

Forwarder Information: 3 Forwarders 0 Active

Config Weight : 255

Running Weight : 5

Forwarder 01

State : Initialize

Virtual MAC : 000f-e2ff-0011 (Owner)

Owner ID : 0000-5e01-1101

Priority : 0

Active : 10.1.1.4

Forwarder 02

State : Initialize

Virtual MAC : 000f-e2ff-0012 (Learnt)

Owner ID : 0000-5e01-1103

Priority : 0

Active : 10.1.1.3

Forwarder 03

State : Initialize

Virtual MAC : 000f-e2ff-0013 (Learnt)

Owner ID : 0000-5e01-1105

Priority : 0

Active : 10.1.1.4

Forwarder Weight Track Information:

Track Object : 1 State : Negative Weight Reduced : 250

# Display detailed information about VRRP group 1 on Switch C.

[SwitchC-Vlan-interface2] display vrrp verbose

IPv4 Virtual Router Information:

Running Mode : Load Balance

Total number of virtual routers : 1

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Backup

Config Pri : 100 Running Pri : 100

Preempt Mode : Yes Delay Time : 5000

Become Master : 401ms left

Auth Type : None

Virtual IP : 10.1.1.1

Member IP List : 10.1.1.4 (Local, Backup)

10.1.1.2 (Master)

10.1.1.3 (Backup)

Forwarder Information: 3 Forwarders 2 Active

Config Weight : 255

Running Weight : 255

Forwarder 01

State : Active

Virtual MAC : 000f-e2ff-0011 (Take Over)

Owner ID : 0000-5e01-1101

Priority : 85

Active : local

Forwarder 02

State : Listening

Virtual MAC : 000f-e2ff-0012 (Learnt)

Owner ID : 0000-5e01-1103

Priority : 85

Active : 10.1.1.3

Forwarder 03

State : Active

Virtual MAC : 000f-e2ff-0013 (Owner)

Owner ID : 0000-5e01-1105

Priority : 255

Active : local

Forwarder Weight Track Information:

Track Object : 1 State : Positive Weight Reduced : 250

The output shows that when VLAN-interface 3 on Switch A fails, the weights of the VFs on Switch A drop below the lower limit of failure. All VFs on Switch A transit to the Initialized state and cannot forward traffic. The VF for MAC address 000f-e2ff-0011 on Switch C becomes the AVF to forward traffic.

# When the timeout timer (about 1800 seconds) expires, display detailed information about VRRP group 1 on Switch C.

[SwitchC-Vlan-interface2] display vrrp verbose

IPv4 Virtual Router Information:

Running Mode : Load Balance

Total number of virtual routers : 1

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Backup

Config Pri : 100 Running Pri : 100

Preempt Mode : Yes Delay Time : 5000

Become Master : 402ms left

Auth Type : None

Virtual IP : 10.1.1.1

Member IP List : 10.1.1.4 (Local, Backup)

10.1.1.2 (Master)

10.1.1.3 (Backup)

Forwarder Information: 2 Forwarders 1 Active

Config Weight : 255

Running Weight : 255

Forwarder 02

State : Listening

Virtual MAC : 000f-e2ff-0012 (Learnt)

Owner ID : 0000-5e01-1103

Priority : 127

Active : 10.1.1.3

Forwarder 03

State : Active

Virtual MAC : 000f-e2ff-0013 (Owner)

Owner ID : 0000-5e01-1105

Priority : 255

Active : local

Forwarder Weight Track Information:

Track Object : 1 State : Positive Weight Reduced : 250

The output shows that when the timeout timer expires, the VF for virtual MAC address 000f-e2ff-0011 is removed. The VF no longer forwards the packets destined for the MAC address.

# When Switch A fails, display detailed information about VRRP group 1 on Switch B.

[SwitchB-Vlan-interface2] display vrrp verbose

IPv4 Virtual Router Information:

Running Mode : Load Balance

Total number of virtual routers : 1

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Master

Config Pri : 110 Running Pri : 110

Preempt Mode : Yes Delay Time : 5000

Auth Type : None

Virtual IP : 10.1.1.1

Member IP List : 10.1.1.3 (Local, Master)

10.1.1.4 (Backup)

Forwarder Information: 2 Forwarders 1 Active

Config Weight : 255

Running Weight : 255

Forwarder 02

State : Active

Virtual MAC : 000f-e2ff-0012 (Owner)

Owner ID : 0000-5e01-1103

Priority : 255

Active : local

Forwarder 03

State : Listening

Virtual MAC : 000f-e2ff-0013 (Learnt)

Owner ID : 0000-5e01-1105

Priority : 127

Active : 10.1.1.4

Forwarder Weight Track Information:

Track Object : 1 State : Positive Weight Reduced : 250

The output shows the following information:

* When Switch A fails, Switch B becomes the master because it has a higher priority than Switch C.
* The VF for virtual MAC address 000f-e2ff-0011 is removed.

## IPv6 VRRP configuration examples

### Example: Configuring a single VRRP group

#### Network configuration

As shown in Figure 12, Switch A and Switch B form a VRRP group. They use the virtual IP addresses 1::10/64 and FE80::10 to provide gateway service for the subnet where Host A resides.

Host A learns 1::10/64 as its default gateway from RA messages sent by the switches.

Switch A operates as the master to forward packets from Host A to Host B. When Switch A fails, Switch B takes over to forward packets for Host A.

Network diagram



‌

#### Procedure

Configure Switch A:

# Configure VLAN 2.

<SwitchA> system-view

[SwitchA] vlan 2

[SwitchA-vlan2] port

[SwitchA-vlan2] quit

[SwitchA] interface vlan-interface 2

[SwitchA-Vlan-interface2] ipv6 address fe80::1 link-local

[SwitchA-Vlan-interface2] ipv6 address 1::1 64

# Create VRRP group 1, and set its virtual IPv6 addresses to FE80::10 and 1::10.

[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local

[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10

# Assign Switch A a higher priority than Switch B in VRRP group 1, so Switch A can become the master.

[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 priority 110

# Configure Switch A to operate in preemptive mode, so it can become the master whenever it operates correctly. Set the preemption delay to 5000 centiseconds to avoid frequent status switchover.

[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 5000

# Enable Switch A to send RA messages, so Host A can learn the default gateway address.

[SwitchA-Vlan-interface2] undo ipv6 nd ra halt

Configure Switch B:

# Configure VLAN 2.

<SwitchB> system-view

[SwitchB] vlan 2

[SwitchB-vlan2] port

[SwitchB-vlan2] quit

[SwitchB] interface vlan-interface 2

[SwitchB-Vlan-interface2] ipv6 address fe80::2 link-local

[SwitchB-Vlan-interface2] ipv6 address 1::2 64

# Create VRRP group 1 and set its virtual IPv6 addresses to FE80::10 and 1::10.

[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local

[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10

# Configure Switch B to operate in preemptive mode, and set the preemption delay to 5000 centiseconds.

[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 5000

# Enable Switch B to send RA messages, so Host A can learn the default gateway address.

[SwitchB-Vlan-interface2] undo ipv6 nd ra halt

#### Verifying the configuration

# Ping Host B from Host A. (Details not shown.)

# Display detailed information about VRRP group 1 on Switch A.

[SwitchA-Vlan-interface2] display vrrp ipv6 verbose

IPv6 Virtual Router Information:

Running Mode : Standard

Total number of virtual routers : 1

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Master

Config Pri : 110 Running Pri : 110

Preempt Mode : Yes Delay Time : 5000

Auth Type : None

Virtual IP : FE80::10

1::10

Virtual MAC : 0000-5e00-0201

Master IP : FE80::1

# Display detailed information about VRRP group 1 on Switch B.

[SwitchB-Vlan-interface2] display vrrp ipv6 verbose

IPv6 Virtual Router Information:

Running Mode : Standard

Total number of virtual routers : 1

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Backup

Config Pri : 100 Running Pri : 100

Preempt Mode : Yes Delay Time : 5000

Become Master : 403ms left

Auth Type : None

Virtual IP : FE80::10

1::10

Master IP : FE80::1

The output shows that Switch A is operating as the master in VRRP group 1 to forward packets from Host A to Host B.

# Disconnect the link between Host A and Switch A, and verify that Host A can still ping Host B. (Details not shown.)

# Display detailed information about VRRP group 1 on Switch B.

[SwitchB-Vlan-interface2] display vrrp ipv6 verbose

IPv6 Virtual Router Information:

Running Mode : Standard

Total number of virtual routers : 1

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Master

Config Pri : 100 Running Pri : 100

Preempt Mode : Yes Delay Time : 5000

Auth Type : None

Virtual IP : FE80::10

1::10

Virtual MAC : 0000-5e00-0201

Master IP : FE80::2

The output shows that when Switch A fails, Switch B takes over to forward packets from Host A to Host B.

# Recover the link between Host A and Switch A, and display detailed information about VRRP group 1 on Switch A.

[SwitchA-Vlan-interface2] display vrrp ipv6 verbose

IPv6 Virtual Router Information:

Running Mode : Standard

Total number of virtual routers : 1

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Master

Config Pri : 110 Running Pri : 110

Preempt Mode : Yes Delay Time : 5000

Auth Type : None

Virtual IP : FE80::10

1::10

Virtual MAC : 0000-5e00-0201

Master IP : FE80::1

The output shows that after Switch A resumes normal operation, it becomes the master to forward packets from Host A to Host B.

### Example: Configuring multiple VRRP groups

#### Network configuration

As shown in Figure 13, Switch A and Switch B form two VRRP groups. VRRP group 1 uses the virtual IPv6 addresses 1::10/64 and FE80::10 to provide gateway service for hosts in VLAN 2. VRRP group 2 uses the virtual IPv6 addresses 2::10/64 and FE90::10 to provide gateway service for hosts in VLAN 3.

From RA messages sent by the switches, hosts in VLAN 2 learn 1::10/64 as their default gateway. Hosts in VLAN 3 learn 2::10/64 as their default gateway.

Assign Switch A a higher priority than Switch B in VRRP group 1 but a lower priority in VRRP group 2. Traffic from VLAN 2 and VLAN 3 can then be distributed between the two switches. When one of the switches fails, the healthy switch provides gateway service for both VLANs.

Network diagram



‌

#### Procedure

Configure Switch A:

# Configure VLAN 2.

<SwitchA> system-view

[SwitchA] vlan 2

[SwitchA-vlan2] port

[SwitchA-vlan2] quit

[SwitchA] interface vlan-interface 2

[SwitchA-Vlan-interface2] ipv6 address fe80::1 link-local

[SwitchA-Vlan-interface2] ipv6 address 1::1 64

# Create VRRP group 1, and set its virtual IPv6 addresses to FE80::10 to 1::10.

[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local

[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10

# Assign Switch A a higher priority than Switch B in VRRP group 1, so Switch A can become the master in the group.

[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 priority 110

# Enable Switch A to send RA messages, so hosts in VLAN 2 can learn the default gateway address.

[SwitchA-Vlan-interface2] undo ipv6 nd ra halt

[SwitchA-Vlan-interface2] quit

# Configure VLAN 3.

[SwitchA] vlan 3

[SwitchA-vlan3] port

[SwitchA-vlan3] quit

[SwitchA] interface vlan-interface 3

[SwitchA-Vlan-interface3] ipv6 address fe90::1 link-local

[SwitchA-Vlan-interface3] ipv6 address 2::1 64

# Create VRRP group 2, and set its virtual IPv6 addresses to FE90::10 and 2::10.

[SwitchA-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip fe90::10 link-local

[SwitchA-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip 2::10

# Enable Switch A to send RA messages, so hosts in VLAN 3 can learn the default gateway address.

[SwitchA-Vlan-interface3] undo ipv6 nd ra halt

Configure Switch B:

# Configure VLAN 2.

<SwitchB> system-view

[SwitchB-vlan2] port

[SwitchB-vlan2] quit

[SwitchB] interface vlan-interface 2

[SwitchB-Vlan-interface2] ipv6 address fe80::2 link-local

[SwitchB-Vlan-interface2] ipv6 address 1::2 64

# Create VRRP group 1, and set its virtual IPv6 addresses to FE80::10 and 1::10.

[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local

[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10

# Enable Switch B to send RA messages, so hosts in VLAN 2 can learn the default gateway address.

[SwitchB-Vlan-interface2] undo ipv6 nd ra halt

[SwitchB-Vlan-interface2] quit

# Configure VLAN 3.

[SwitchB] vlan 3

[SwitchB-vlan3] port

[SwitchB-vlan3] quit

[SwitchB] interface vlan-interface 3

[SwitchB-Vlan-interface3] ipv6 address fe90::2 link-local

[SwitchB-Vlan-interface3] ipv6 address 2::2 64

# Create VRRP group 2, and set its virtual IPv6 addresses to FE90::10 and 2::10.

[SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip fe90::10 link-local

[SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip 2::10

# Assign Switch B a higher priority than Switch A in VRRP group 2, so Switch B can become the master in the group.

[SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 priority 110

# Enable Switch B to send RA messages, so hosts in VLAN 3 can learn the default gateway address.

[SwitchB-Vlan-interface3] undo ipv6 nd ra halt

#### Verifying the configuration

# Display detailed information about the VRRP groups on Switch A.

[SwitchA-Vlan-interface3] display vrrp ipv6 verbose

IPv6 Virtual Router Information:

Running Mode : Standard

Total number of virtual routers : 2

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Master

Config Pri : 110 Running Pri : 110

Preempt Mode : Yes Delay Time : 0

Auth Type : None

Virtual IP : FE80::10

1::10

Virtual MAC : 0000-5e00-0201

Master IP : FE80::1

Interface Vlan-interface3

VRID : 2 Adver Timer : 100

Admin Status : Up State : Backup

Config Pri : 100 Running Pri : 100

Preempt Mode : Yes Delay Time : 0

Become Master : 402ms left

Auth Type : None

Virtual IP : FE90::10

2::10

Master IP : FE90::2

# Display detailed information about the VRRP groups on Switch B.

[SwitchB-Vlan-interface3] display vrrp ipv6 verbose

IPv6 Virtual Router Information:

Running Mode : Standard

Total number of virtual routers : 2

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Backup

Config Pri : 100 Running Pri : 100

Preempt Mode : Yes Delay Time : 0

Become Master : 401ms left

Auth Type : None

Virtual IP : FE80::10

1::10

Master IP : FE80::1

Interface Vlan-interface3

VRID : 2 Adver Timer : 100

Admin Status : Up State : Master

Config Pri : 110 Running Pri : 110

Preempt Mode : Yes Delay Time : 0

Auth Type : None

Virtual IP : FE90::10

2::10

Virtual MAC : 0000-5e00-0202

Master IP : FE90::2

The output shows the following information:

* Switch A is operating as the master in VRRP group 1 to forward Internet traffic for hosts that use the default gateway 1::10/64.
* Switch B is operating as the master in VRRP group 2 to forward Internet traffic for hosts that use the default gateway 2::10/64.

### Example: Configuring VRRP load balancing

#### Network configuration

As shown in Figure 14, Switch A, Switch B, and Switch C form a load balanced VRRP group. They use the virtual IPv6 addresses FE80::10 and 1::10 to provide gateway service for subnet 1::/64.

Hosts on subnet 1::/64 learn 1::10 as their default gateway from RA messages sent by the switches.

Configure VFs on Switch A, Switch B, or Switch C to monitor their respective VLAN-interface 3. When the interface on any of them fails, the weights of the VFs on the problematic switch decrease so another AVF can take over.

Network diagram



‌

#### Procedure

Configure Switch A:

# Configure VLAN 2.

<SwitchA> system-view

[SwitchA] vlan 2

[SwitchA-vlan2] port

[SwitchA-vlan2] quit

# Configure VRRP to operate in load balancing mode.

[SwitchA] vrrp ipv6 mode load-balance

# Create VRRP group 1, and set its virtual IPv6 addresses to FE80::10 and 1::10.

[SwitchA] interface vlan-interface 2

[SwitchA-Vlan-interface2] ipv6 address fe80::1 link-local

[SwitchA-Vlan-interface2] ipv6 address 1::1 64

[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local

[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10

# Assign Switch A the highest priority in VRRP group 1, so Switch A can become the master.

[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 priority 120

# Configure Switch A to operate in preemptive mode, so it can become the master whenever it operates correctly. Set the preemption delay to 5000 centiseconds to avoid frequent status switchover.

[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 5000

# Enable Switch A to send RA messages, so hosts on subnet 1::/64 can learn the default gateway address.

[SwitchA-Vlan-interface2] undo ipv6 nd ra halt

[SwitchA-Vlan-interface2] quit

# Create track entry 1 to monitor the upstream link status of VLAN-interface 3. When the upstream link fails, the track entry transits to Negative.

[SwitchA] track 1 interface vlan-interface 3

# Configure the VFs in VRRP group 1 to monitor track entry 1, and decrease their weights by 250 when the track entry transits to Negative.

[SwitchA] interface vlan-interface 2

[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 track 1 weight reduced 250

Configure Switch B:

# Configure VLAN 2.

<SwitchB> system-view

[SwitchB] vlan 2

[SwitchB-vlan2] port

[SwitchB-vlan2] quit

# Configure VRRP to operate in load balancing mode.

[SwitchB] vrrp ipv6 mode load-balance

# Create VRRP group 1, and set its virtual IPv6 addresses to FE80::10 and 1::10.

[SwitchB] interface vlan-interface 2

[SwitchB-Vlan-interface2] ipv6 address fe80::2 link-local

[SwitchB-Vlan-interface2] ipv6 address 1::2 64

[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local

[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10

# Assign Switch B a higher priority than Switch C in VRRP group 1, so Switch B can become the master when Switch A fails.

[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 priority 110

# Configure Switch B to operate in preemptive mode, and set the preemption delay to 5000 centiseconds.

[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 5000

# Enable Switch B to send RA messages so hosts on subnet 1::/64 can learn the default gateway address.

[SwitchB-Vlan-interface2] undo ipv6 nd ra halt

[SwitchB-Vlan-interface2] quit

# Create track entry 1 to monitor the upstream link status of VLAN-interface 3. When the upstream link fails, the track entry transits to Negative.

[SwitchB] track 1 interface vlan-interface 3

# Configure the VFs in VRRP group 1 to monitor track entry 1, and decrease their weights by 250 when the track entry transits to Negative.

[SwitchB] interface vlan-interface 2

[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 track 1 weight reduced 250

Configure Switch C:

# Configure VLAN 2.

<SwitchC> system-view

[SwitchC] vlan 2

[SwitchC-vlan2] port

[SwitchC-vlan2] quit

# Configure VRRP to operate in load balancing mode.

[SwitchC] vrrp ipv6 mode load-balance

# Create VRRP group 1, and set its virtual IPv6 addresses to FE80::10 and 1::10.

[SwitchC] interface vlan-interface 2

[SwitchC-Vlan-interface2] ipv6 address fe80::3 link-local

[SwitchC-Vlan-interface2] ipv6 address 1::3 64

[SwitchC-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local

[SwitchC-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10

# Configure Switch C to operate in preemptive mode, and set the preemption delay to 5000 centiseconds.

[SwitchC-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 5000

# Enable Switch C to send RA messages, so the hosts on the subnet 1::/64 can learn the default gateway address.

[SwitchC-Vlan-interface2] undo ipv6 nd ra halt

[SwitchC-Vlan-interface2] quit

# Create track entry 1 to monitor the upstream link status of VLAN-interface 3. When the upstream link fails, the track entry transits to Negative.

[SwitchC] track 1 interface vlan-interface 3

# Configure the VFs in VRRP group 1 to monitor track entry 1, and decrease their weights by 250 when the track entry transits to Negative.

[SwitchC] interface vlan-interface 2

[SwitchC-Vlan-interface2] vrrp ipv6 vrid 1 track 1 weight reduced 250

#### Verifying the configuration

# Verify that Host A can ping the external network. (Details not shown.)

# Display detailed information about VRRP group 1 on Switch A.

[SwitchA-Vlan-interface2] display vrrp ipv6 verbose

IPv6 Virtual Router Information:

Running Mode : Load Balance

Total number of virtual routers : 1

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Master

Config Pri : 120 Running Pri : 120

Preempt Mode : Yes Delay Time : 5000

Auth Type : None

Virtual IP : FE80::10

1::10

Member IP List : FE80::1 (Local, Master)

FE80::2 (Backup)

FE80::3 (Backup)

Forwarder Information: 3 Forwarders 1 Active

Config Weight : 255

Running Weight : 255

Forwarder 01

State : Active

Virtual MAC : 000f-e2ff-4011 (Owner)

Owner ID : 0000-5e01-1101

Priority : 255

Active : local

Forwarder 02

State : Listening

Virtual MAC : 000f-e2ff-4012 (Learnt)

Owner ID : 0000-5e01-1103

Priority : 127

Active : FE80::2

Forwarder 03

State : Listening

Virtual MAC : 000f-e2ff-4013 (Learnt)

Owner ID : 0000-5e01-1105

Priority : 127

Active : FE80::3

Forwarder Weight Track Information:

Track Object : 1 State : Positive Weight Reduced : 250

# Display detailed information about VRRP group 1 on Switch B.

[SwitchB-Vlan-interface2] display vrrp ipv6 verbose

IPv6 Virtual Router Information:

Running Mode : Load Balance

Total number of virtual routers : 1

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Backup

Config Pri : 110 Running Pri : 110

Preempt Mode : Yes Delay Time : 5000

Become Master : 401ms left

Auth Type : None

Virtual IP : FE80::10

1::10

Member IP List : FE80::2 (Local, Backup)

FE80::1 (Master)

FE80::3 (Backup)

Forwarder Information: 3 Forwarders 1 Active

Config Weight : 255

Running Weight : 255

Forwarder 01

State : Listening

Virtual MAC : 000f-e2ff-4011 (Learnt)

Owner ID : 0000-5e01-1101

Priority : 127

Active : FE80::1

Forwarder 02

State : Active

Virtual MAC : 000f-e2ff-4012 (Owner)

Owner ID : 0000-5e01-1103

Priority : 255

Active : local

Forwarder 03

State : Listening

Virtual MAC : 000f-e2ff-4013 (Learnt)

Owner ID : 0000-5e01-1105

Priority : 127

Active : FE80::3

Forwarder Weight Track Information:

Track Object : 1 State : Positive Weight Reduced : 250

# Display detailed information about VRRP group 1 on Switch C.

[SwitchC-Vlan-interface2] display vrrp ipv6 verbose

IPv6 Virtual Router Information:

Running Mode : Load Balance

Total number of virtual routers : 1

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Backup

Config Pri : 100 Running Pri : 100

Preempt Mode : Yes Delay Time : 5000

Become Master : 402ms left

Auth Type : None

Virtual IP : FE80::10

1::10

Member IP List : FE80::3 (Local, Backup)

FE80::1 (Master)

FE80::2 (Backup)

Forwarder Information: 3 Forwarders 1 Active

Config Weight : 255

Running Weight : 255

Forwarder 01

State : Listening

Virtual MAC : 000f-e2ff-4011 (Learnt)

Owner ID : 0000-5e01-1101

Priority : 127

Active : FE80::1

Forwarder 02

State : Listening

Virtual MAC : 000f-e2ff-4012 (Learnt)

Owner ID : 0000-5e01-1103

Priority : 127

Active : FE80::2

Forwarder 03

State : Active

Virtual MAC : 000f-e2ff-4013 (Owner)

Owner ID : 0000-5e01-1105

Priority : 255

Active : local

Forwarder Weight Track Information:

Track Object : 1 State : Positive Weight Reduced : 250

The output shows that Switch A is the master in VRRP group 1, and each of the three switches has one AVF and two LVFs.

# Disconnect the link of VLAN-interface 3 on Switch A and display detailed information about VRRP group 1 on Switch A.

[SwitchA-Vlan-interface2] display vrrp ipv6 verbose

IPv6 Virtual Router Information:

Running Mode : Load Balance

Total number of virtual routers : 1

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Master

Config Pri : 120 Running Pri : 120

Preempt Mode : Yes Delay Time : 5000

Auth Type : None

Virtual IP : FE80::10

1::10

Member IP List : FE80::1 (Local, Master)

FE80::2 (Backup)

FE80::3 (Backup)

Forwarder Information: 3 Forwarders 0 Active

Config Weight : 255

Running Weight : 5

Forwarder 01

State : Initialize

Virtual MAC : 000f-e2ff-4011 (Owner)

Owner ID : 0000-5e01-1101

Priority : 0

Active : FE80::3

Forwarder 02

State : Initialize

Virtual MAC : 000f-e2ff-4012 (Learnt)

Owner ID : 0000-5e01-1103

Priority : 0

Active : FE80::2

Forwarder 03

State : Initialize

Virtual MAC : 000f-e2ff-4013 (Learnt)

Owner ID : 0000-5e01-1105

Priority : 0

Active : FE80::3

Forwarder Weight Track Information:

Track Object : 1 State : Negative Weight Reduced : 250

# Display detailed information about VRRP group 1 on Switch C.

[SwitchC-Vlan-interface2] display vrrp ipv6 verbose

IPv6 Virtual Router Information:

Running Mode : Load Balance

Total number of virtual routers : 1

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Backup

Config Pri : 100 Running Pri : 100

Preempt Mode : Yes Delay Time : 5000

Become Master : 410ms left

Auth Type : None

Virtual IP : FE80::10

1::10

Member IP List : FE80::3 (Local, Backup)

FE80::1 (Master)

FE80::2 (Backup)

Forwarder Information: 3 Forwarders 2 Active

Config Weight : 255

Running Weight : 255

Forwarder 01

State : Active

Virtual MAC : 000f-e2ff-4011 (Take Over)

Owner ID : 0000-5e01-1101

Priority : 85

Active : local

Forwarder 02

State : Listening

Virtual MAC : 000f-e2ff-4012 (Learnt)

Owner ID : 0000-5e01-1103

Priority : 85

Active : FE80::2

Forwarder 03

State : Active

Virtual MAC : 000f-e2ff-4013 (Owner)

Owner ID : 0000-5e01-1105

Priority : 255

Active : local

Forwarder Weight Track Information:

Track Object : 1 State : Positive Weight Reduced : 250

The output shows that when VLAN-interface 3 on Switch A fails, the weights of the VFs on Switch A drop below the lower limit of failure. All VFs on Switch A transit to the Initialized state and cannot forward traffic. The VF for MAC address 000f-e2ff-4011 on Switch C becomes the AVF to forward traffic.

# When the timeout timer (about 1800 seconds) expires, display detailed information about VRRP group 1 on Switch C.

[SwitchC-Vlan-interface2] display vrrp ipv6 verbose

IPv6 Virtual Router Information:

Running Mode : Load Balance

Total number of virtual routers : 1

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Backup

Config Pri : 100 Running Pri : 100

Preempt Mode : Yes Delay Time : 5000

Become Master : 400ms left

Auth Type : None

Virtual IP : FE80::10

1::10

Member IP List : FE80::3 (Local, Backup)

FE80::1 (Master)

FE80::2 (Backup)

Forwarder Information: 2 Forwarders 1 Active

Config Weight : 255

Running Weight : 255

Forwarder 02

State : Listening

Virtual MAC : 000f-e2ff-4012 (Learnt)

Owner ID : 0000-5e01-1103

Priority : 127

Active : FE80::2

Forwarder 03

State : Active

Virtual MAC : 000f-e2ff-4013 (Owner)

Owner ID : 0000-5e01-1105

Priority : 255

Active : local

Forwarder Weight Track Information:

Track Object : 1 State : Positive Weight Reduced : 250

The output shows that when the timeout timer expires, the VF for virtual MAC address 000f-e2ff-4011 is removed. The VF no longer forwards the packets destined for the MAC address.

# When Switch A fails, display detailed information about VRRP group 1 on Switch B.

[SwitchB-Vlan-interface2] display vrrp ipv6 verbose

IPv6 Virtual Router Information:

Running Mode : Load Balance

Total number of virtual routers : 1

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Master

Config Pri : 110 Running Pri : 110

Preempt Mode : Yes Delay Time : 5000

Auth Type : None

Virtual IP : FE80::10

1::10

Member IP List : FE80::2 (Local, Master)

FE80::3 (Backup)

Forwarder Information: 2 Forwarders 1 Active

Config Weight : 255

Running Weight : 255

Forwarder 02

State : Active

Virtual MAC : 000f-e2ff-4012 (Owner)

Owner ID : 0000-5e01-1103

Priority : 255

Active : local

Forwarder 03

State : Listening

Virtual MAC : 000f-e2ff-4013 (Learnt)

Owner ID : 0000-5e01-1105

Priority : 127

Active : FE80::3

Forwarder Weight Track Information:

Track Object : 1 State : Positive Weight Reduced : 250

The output shows the following information:

* When Switch A fails, Switch B becomes the master because it has a higher priority than Switch C.
* The VF for virtual MAC address 000f-e2ff-4011 is removed.

## Troubleshooting VRRP

### An error prompt is displayed

#### Symptom

An error prompt "The virtual router detected a VRRP configuration error." is displayed during configuration.

#### Analysis

This symptom is probably caused by the following reasons:

* The VRRP advertisement interval in the packet is not the same as that for the current VRRP group (in VRRPv2 only).
* The number of virtual IP addresses in the packet is not the same as that for the current VRRP group.
* The virtual IP address list is not the same as that for the current VRRP group.
* A device in the VRRP group receives illegitimate VRRP packets. For example, the IP address owner receives a VRRP packet with the priority 255.

#### Solution

To resolve the problem:

Modify the configuration on routers in VRRP groups to ensure consistent configuration.

Take fault location and anti-attack measures to eliminate potential threats.

If the problem persists, contact Hewlett Packard Enterprise Support.

### Multiple masters appear in a VRRP group

#### Symptom

Multiple masters appear in a VRRP group.

#### Analysis

It is normal for a VRRP group to have multiple masters for a short time, and this situation requires no manual intervention.

If multiple masters coexist for a longer period, check for the following conditions:

* The masters cannot receive advertisements from each other.
* The received advertisements are illegitimate.

#### Solution

To resolve the problem:

Ping between these masters:

* + If the ping operation fails, examine network connectivity.
  + If the ping operation succeeds, check for configuration inconsistencies in the number of virtual IP addresses, virtual IP addresses, and authentication. For IPv4 VRRP, also make sure the same version of VRRP is configured on all routers in the VRRP group. For VRRPv2, make sure the same VRRP advertisement interval is configured on the routers in the VRRP group.

If the problem persists, contact Hewlett Packard Enterprise Support.

### Fast VRRP state flapping

#### Symptom

Fast VRRP state flapping occurs.

#### Analysis

The VRRP advertisement interval is set too short.

#### Solution

To resolve the problem:

Increase the interval for sending VRRP advertisements or introduce a preemption delay.

If the problem persists, contact Hewlett Packard Enterprise Support.

## IPv4 VRRP commands

VRRP does not take effect on member ports of aggregation groups.

### display vrrp

Use display vrrp to display the states of IPv4 VRRP groups.

Syntax

display vrrp [ interface interface-type interface-number [ vrid virtual-router-id ] ] [ verbose ]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface interface-type interface-number: Specifies an interface by its type and number.

vrid virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

verbose: Displays detailed IPv4 VRRP group information. If you do not specify the verbose keyword, the command displays brief IPv4 VRRP group information.

Usage guidelines

If no interface or VRRP group is specified, this command displays the states of all IPv4 VRRP groups.

If only an interface is specified, this command displays the states of all IPv4 VRRP groups on the specified interface.

If both an interface and an IPv4 VRRP group are specified, this command displays the states of the specified IPv4 VRRP group on the specified interface.

Examples

# Display brief information about all IPv4 VRRP groups on the device when VRRP operates in standard mode.

<Sysname> display vrrp

IPv4 Virtual Router Information:

Running Mode : Standard

Gratuitous ARP sending interval : 120 sec

Total number of virtual routers : 1

Interface VRID State Running Adver Auth Virtual

Pri Timer Type IP

---------------------------------------------------------------------

Vlan2 1 Master 150 100 Simple 1.1.1.1

Command output (in standard mode)

| Field | Description |
| --- | --- |
| Running Mode | VRRP operating mode (standard mode). |
| Gratuitous ARP sending interval | Sending interval for gratuitous ARP packets. This field is displayed only after you configure the vrrp send-gratuitous-arp command. |
| Total number of virtual routers | Total number of VRRP groups. |
| Interface | Interface where the VRRP group is configured. |
| VRID | Virtual router ID (VRRP group number). |
| State | Status of the router in the VRRP group:   * + - * Master.       * Backup.       * Initialize.       * Inactive. |
| Running Pri | Current priority of the router.  When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes. |
| Adver Timer | VRRP advertisement sending interval in centiseconds. |
| Auth Type | Authentication type:   * + - * None—No authentication.       * Simple—Simple text authentication.       * MD5—MD5 authentication. |
| Virtual IP | Virtual IP address of the VRRP group. |

# Display detailed information about all IPv4 VRRP groups on the device when VRRP operates in standard mode.

<Sysname> display vrrp verbose

IPv4 Virtual Router Information:

Running Mode : Standard

Gratuitous ARP sending interval : 120 sec

Total number of virtual routers : 2

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Master

Config Pri : 150 Running Pri : 150

Preempt Mode : Yes Delay Time : 5

Auth Type : Simple Key : \*\*\*\*\*\*

Virtual IP : 1.1.1.1

Virtual MAC : 0000-5e00-0101

Master IP : 1.1.1.2

Config Role : Master

Name : abc

VRRP Track Information:

Track Object : 1 State : Positive Pri Reduced : 50

Interface Vlan-interface2

VRID : 2 Adver Timer : 100

Admin Status : Up State : Backup

Config Pri : 80 Running Pri : 80

Preempt Mode : Yes Delay Time : 0

Become Master : 2370ms left

Auth Type : None

Virtual IP : 1.1.1.11

Virtual MAC : 0000-5e00-0102

Master IP : 1.1.1.12

Interface Vlan-interface2

VRID : 3 Adver Timer : 100

Admin Status : Up State : Master

Config Pri : 100 Running Pri : 100

Preempt Mode : Yes Delay Time : 0

Auth Type : None

Pkt Sending Mode : v2-only

Virtual IP : 1.1.1.10

Virtual MAC : 0000-5e00-0103

Master IP : 1.1.1.2

Config Role : Subordinate

Follow Name : abc

Command output (in standard mode)

| Field | Description |
| --- | --- |
| Running Mode | VRRP operating mode (standard mode). |
| Gratuitous ARP sending interval | Sending interval for gratuitous ARP packets. This field is displayed only after you configure the vrrp send-gratuitous-arp command. |
| Total number of virtual routers | Total number of VRRP groups. |
| Interface | Interface where the VRRP group is configured. |
| VRID | Virtual router ID (VRRP group number). |
| Adver Timer | VRRP advertisement sending interval in centiseconds. |
| Admin Status | Administrative status: Up or Down. |
| State | Status of the router in the VRRP group:   * + - * Master.       * Backup.       * Initialize.       * Inactive. |
| Config Pri | Configured priority of the router, which is configured by using the vrrp vrid priority command. |
| Running Pri | Current priority of the router.  When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes. |
| Preempt Mode | Preemptive mode:   * + - * Yes.       * No. |
| Delay Time | Preemption delay in centiseconds. |
| Become Master | Time (in milliseconds) that a backup router has to wait before it becomes the master. This field is displayed only when the router is a backup. |
| Auth Type | Authentication type:   * + - * None—No authentication.       * Simple—Simple text authentication.       * MD5—MD5 authentication. |
| Key | Authentication key, which is not displayed if no authentication is required. |
| Virtual IP | Virtual IP address of the VRRP group. |
| Virtual MAC | Virtual MAC address of the VRRP group's virtual IP address, which is displayed when the router is the master. |
| Master IP | Primary IP address of the interface where the master resides. |
| Config Role | The configured role of the VRRP group to which the router belongs.   * + - * Master.       * Subordinate. |
| Name | Master group name assigned to the VRRP group. This field is displayed only after you configure the vrrp vrid name command. |
| Follow Name | Name of the master VRRP group that the VRRP group follows. This field is displayed only after you configure the vrrp vrid follow command. |
| VRRP Track Information | Track entry information. This field is displayed only after you configure the vrrp vrid track command. |
| Track Object | Track entry which is associated with the VRRP group. |
| State | Track entry state:   * + - * Negative.       * Positive.       * NotReady. |
| Pri Reduced | Value by which the priority decreases when the status of the associated track entry changes to the Negative state. |
| Switchover | Switchover mode. When the status of the associated track entry changes to the Negative state, the backup immediately becomes the master. |

# Display brief information about all IPv4 VRRP groups on the device when VRRP operates in load balancing mode.

<Sysname> display vrrp

IPv4 Virtual Router Information:

Running Mode : Load Balance

Total number of virtual routers : 1

Interface VRID State Running Address Active

Pri

----------------------------------------------------------------------

Vlan2 1 Master 150 1.1.1.1 Local

----- VF 1 Active 255 000f-e2ff-0011 Local

Command output (in load balancing mode)

| Field | Description |
| --- | --- |
| Running Mode | VRRP operating mode (load balancing mode). |
| Total number of virtual routers | Total number of VRRP groups. |
| Interface | Interface where the VRRP group is configured. |
| VRID | Virtual router ID (VRRP group number) or virtual forwarder (VF) ID. |
| State | * + - * For a VRRP group, this field indicates the state of the router in the VRRP group, which is Master, Backup, Initialize, or Inactive.       * For a VF, this field indicates the state of the VF in the VRRP group, which is Active, Listening, or Initialize. |
| Running Pri | * + - * For a VRRP group, this field indicates the running priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes.       * For a VF, this field indicates the running priority of the VF. When a track entry is associated with a VF, the priority of the VF changes if the track entry's status changes. |
| Address | * + - * For a VRRP group, this field indicates the virtual IP address of the VRRP group.       * For a VF, this field indicates the virtual MAC address of the VF. |
| Active | * + - * For a VRRP group, this field indicates the IP address of the interface where the master resides. If the current router is the master, this field displays local.       * For a VF, this field indicates the IP address of the interface where the active virtual forwarder (AVF) resides. If the current VF is the AVF, this field displays local. |

# Display detailed information about all IPv4 VRRP groups on the device when VRRP operates in load balancing mode.

<Sysname> display vrrp verbose

IPv4 Virtual Router Information:

Running Mode : Load Balance

Total number of virtual routers : 2

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Master

Config Pri : 150 Running Pri : 150

Preempt Mode : Yes Delay Time : 5

Auth Type : None

Virtual IP : 10.1.1.1

10.1.1.2

10.1.1.3

Member IP List : 10.1.1.10 (Local, Master)

10.1.1.20 (Backup)

VRRP Track Information:

Track Object : 1 State : Positive Pri Reduced : 50

Forwarder Information: 2 Forwarders 1 Active

Config Weight : 255

Running Weight : 255

Forwarder 01

State : Active

Virtual MAC : 000f-e2ff-0011 (Owner)

Owner ID : 0000-5e01-1101

Priority : 255

Active : local

Forwarder 02

State : Listening

Virtual MAC : 000f-e2ff-0012 (Learnt)

Owner ID : 0000-5e01-1103

Priority : 127

Active : 10.1.1.20

Forwarder Weight Track Information:

Track Object : 1 State : Positive Weight Reduced : 250

Interface Vlan-interface2

VRID : 11 Adver Timer : 100

Admin Status : Up State : Backup

Config Pri : 80 Running Pri : 80

Preempt Mode : Yes Delay Time : 0

Become Master : 2370ms left

Auth Type : None

Virtual IP : 10.1.1.11

: 10.1.1.12

: 10.1.1.13

Member IP List : 10.1.1.10 (Local, Backup)

10.1.1.15 (Master)

Forwarder Information: 2 Forwarders 1 Active

Config Weight : 255

Running Weight : 255

Forwarder 01

State : Active

Virtual MAC : 000f-e2ff-40b1 (Learnt)

Owner ID : 0000-5e01-1103

Priority : 127

Active : 10.1.1.15

Forwarder 02

State : Listening

Virtual MAC : 000f-e2ff-40b2 (Owner)

Owner ID : 0000-5e01-1101

Priority : 255

Active : local

Command output (in load balancing mode)

| Field | Description |
| --- | --- |
| Running Mode | VRRP operating mode (load balancing mode). |
| Total number of virtual routers | Total number of VRRP groups. |
| Interface | Interface where the VRRP group is configured. |
| VRID | Virtual router ID (VRRP group number). |
| Adver Timer | VRRP advertisement sending interval in centiseconds. |
| Admin Status | Administrative status: Up or Down. |
| State | Status of the router in the VRRP group:   * + - * Master.       * Backup.       * Initialize.       * Inactive. |
| Config Pri | Configured priority of the router, which is configured by using the vrrp vrid priority command. |
| Running Pri | Current priority of the router.  When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes. |
| Preempt Mode | Preemptive mode:   * + - * Yes.       * No. |
| Delay Time | Preemption delay in centiseconds. |
| Become Master | Time (in milliseconds) that a backup router has to wait before it becomes the master. This field is displayed only when the router is a backup. |
| Auth Type | Authentication type:   * + - * None—No authentication.       * Simple—Simple text authentication.       * MD5—MD5 authentication. |
| Key | Authentication key, which is not displayed if no authentication is required. |
| Virtual IP | Virtual IP address list of the VRRP group. |
| Member IP List | IP addresses of the member devices in the VRRP group:   * + - * Local—IP address of the local router.       * Master—IP address of the master.       * Backup—IP address of the backup. |
| VRRP Track Information | Track entry which is associated with the VRRP group. This field is displayed only after you configure the vrrp vrid track command. |
| Track Object | Track entry to be monitored. |
| State | Track entry state:   * + - * Negative.       * Positive.       * NotReady. |
| Pri Reduced | Value by which the priority decreases when the status of the associated track entry changes to the Negative state. This field is displayed only after you configure the vrrp vrid track command. |
| Switchover | Switchover mode. When the status of the associated track entry changes to the Negative state, the backup immediately becomes the master. |
| Forwarder Information: 2 Forwarders 1 Active | VF information: Two VFs exist, and one is the AVF. |
| Config Weight | Configured weight of the VF: 255. |
| Running Weight | Current weight of the VF.  When a track entry is associated with the VFs of a VRRP group, the VFs' weights change when the track entry's status changes. |
| Forwarder 01 | Information about VF 01. |
| State | VF state:   * + - * Active.       * Listening.       * Initialize. |
| Virtual MAC | Virtual MAC address of the VF. |
| Owner ID | Real MAC address of the VF owner. |
| Priority | VF priority in the range of 1 to 255. |
| Active | IP address of the interface where the AVF resides. If the current VF is the AVF, this field displays local. |
| Forwarder Weight Track Configuration | VF weight Track configuration.  The field is displayed only after you configure the vrrp vrid track command. |
| Track Object | Track entry that is associated with the VFs.  The field is displayed only after you configure the vrrp vrid track command. |
| State | Track entry state:   * + - * Negative.       * Positive.       * NotReady. |
| Weight Reduced | Value by which the weights of the VFs decrease when the state of the associated track entry changes to Negative.  The field is displayed only after you configure the vrrp vrid track command. |
| Forwarder Switchover Track Information: | VF switchover Track configuration.  The field is displayed only after you configure the vrrp vrid track command. |
| Member IP | IP address of a member device.  The field is displayed only after you configure the vrrp vrid track command. |

### display vrrp binding

Use display vrrp binding to display master-to-subordinate IPv4 VRRP group bindings.

Syntax

display vrrp binding [ interface interface-type interface-number [ vrid virtual-router-id ] | name name ]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface interface-type interface-number: Specifies an interface by its type and number. The interface must be an interface to which master IPv4 VRRP groups belong.

vrid virtual-router-id: Specifies a master IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

name name: Specifies a master IPv4 VRRP group by its name, a case-sensitive string of 1 to 20 characters.

Usage guidelines

If you do not specify any parameters, this command displays all master-to-subordinate IPv4 VRRP group bindings.

If you specify an interface but do not specify the virtual router ID of a master VRRP group, this command displays all master-to-subordinate VRRP group bindings on the specified interface.

If you specify an interface and the virtual router ID of a master VRRP group, this command displays the binding information about the specified master VRRP group on the specified interface.

Examples

# Display master-to-subordinate IPv4 VRRP group bindings.

<Sysname> display vrrp binding

IPv4 virtual router binding information:

Total number of master virtual routers : 1

Total number of subordinate virtual routers : 2

Interface : Vlan2 Master VRID : 1

Name : a Status : Backup

Subordinate virtual routers : 1

Interface : Vlan2 VRID : 4

Interface : -- Master VRID : --

Name : c Status : --

Subordinate virtual routers : 1

Interface : Vlan2 VRID : 5

Command output

|  |  |
| --- | --- |
| Field | Description |
| Total number of master virtual routers | Total number of master VRRP groups. |
| Total number of subordinate virtual routers | Total number of subordinate VRRP groups. |
| Interface | Interface to which the master VRRP group belongs. If the master VRRP group does not exist, this field displays two hyphens (--). |
| Master VRID | Virtual router ID of the master VRRP group. If the master VRRP group does not exist, this field displays two hyphens (--). |
| Name | Name of the master VRRP group. |
| Status | Status of the router in the master VRRP group:   * + - * Master.       * Backup.       * Initialize.       * Inactive.   If the master VRRP group does not exist, this field displays two hyphens (--). |
| Subordinate virtual routers | Number of subordinate VRRP groups. |
| Interface | Interface to which the subordinate VRRP group belongs. |
| VRID | Virtual router ID of the subordinate VRRP group. |

Related commands

vrrp vrid follow

vrrp vrid name

### display vrrp statistics

Use display vrrp statistics to display statistics for IPv4 VRRP groups.

Syntax

display vrrp statistics [ interface interface-type interface-number [ vrid virtual-router-id ] ]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface interface-type interface-number: Specifies an interface by its type and number.

vrid virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

Usage guidelines

If no interface or VRRP group is specified, this command displays statistics for all IPv4 VRRP groups.

If only an interface is specified, this command displays statistics for all IPv4 VRRP groups on the specified interface.

If both an interface and an IPv4 VRRP group are specified, this command displays statistics for the specified IPv4 VRRP group on the specified interface.

Examples

# Display statistics for all IPv4 VRRP groups when VRRP operates in standard mode.

<Sysname> display vrrp statistics

Interface : Vlan-interface2

VRID : 1

CheckSum Errors : 0 Version Errors : 0

Invalid Pkts Rcvd : 0 Unexpected Pkts Rcvd : 0

IP TTL Errors : 0 Advertisement Interval Errors : 0

Invalid Auth Type : 0 Auth Failures : 0

Packet Length Errors : 0 Auth Type Mismatch : 0

Become Master : 1 Address List Errors : 0

Adver Rcvd : 0 Priority Zero Pkts Rcvd : 0

Adver Sent : 807 Priority Zero Pkts Sent : 0

IP Owner Conflicts : 0

Global statistics

CheckSum Errors : 0

Version Errors : 0

VRID Errors : 0

# Display statistics for all IPv4 VRRP groups when VRRP operates in load balancing mode.

<Sysname> display vrrp statistics

Interface : Vlan-interface2

VRID : 1

CheckSum Errors : 0 Version Errors : 0

Invalid Pkts Rcvd : 0 Unexpected Pkts Rcvd : 0

IP TTL Errors : 0 Advertisement Interval Errors : 0

Invalid Auth Type : 0 Auth Failures : 0

Packet Length Errors : 0 Auth Type Mismatch : 0

Become Master : 39 Address List Errors : 0

Become AVF : 13 Packet Option Errors : 0

Adver Rcvd : 2562 Priority Zero Pkts Rcvd : 1

Adver Sent : 16373 Priority Zero Pkts Sent : 49

Request Rcvd : 2 Reply Rcvd : 10

Request Sent : 12 Reply Sent : 2

Release Rcvd : 0 VF Priority Zero Pkts Rcvd : 1

Release Sent : 0 VF Priority Zero Pkts Sent : 11

Redirect Timer Expires : 1 Time-out Timer Expires : 0

Global statistics

CheckSum Errors : 0

Version Errors : 0

VRID Errors : 0

Command output (in standard mode)

| Field | Description |
| --- | --- |
| Interface | Interface where the VRRP group is configured. |
| VRID | VRRP group number. |
| CheckSum Errors | Number of packets with checksum errors. |
| Version Errors | Number of packets with version errors. |
| Invalid Pkts Rcvd | Number of received packets of invalid packet types. |
| Unexpected Pkts Rcvd | Number of received unexpected packets. |
| Advertisement Interval Errors | Number of packets with advertisement interval errors. |
| IP TTL Errors | Number of packets with TTL errors. |
| Auth Failures | Number of packets with authentication failures. |
| Invalid Auth Type | Number of packets with authentication failures because of invalid authentication types. |
| Auth Type Mismatch | Number of packets with authentication failures because of mismatching authentication types. |
| Packet Length Errors | Number of packets with VRRP packet length errors. |
| Address List Errors | Number of packets with virtual IP address list errors. |
| Become Master | Number of times that the router has been elected as the master. |
| Priority Zero Pkts Rcvd | Number of received advertisements with the router priority of 0. |
| Adver Rcvd | Number of received advertisements. |
| Priority Zero Pkts Sent | Number of sent advertisements with the router priority of 0. |
| Adver Sent | Number of sent advertisements. |
| IP Owner Conflicts | Number of VRRP packets that the local router (IP address owner) has received from conflicting IP address owners. |
| Global statistics | Global statistics for all VRRP groups. |
| CheckSum Errors | Total number of packets with checksum errors. |
| Version Errors | Total number of packets with version errors. |
| VRID Errors | Total number of packets with VRID errors. |

Command output (in load balancing mode)

| Field | Description |
| --- | --- |
| Interface | Interface where the VRRP group is configured. |
| VRID | VRRP group number. |
| CheckSum Errors | Number of packets with checksum errors. |
| Version Errors | Number of packets with version errors. |
| Invalid Pkts Rcvd | Number of received packets of invalid packet types. |
| Unexpected Pkts Rcvd | Number of received unexpected packets. |
| Advertisement Interval Errors | Number of packets with advertisement interval errors. |
| IP TTL Errors | Number of packets with TTL errors. |
| Auth Failures | Number of packets with authentication failures. |
| Invalid Auth Type | Number of packets with authentication failures because of invalid authentication types. |
| Auth Type Mismatch | Number of packets with authentication failures because of mismatching authentication types. |
| Packet Length Errors | Number of packets with VRRP packet length errors. |
| Address List Errors | Number of packets with virtual IP address list errors. |
| Become Master | Number of times that the router has been elected as the master. |
| Redirect Timer Expires | Number of times that the redirect timer expired. |
| Become AVF | Number of times that the VF has been elected as the AVF. |
| Time-out Timer Expires | Number of times that the time-out timer expired. |
| Adver Rcvd | Number of received advertisements. |
| Request Rcvd | Number of received requests. |
| Adver Sent | Number of sent advertisements. |
| Request Sent | Number of sent requests. |
| Reply Rcvd | Number of received replies. |
| Release Rcvd | Number of received release packets. |
| Reply Sent | Number of sent replies. |
| Release Sent | Number of sent release packets. |
| Priority Zero Pkts Rcvd | Number of received advertisements with the router priority of 0. |
| VF Priority Zero Pkts Rcvd | Number of received advertisements with the VF priority of 0. |
| Priority Zero Pkts Sent | Number of sent advertisements with the router priority of 0. |
| VF Priority Zero Pkts Sent | Number of sent advertisements with the VF priority of 0. |
| Packet Option Errors | Number of packet option errors. |
| Global statistics | Global statistics for all IPv4 VRRP groups. |
| CheckSum Errors | Total number of packets with checksum errors. |
| Version Errors | Total number of packets with version errors. |
| VRID Errors | Total number of packets with VRID errors. |

Related commands

reset vrrp statistics

### reset vrrp statistics

Use reset vrrp statistics to clear statistics for IPv4 VRRP groups.

Syntax

reset vrrp statistics [ interface interface-type interface-number [ vrid virtual-router-id ] ]

Views

User view

Predefined user roles

network-admin

Parameters

interface interface-type interface-number: Specifies an interface by its type and number.

vrid virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

Usage guidelines

If no interface or VRRP group is specified, this command clears statistics for all IPv4 VRRP groups.

If only an interface is specified, this command clears statistics for all IPv4 VRRP groups on the specified interface.

If both an interface and an IPv4 VRRP group are specified, this command clears statistics for the specified IPv4 VRRP group on the specified interface.

Examples

# Clear statistics for all IPv4 VRRP groups on all interfaces.

<Sysname> reset vrrp statistics

Related commands

display vrrp statistics

### snmp-agent trap enable vrrp

Use snmp-agent trap enable vrrp to enable SNMP notifications for VRRP.

Use undo snmp-agent trap enable vrrp to disable SNMP notifications for VRRP.

Syntax

snmp-agent trap enable vrrp [ auth-failure | new-master ]

undo snmp-agent trap enable vrrp [ auth-failure | new-master ]

Default

SNMP notifications for VRRP are enabled.

Views

System view

Predefined user roles

network-admin

Parameters

auth-failure: Generates notifications as defined in RFC 2787 when the device in a VRRP group receives a VRRP advertisement with the authentication type or key not matching the local configuration.

new-master: Generates notifications as defined in RFC 2787 when the state of a device in a VRRP group changes from Initialize or Backup to Master.

Usage guidelines

To report critical VRRP events to an NMS, enable SNMP notifications for VRRP. For VRRP event notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

Examples

# Generate notifications as defined in RFC 2787 when the device in a VRRP group receives a VRRP advertisement with the authentication type or key not matching the local configuration.

<Sysname> system-view

[Sysname] snmp-agent trap enable vrrp auth-failure

### vrrp check-ttl enable

Use vrrp check-ttl enable to enable TTL check for IPv4 VRRP packets.

Use undo vrrp check-ttl enable to disable TTL check for IPv4 VRRP packets.

Syntax

vrrp check-ttl enable

undo vrrp check-ttl enable

Default

TTL check for IPv4 VRRP packets is enabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

The master in an IPv4 VRRP group periodically sends VRRP advertisements to declare its presence. The VRRP advertisements are multicast in the local subnet and cannot be forwarded by routers, so the TTL value is not changed. When the master sends VRRP advertisements, it sets the TTL value to 255. If you enable TTL check, the backups drop the VRRP advertisements with TTL other than 255, preventing attacks from other subnets.

Devices from different vendors might implement VRRP differently. When the device is interoperating with devices of other vendors, TTL check on VRRP packets might result in unexpected dropping of packets. In this scenario, use the undo vrrp check-ttl enable command to disable TTL check on VRRP packets.

Examples

# Disable TTL check for IPv4 VRRP packets.

<Sysname> system-view

[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] undo vrrp check-ttl enable

### vrrp dscp

Use vrrp dscp to set a DSCP value for VRRP packets.

Use undo vrrp dscp to restore the default.

Syntax

vrrp dscp dscp-value

undo vrrp dscp

Default

The DSCP value for VRRP packets is 48.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value for VRRP packets, in the range of 0 to 63.

Usage guidelines

The DSCP value identifies the packet priority during transmission. A greater DSCP value means a higher packet priority.

Examples

# Set the DSCP value to 30 for VRRP packets.

<Sysname> system-view

[Sysname] vrrp dscp 30

### vrrp mode

Use vrrp mode to specify the operating mode for IPv4 VRRP.

Use undo vrrp mode to restore the default.

Syntax

vrrp mode load-balance [ version-8 ]

undo vrrp mode

Default

IPv4 VRRP operates in standard mode.

Views

System view

Predefined user roles

network-admin

Parameters

load-balance: Specifies the load balancing mode.

version-8: Specifies the version carried in VRRP packets as 8.

Usage guidelines

After you create IPv4 VRRP groups on the router, you can use this command to modify their operating mode. All IPv4 VRRP groups on the router operate in the specified mode.

The version-8 keyword takes effect only when the version of IPv4 VRRP configured on the interface is VRRPv2. The version-8 keyword is required in the following conditions:

* A router running Comware 5 software exists in the VRRP group.

To display the software version, use the display version command.

* All routers in the IPv4 VRRP group are operating in load balancing mode.
* All routers in the IPv4 VRRP group are configured with the version of VRRPv2.

Examples

# Specify the load balancing mode for IPv4 VRRP.

<Sysname> system-view

[Sysname] vrrp mode load-balance

Related commands

display vrrp

### vrrp send-gratuitous-arp

Use vrrp send-gratuitous-arp to enable periodic sending of gratuitous ARP packets for IPv4 VRRP.

Use undo vrrp send-gratuitous-arp to disable periodic sending of gratuitous ARP packets for IPv4 VRRP.

Syntax

vrrp send-gratuitous-arp [ interval interval ]

undo vrrp send-gratuitous-arp

Default

Periodic sending of gratuitous ARP packets is disabled for IPv4 VRRP.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the sending interval in the range of 30 to 1200 seconds. The default value is 120 seconds.

Usage guidelines

This command ensures that the MAC address entry for the virtual MAC address of a VRRP group can be updated on downstream devices in a timely manner.

This command takes effect only in VRRP standard mode.

If you change the sending interval for gratuitous ARP packets, the configuration takes effect at the next sending interval.

The master sends the first gratuitous ARP packet at a random time in the second half of the set interval after you execute the vrrp send-gratuitous-arp command. This prevents too many gratuitous ARP packets from being sent at the same time.

The sending interval for gratuitous ARP packets might be much longer than the set interval when the following conditions are met:

* Multiple VRRP groups exist on the device.
* A short sending interval is set.

Examples

# Enable periodic sending of gratuitous ARP packets for IPv4 VRRP and set the sending interval to 200 seconds.

<Sysname> system-view

[Sysname] vrrp send-gratuitous-arp interval 200

### vrrp version

Use vrrp version to specify the version of IPv4 VRRP on an interface.

Use undo vrrp version to restore the default.

Syntax

vrrp version version-number

undo vrrp version

Default

VRRPv3 is used.

Views

Interface view

Predefined user roles

network-admin

Parameters

version-number: Specifies a VRRP version. The version number is 2 or 3, where 2 indicates VRRPv2 (described in RFC 3768), and 3 indicates VRRPv3 (described in RFC 5798).

Usage guidelines

The version of VRRP on all routers in an IPv4 VRRP group must be the same.

Examples

# Specify VRRPv2 to run on VLAN-interface 10.

<Sysname> system-view

[Sysname] interface vlan-interface 10

[Sysname-Vlan-interface10] vrrp version 2

### vrrp vrid

Use vrrp vrid to create an IPv4 VRRP group and assign a virtual IP address to it, or to assign a virtual IP address to an existing IPv4 VRRP group.

Use undo vrrp vrid to remove all configurations of an IPv4 VRRP group, or to remove a virtual IP address from an IPv4 VRRP group.

Syntax

vrrp vrid virtual-router-id virtual-ip virtual-address

undo vrrp vrid virtual-router-id [ virtual-ip [ virtual-address ] ]

Default

No IPv4 VRRP groups exist.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

virtual-ip virtual-address: Specifies a virtual IP address. You cannot specify the virtual IP address as any of the following IP addresses:

* All-zero address (0.0.0.0).
* Broadcast address (255.255.255.255).
* Loopback address.
* IP address of other than Class A, Class B, and Class C.
* Invalid IP address (for example, 0.0.0.1).

If you do not specify the virtual-address argument, the undo vrrp vrid command removes all virtual IP addresses from the specified IPv4 VRRP group.

Usage guidelines

You can execute this command multiple times to assign multiple virtual IP addresses to an IPv4 VRRP group. An IPv4 VRRP group can have a maximum of 16 virtual IP addresses.

An IPv4 VRRP group without virtual IP addresses configured can exist on a device provided that other settings (for example, priority and preemption mode) are available. Such a VRRP group stays in inactive state and does not function.

The virtual IP address of an IPv4 VRRP group and the downlink interface IP addresses of the VRRP group members must be in the same subnet. Otherwise, the hosts in the subnet might fail to access external networks.

For VRRP to operate correctly in load balancing mode, make sure the virtual IP address of an IPv4 VRRP group is not the IP address of any interfaces in the VRRP group.

Examples

# Create IPv4 VRRP group 1 and assign virtual IP address 10.10.10.10 to the VRRP group. Then assign virtual IP address 10.10.10.11 to the VRRP group.

<Sysname> system-view

[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.10.10.10

[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.10.10.11

Related commands

display vrrp

### vrrp vrid authentication-mode

Use vrrp vrid authentication-mode to configure the authentication mode and the authentication key for an IPv4 VRRP group to send and receive VRRP packets.

Use undo vrrp vrid authentication-mode to restore the default.

Syntax

vrrp vrid virtual-router-id authentication-mode { md5 | simple } { cipher | plain } string

undo vrrp vrid virtual-router-id authentication-mode

Default

Authentication is disabled when a VRRP group sends and receives VRRP packets.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 8 characters. Its encrypted form is a case-sensitive string of 1 to 41 characters.

Usage guidelines

To avoid attacks from unauthorized users, VRRP member routers add authentication keys in VRRP packets to authenticate one another. VRRP provides the following authentication modes:

* simple—Simple text authentication.

The sender fills an authentication key into the VRRP packet, and the receiver compares the received authentication key with its local authentication key. If the two authentication keys are the same, the received VRRP packet is legitimate. Otherwise, the received packet is illegitimate.

* md5—MD5 authentication.

The sender computes a digest for the VRRP packet by using the authentication key and MD5 algorithm, and saves the result to the authentication header. The receiver performs the same operation by using the authentication key and MD5 algorithm, and it compares the result with the content in the authentication header. If the results are the same, the received VRRP packet is legitimate. Otherwise, the received packet is illegitimate.

The MD5 authentication is more secure than the simple text authentication, but it costs more resources.

|  |  |
| --- | --- |
| IMPORTANT | IMPORTANT:  You can configure different authentication modes and authentication keys for the VRRP groups on an interface. However, members of the same VRRP group must use the same authentication mode and authentication key.  For VRRPv3, this command does not take effect because VRRPv3 does not support authentication. |

Examples

# Set the authentication mode to simple and the authentication key to Sysname for VRRP group 1 on VLAN-interface 2.

<Sysname> system-view

[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] vrrp vrid 1 authentication-mode simple plain Sysname

Related commands

display vrrp

vrrp version

### vrrp vrid follow

Use vrrp vrid follow to configure an IPv4 VRRP group to follow a master group.

Use undo vrrp vrid follow to remove the configuration.

Syntax

vrrp vrid virtual-router-id follow name

undo vrrp vrid virtual-router-id follow

Default

An IPv4 VRRP group does not follow a master group.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

name: Specifies a master IPv4 VRRP group by its name, a case-sensitive string of 1 to 20 characters.

Usage guidelines

This command configures an IPv4 VRRP group as a subordinate VRRP group to follow a master group. A subordinate VRRP group can forward service traffic.

An IPv4 VRRP group cannot be both a master group and a subordinate group.

An IPv4 VRRP group stays in Inactive state if it is configured to follow a nonexistent master VRRP group.

If an IPv4 VRRP group in Inactive or Initialize state follows a master group that is not in Inactive state, the state of the VRRP group does not change.

Examples

# Configure IPv4 VRRP group 1 to follow master group abc.

<Sysname> system-view

[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] vrrp vrid 1 follow abc

Related commands

display vrrp binding

vrrp vrid name

### vrrp vrid name

Use vrrp vrid name to configure an IPv4 VRRP group as a master group and assign a name to it.

Use undo vrrp vrid name to remove the configuration.

Syntax

vrrp vrid virtual-router-id name name

undo vrrp vrid virtual-router-id name

Default

An IPv4 VRRP group does not act as a master group.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

name: Specifies a master IPv4 VRRP group name, a case-sensitive string of 1 to 20 characters.

Usage guidelines

This command configures an IPv4 VRRP group as a master group by assigning a master group name to it. A VRRP group that follows the master group is a subordinate VRRP group. The master VRRP group exchanges VRRP packets among member devices. The subordinate VRRP group does not exchange VRRP packets and follows the state of the master group. Both the master and subordinate VRRP groups can forward service traffic.

You cannot assign the same master VRRP group name to different VRRP groups on a device.

Examples

# Configure IPv4 VRRP group 1 as a master group and assign master group name abc to it.

<Sysname> system-view

[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] vrrp vrid 1 name abc

Related commands

display vrrp binding

vrrp vrid follow

### vrrp vrid preempt-mode

Use vrrp vrid preempt-mode to enable the preemptive mode for the device in an IPv4 VRRP group and set the preemption delay.

Use undo vrrp vrid preempt-mode to disable the preemptive mode for the device in an IPv4 VRRP group.

Use undo vrrp vrid preempt-mode delay to restore the default preemption delay.

Syntax

vrrp vrid virtual-router-id preempt-mode [ delay delay-value ]

undo vrrp vrid virtual-router-id preempt-mode [ delay ]

Default

The device operates in preemptive mode and the preemption delay is 0 centiseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

delay delay-value: Specifies the preemption delay in the range of 0 to 180000 in centiseconds.

Usage guidelines

In non-preemptive mode, the master router acts as the master as long as it operates correctly, even if a backup is assigned a higher priority later. The non-preemptive mode helps avoid frequent switchover between the master and backups.

In preemptive mode, a backup sends VRRP advertisements when it detects that it has a higher priority than the master. Then the backup takes over as the master and the previous master becomes a backup. This mechanism ensures that the master is always the device with the highest priority.

You can configure the VRRP preemption delay for the following purposes:

* Avoid frequent state changes among members in a VRRP group.
* Provide the backups with enough time to collect information (such as routing information).

A backup does not immediately become the master after it receives an advertisement with a lower priority than the local priority. Instead, it waits for a period of time before taking over as the master.

Examples

# Enable the preemptive mode for the device in VRRP group 1, and set the preemption delay to 5000 centiseconds.

<Sysname> system-view

[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000

Related commands

display vrrp

### vrrp vrid priority

Use vrrp vrid priority to set the priority of the device in an IPv4 VRRP group.

Use undo vrrp vrid priority to restore the default.

Syntax

vrrp vrid virtual-router-id priority priority-value

undo vrrp vrid virtual-router-id priority

Default

The priority of a device in an IPv4 VRRP group is 100.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

priority-value: Specifies a priority value in the range of 1 to 254. A higher value indicates a higher priority.

Usage guidelines

VRRP determines the role (master or backup) of each device in a VRRP group by priority. A device with a higher priority is more likely to become the master.

Priorities 1 to 254 are configurable. Priority 0 is reserved for special uses, and priority 255 is for the IP address owner. The IP address owner in a VRRP group always has a running priority of 255 and acts as the master as long as it operates correctly.

Examples

# Set the priority of the switch to 150 in VRRP group 1 on VLAN-interface 2.

<Sysname> system-view

[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] vrrp vrid 1 priority 150

Related commands

display vrrp

vrrp vrid track

### vrrp vrid shutdown

Use vrrp vrid shutdown to disable an IPv4 VRRP group.

Use undo vrrp vrid shutdown to enable an IPv4 VRRP group.

Syntax

vrrp vrid virtual-router-id shutdown

undo vrrp vrid virtual-router-id shutdown

Default

An IPv4 VRRP group is enabled.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

Usage guidelines

You can use this command to temporarily disable an IPv4 VRRP group. After this command is configured, the VRRP group stays in Initialize state, and its configurations remain unchanged. You can change the configuration of the VRRP group, and your changes take effect when you enable the VRRP group again.

Examples

# Disable IPv4 VRRP group 1.

<Sysname> system-view

[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] vrrp vrid 1 shutdown

### vrrp vrid source-interface

Use vrrp vrid source-interface to specify the source interface for an IPv4 VRRP group, instead of the interface where the VRRP group resides, to send and receive VRRP packets.

Use undo vrrp source-interface to cancel the specified source interface.

Syntax

vrrp vrid virtual-router-id source-interface interface-type interface-number

undo vrrp vrid virtual-router-id source-interface

Default

No source interface is specified for a VRRP group. The interface where the VRRP group resides sends and receives VRRP packets.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

If VRRP group members cannot exchange VRRP packets through the interfaces where the VRRP group resides, use this command to specify interfaces for VRRP packet exchange.

Examples

# Specify VLAN-interface 20 as the source interface for VRRP packet exchange in IPv4 VRRP group 10.

<Sysname> system-view

[Sysname] interface vlan-interface 10

[Sysname-Vlan-interface10] vrrp vrid 10 source-interface vlan-interface 20

### vrrp vrid timer advertise

Use vrrp vrid timer advertise to set the interval at which the master in an IPv4 VRRP group sends VRRP advertisements.

Use undo vrrp vrid timer advertise to restore the default.

Syntax

vrrp vrid virtual-router-id timer advertise adver-interval

undo vrrp vrid virtual-router-id timer advertise

Default

The master in an IPv4 VRRP group sends VRRP advertisements at an interval of 100 centiseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

adver-interval: Specifies an interval for the master in the specified IPv4 VRRP group to send VRRP advertisements. The value range for this argument is 10 to 4095 centiseconds. For VRRPv2, the value of the adver-interval argument can only be a multiple of 100. For example, if you configure values in the range of 10 to 100, 101 to 200, and 4001 to 4095, the actual values are 100, 200, and 4100, respectively. For VRRPv3, the configured value for the adver-interval argument takes effect.

Usage guidelines

The master in an IPv4 VRRP group periodically sends VRRP advertisements to declare its presence. You can use this command to configure the interval at which the master sends VRRP advertisements.

As a best practice to maintain system stability, set the VRRP advertisement interval to be greater than 100 centiseconds.

In VRRPv2, all routers in an IPv4 VRRP group must have the same interval for sending VRRP advertisements.

In VRRPv3, the routers in an IPv4 VRRP group can have different intervals for sending VRRP advertisements. The master in the VRRP group sends VRRP advertisements at the specified interval and carries the interval attribute in the advertisements. After a backup receives the advertisement, it records the interval in the advertisement. If the backup does not receive any VRRP advertisement when the timer (3 × recorded interval + Skew\_Time) expires, it regards the master as failed and takes over.

Large network traffic might disable a backup from receiving VRRP advertisements from the master within the specified timer and trigger an unexpected master switchover. To solve this problem, you can use this command to set a larger interval.

Examples

# Configure the master in IPv4 VRRP group 1 to send VRRP advertisements at an interval of 500 centiseconds.

<Sysname> system-view

[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] vrrp vrid 1 timer advertise 500

Related commands

display vrrp

### vrrp vrid track

Use vrrp vrid track to associate a VRRP group or the VFs in a VRRP group with a track entry.

Use undo vrrp vrid track to remove the association between a VRRP group or the VFs in a VRRP group and a track entry.

Syntax

vrrp vrid virtual-router-id track track-entry-number { forwarder-switchover member-ip ip-address | priority reduced [ priority-reduced ] | switchover | weight reduced [ weight-reduced ] }

undo vrrp vrid virtual-router-id track [ track-entry-number ] [ forwarder-switchover | priority reduced | switchover | weight reduced ]

Default

A VRRP group and the VFs in a VRRP group are not associated with any track entries.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group number in the range of 1 to 255.

track-entry-number: Specifies a track entry by its number in the range of 1 to 1024.

forwarder-switchover member-ip ip-address: Enables the LVF on the router to take over the role of the AVF at the specified IP address immediately after the specified track entry changes to the Negative state. The ip-address argument specifies the IP address of a member router. You can use the display vrrp verbose command to view the IP addresses of the members.

priority reduced [ priority-reduced ]: Reduces the priority of the router in the VRRP group by the specified value when the state of the specified track entry changes to Negative. The value range for the priority-reduced argument is 1 to 255, and the default value is 10.

switchover: Enables the router in backup state to take over as the master immediately after the specified track entry changes to the Negative state.

weight reduced [ weight-reduced ]: Reduces the weight of all VFs on the router in the VRRP group by the specified value when the state of the specified track entry changes to Negative. The value range for the weight-reduced argument is 1 to 255, and the default value is 30.

Usage guidelines

When the associated track entry changes to the Negative state, one of the following events occurs depending on your configuration:

* The priority of the router in the VRRP group decreases by a specified value.
* The weight of VFs decreases by a specified value.
* The router immediately takes over as the master if it is a backup.
* The LVF on the router immediately takes over the role of the AVF at the specified IP address.

When the track entry changes from Negative to Positive or NotReady, one of the following events occurs:

* The router automatically restores its priority or VF weight.
* The failed master router becomes the master again.
* The failed AVF becomes active again.

Before executing this command, create a VRRP group on the interface and assign a virtual IP address to the VRRP group.

You can create a track entry by using the track command before or after you associate it with a VRRP group or the VFs in a VRRP group. For more information about configuring track entries, see High Availability Configuration Guide.

If no track entry is specified, the undo vrrp vrid track command removes all associations between track entries and the VRRP group or VFs in the VRRP group.

The vrrp vrid track priority reduced command and the vrrp vrid track switchover command do not take effect on an IP address owner. If you configure the command on an IP address owner, the configuration takes effect after the router changes to be a non-IP address owner.

The following parameters take effect only when the IPv4 VRRP group is operating in load balancing mode:

* The forwarder-switchover member-ip ip-address option.
* The weight reduced weight-reduced option.
* The weight reduced keyword.

The weight of a VF is 255, and its lower limit of failure is 10.

When the weight of a VF owner is higher than or equal to the lower limit of failure, its priority is always 255. The priority does not change with the weight. When the upstream link of the VF owner fails, an LVF must take over as the AVF. The switchover occurs when the weight of the VF owner drops below the lower limit of failure. This requires that the reduced weight for the VF owner be higher than 245.

Examples

# Associate VRRP group 1 on VLAN-interface 2 with track entry 1 and decrease the router priority by 50 when the state of track entry 1 changes to Negative.

<Sysname> system-view

[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] vrrp vrid 1 track 1 priority reduced 50

# Associate the VFs of IPv4 VRRP group 1 on VLAN-interface 2 with track entry 1. Enable the LVF to take over the role of the AVF at the IP address of 10.1.1.3 immediately when the state of track entry 1 changes to Negative.

<Sysname> system-view

[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] vrrp vrid 1 track 1 forwarder-switchover member-ip 10.1.1.3

# Associate the VFs of IPv4 VRRP group 1 on VLAN-interface 2 with track entry 1. Decrease the weight of all VFs on the router in the VRRP group by 50 when the state of track entry 1 changes to Negative.

<Sysname> sysname-view

[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] vrrp vrid 1 track 1 weight reduced 50

Related commands

display vrrp

### vrrp vrid vrrpv3-send-packet

Use vrrp vrid vrrpv3-send-packet to set the packet sending mode for IPv4 VRRPv3.

Use undo vrrp vrid vrrpv3-send-packet to restore the default.

Syntax

vrrp vrid virtual-router-id vrrpv3-send-packet { v2-only | v2v3-both }

undo vrrp vrid virtual-router-id vrrpv3-send-packet

Default

A router configured with IPv4 VRRPv3 sends only VRRPv3 packets.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

v2-only: Sends VRRPv2 packets only.

v2v3-both: Sends both VRRPv2 and VRRPv3 packets.

Usage guidelines

This command takes effect only on IPv4 VRRPv3.

The packet sending mode for IPv4 VRRPv3 takes effect only on outgoing VRRP packets. A router configured with VRRPv3 can process incoming VRRPv2 and VRRPv3 packets.

If you set the packet sending mode for IPv4 VRRPv3 and configure VRRP packet authentication, authentication information will be carried in outgoing VRRPv2 packets but not in outgoing VRRPv3 packets.

The VRRP advertisement interval is set in centiseconds by using the vrrp vrid timer advertise command. The VRRP advertisement interval carried in VRRPv2 packets sent from routers configured with VRRPv3 might be different from the configured value. For information about the VRRP advertisement interval, see the vrrp vrid timer advertise command.

Examples

# Configure VRRP group 1 to send both VRRPv2 and VRRPv3 packets.

<Sysname> system-view

[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] vrrp vrid 1 version-3 send-packet-mode v2v3-both

Related commands

display vrrp

## IPv6 VRRP commands

VRRP does not take effect on member ports of aggregation groups.

### display vrrp ipv6

Use display vrrp ipv6 to display the states of IPv6 VRRP groups.

Syntax

display vrrp ipv6 [ interface interface-type interface-number [ vrid virtual-router-id ] ] [ verbose ]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface interface-type interface-number: Specifies an interface by its type and number.

vrid virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

verbose: Displays detailed IPv6 VRRP group information. If you do not specify the verbose keyword, the command displays brief IPv6 VRRP group information.

Usage guidelines

If no interface or VRRP group is specified, this command displays the states of all IPv6 VRRP groups.

If only an interface is specified, this command displays the states of all IPv6 VRRP groups on the specified interface.

If both an interface and an IPv6 VRRP group are specified, this command displays the states of the specified IPv6 VRRP group on the specified interface.

Examples

# Display brief information about all IPv6 VRRP groups on the device when VRRP operates in standard mode.

<Sysname> display vrrp ipv6

IPv6 Virtual Router Information:

Running Mode : Standard

ND sending interval : 120 sec

Total number of virtual routers : 1

Interface VRID State Running Adver Auth Virtual

Pri Timer Type IP

---------------------------------------------------------------------

Vlan2 1 Master 150 100 None FE80::1

Command output (in standard mode)

| Field | Description |
| --- | --- |
| Running Mode | VRRP operating mode (standard mode). |
| ND sending interval | Sending interval for ND packets. This field is displayed only after you configure the vrrp ipv6 send-nd command. |
| Total number of virtual routers | Total number of VRRP groups. |
| Interface | Interface where the VRRP group is configured. |
| VRID | Virtual router ID (VRRP group number). |
| State | Status of the router in the VRRP group:   * + - * Master.       * Backup.       * Initialize.       * Inactive. |
| Running Pri | Current priority of the router.  When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes. |
| Adver Timer | VRRP advertisement sending interval in centiseconds. |
| Auth Type | Authentication type. Only none is available, which means no authentication is required. |
| Virtual IP | Virtual IP address of the VRRP group. |

# Display detailed information about all IPv6 VRRP groups on the device when VRRP operates in standard mode.

<Sysname> display vrrp ipv6 verbose

IPv6 Virtual Router Information:

Running Mode : Standard

ND sending interval : 120 sec

Total number of virtual routers : 2

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Master

Config Pri : 150 Running Pri : 150

Preempt Mode : Yes Delay Time : 10

Auth Type : None

Virtual IP : FE80::1

Virtual MAC : 0000-5e00-0201

Master IP : FE80::2

Config Role : Master

Name : abc

VRRP Track Information:

Track Object : 1 State : Positive Pri Reduced : 50

Interface Vlan-interface2

VRID : 2 Adver Timer : 100

Admin Status : Up State : Backup

Config Pri : 80 Running Pri : 80

Preempt Mode : Yes Delay Time : 0

Become Master : 2450ms left

Auth Type : None

Virtual IP : FE80::11

Virtual MAC : 0000-5e00-0202

Master IP : FE80::12

Interface Vlan-interface2

VRID : 3 Adver Timer : 100

Admin Status : Up State : Master

Config Pri : 100 Running Pri : 100

Preempt Mode : Yes Delay Time : 0

Auth Type : None

Virtual IP : FE80::10

Virtual MAC : 0000-5e00-0203

Master IP : FE80::2

Config Role : Subordinate

Follow Name : abc

Command output (in standard mode)

| Field | Description |
| --- | --- |
| Running Mode | VRRP operating mode (standard mode). |
| ND sending interval | Sending interval for ND packets. This field is displayed only after you configure the vrrp ipv6 send-nd command. |
| Total number of virtual routers | Total number of VRRP groups. |
| Interface | Interface where the VRRP group is configured. |
| VRID | Virtual router ID (VRRP group number). |
| Adver Timer | VRRP advertisement sending interval in centiseconds. |
| Admin Status | Administrative status: Up or Down. |
| State | Status of the router in the VRRP group:   * + - * Master.       * Backup.       * Initialize.       * Inactive. |
| Config Pri | Configured priority of the router, which is configured by using the vrrp ipv6 vrid priority command. |
| Running Pri | Current priority of the router.  When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes. |
| Preempt Mode | Preemptive mode:   * + - * Yes.       * No. |
| Delay Time | Preemption delay in centiseconds. |
| Become Master | Time (in milliseconds) that a backup router has to wait before it becomes the master. This field is displayed only when the router is a backup. |
| Auth Type | Authentication type. Only none is available, which means no authentication is required. |
| Virtual IP | Virtual IP address of the VRRP group. |
| Virtual MAC | Virtual MAC address of the VRRP group's virtual IP address, which is displayed when the router is the master. |
| Master IP | Link-local address of the interface where the master resides. |
| Config Role | The configured role of the IPv6 VRRP group to which the router belongs.   * + - * Master.       * Subordinate. |
| Name | Master group name assigned to the IPv6 VRRP group. This field is displayed only after you configure the vrrp ipv6 vrid name command. |
| Follow Name | Name of the master VRRP group that the IPv6 VRRP group follows. This field is displayed only after you configure the vrrp ipv6 vrid follow command. |
| VRRP Track Information | Track entry information. This field is displayed only after you configure the vrrp ipv6 vrid track command. |
| Track Object | Track entry which is associated with the VRRP group. |
| State | Track entry state:   * + - * Negative.       * Positive.       * NotReady. |
| Pri Reduced | Value by which the priority decreases when the state of the associated track entry becomes Negative. |
| Switchover | Switchover mode. When the state of the associated track entry becomes Negative, the backup immediately becomes the master. |

# Display brief information about all IPv6 VRRP groups on the device when VRRP operates in load balancing mode.

<Sysname> display vrrp ipv6

IPv6 Virtual Router Information:

Running Mode : Load Balance

Total number of virtual routers : 1

Interface VRID State Running Address Active

Pri

----------------------------------------------------------------------

Vlan2 1 Master 150 FE80::1 Local

----- VF 1 Active 255 000f-e2ff-4011 Local

Command output (in load balancing mode)

| Field | Description |
| --- | --- |
| Running Mode | VRRP operating mode (load balancing mode). |
| Total number of virtual routers | Total number of VRRP groups. |
| Interface | Interface where the VRRP group is configured. |
| VRID | Virtual router ID (VRRP group number) or VF ID. |
| State | * + - * For a VRRP group, this field indicates the state of the router in the VRRP group. The state can be Master, Backup, Initialize, or Inactive.       * For a VF, this field indicates the state of the VF in the VRRP group. The state can be Active, Listening, or Initialize. |
| Running Pri | * + - * For a VRRP group, this field indicates the running priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes.       * For a VF, this field indicates the running priority of the VF. When a track entry is associated with a VF, the priority of the VF changes if the state of the track entry changes. |
| Address | * + - * For a VRRP group, this field indicates the virtual IP address of the VRRP group.       * For a VF, this field indicates the virtual MAC address of the VF. |
| Active | * + - * For a VRRP group, this field indicates the link-local address of the interface where the master resides. If the current router is the master, this field displays local.       * For a VF, this field indicates the link-local address of the interface where the AVF resides. If the current VF is the AVF, this field displays local. |

# Display detailed information about all IPv6 VRRP groups on the device when VRRP operates in load balancing mode.

<Sysname> display vrrp ipv6 verbose

IPv6 Virtual Router Information:

Running Mode : Load Balance

Total number of virtual routers : 2

Interface Vlan-interface2

VRID : 1 Adver Timer : 100

Admin Status : Up State : Master

Config Pri : 150 Running Pri : 150

Preempt Mode : Yes Delay Time : 5

Auth Type : None

Virtual IP : FE80::10

Member IP List : FE80::3 (Local, Master)

FE80::2 (Backup)

Master IP : FE80::3

VRRP Track Information:

Track Object : 1 State : Positive Pri Reduced : 50

Forwarder Information: 2 Forwarders 1 Active

Config Weight : 255

Running Weight : 255

Forwarder 01

State : Active

Virtual MAC : 000f-e2ff-4011 (Owner)

Owner ID : 0000-5e01-1101

Priority : 255

Active : local

Forwarder 02

State : Listening

Virtual MAC : 000f-e2ff-4012 (Learnt)

Owner ID : 0000-5e01-1103

Priority : 127

Active : FE80::2

Forwarder Weight Track Information:

Track Object : 1 State : Positive Weight Reduced : 250

Interface Vlan-interface2

VRID : 11 Adver Timer : 100

Admin Status : Up State : Backup

Config Pri : 80 Running Pri : 80

Preempt Mode : Yes Delay Time : 0

Become Master : 2450ms left

Auth Type : None

Virtual IP : FE80::11

Member IP List : FE80::3 (Local, Backup)

FE80::2 (Master)

Master IP : FE80::2

Forwarder Information: 2 Forwarders 1 Active

Config Weight : 255

Running Weight : 255

Forwarder 01

State : Active

Virtual MAC : 000f-e2ff-40b1 (Learnt)

Owner ID : 0000-5e01-1103

Priority : 127

Active : FE80::2

Forwarder 02

State : Listening

Virtual MAC : 000f-e2ff-40b2 (Owner)

Owner ID : 0000-5e01-1101

Priority : 255

Active : local

Command output (in load balancing mode)

| Field | Description |
| --- | --- |
| Running Mode | VRRP operating mode (load balancing mode). |
| Total number of virtual routers | Total number of VRRP groups. |
| Interface | Interface where the VRRP group is configured. |
| VRID | Virtual router ID (VRRP group number). |
| Adver Timer | VRRP advertisement sending interval in centiseconds. |
| Admin Status | Administrative status: Up or Down. |
| State | Status of the router in the VRRP group:   * + - * Master.       * Backup.       * Initialize.       * Inactive. |
| Config Pri | Configured priority of the router, which is configured by using the vrrp ipv6 vrid priority command. |
| Running Pri | Current priority of the router.  When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes. |
| Preempt Mode | Preemptive mode:   * + - * Yes.       * No. |
| Delay Time | Preemption delay in centiseconds. |
| Become Master | Time (in milliseconds) that a backup router has to wait before it becomes the master. This field is displayed only when the router is a backup. |
| Auth Type | Authentication type. Only none is available, which means no authentication is required. |
| Virtual IP | Virtual IP address list of the VRRP group. |
| Member IP List | IP addresses of the member devices in the VRRP group:   * + - * Local—IP address of the local router.       * Master—IP address of the master.       * Backup—IP address of the backup. |
| VRRP Track Information | Track entry that is associated with the VRRP group. This field is displayed only after you configure the vrrp ipv6 vrid track command. |
| Track Object | Track entry to be monitored. This field is displayed only after you configure the vrrp ipv6 vrid track command. |
| State | Track entry state:   * + - * Negative.       * Positive.       * NotReady. |
| Pri Reduced | Value by which the priority decreases when the status of the associated track entry becomes Negative. This field is displayed only after you configure the vrrp ipv6 vrid track command. |
| Switchover | Switchover mode. When the status of the associated track entry becomes Negative, the backup immediately becomes the master. |
| Forwarder Information: 2 Forwarders 1 Active | VF information: Two VFs exist and one is the AVF. |
| Config Weight | Configured weight of the VF: 255. |
| Running Weight | Current weight of the VF.  When a track entry is associated with the VFs of a VRRP group, the VFs' weights change when the track entry's status changes. |
| Forwarder 01 | Information about VF 01. |
| State | VF state:   * + - * Active.       * Listening.       * Initialize. |
| Virtual MAC | Virtual MAC address of the VF. |
| Owner ID | Real MAC address of the VF owner. |
| Priority | VF priority in the range of 1 to 255. |
| Active | Link-local address of the interface where the AVF resides. If the current VF is the AVF, this field displays local. |
| Forwarder Weight Track Configuration | VF weight Track configuration.  The field is displayed only after you configure the vrrp ipv6 vrid track command. |
| Track Object | Track entry which is associated with the VFs.  The field is displayed only after you configure the vrrp ipv6 vrid track command. |
| State | Track entry state:   * + - * Negative.       * Positive.       * NotReady. |
| Weight Reduced | Value by which the weights of the VFs decrease when the state of the associated track entry changes to Negative.  The field is displayed only after you configure the vrrp ipv6 vrid track command. |
| Forwarder Switchover Track Information: | VF switchover Track configuration.  The field is displayed only after you configure the vrrp ipv6 vrid track command. |
| Member IP | IPv6 address of a member device.  The field is displayed only after you configure the vrrp ipv6 vrid track command. |

### display vrrp ipv6 binding

Use display vrrp ipv6 binding to display master-to-subordinate IPv6 VRRP group bindings.

Syntax

display vrrp ipv6 binding [ interface interface-type interface-number [ vrid virtual-router-id ] | name name ]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface interface-type interface-number: Specifies an interface by its type and number. The interface must be an interface to which master IPv6 VRRP groups belong.

vrid virtual-router-id: Specifies a master IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

name name: Specifies a master IPv6 VRRP group by its name, a case-sensitive string of 1 to 20 characters.

Usage guidelines

If you do not specify any parameters, this command displays all master-to-subordinate IPv6 VRRP group bindings.

If you specify an interface but do not specify the virtual router ID of a master IPv6 VRRP group, this command displays all master-to-subordinate IPv6 VRRP group bindings on the specified interface.

If you specify an interface and the virtual router ID of a master IPv6 VRRP group, this command displays the binding information about the specified master VRRP group on the specified interface.

Examples

# Display master-to-subordinate IPv6 VRRP group bindings.

<Sysname> display vrrp ipv6 binding

IPv6 virtual router binding information:

Total number of master virtual routers : 1

Total number of subordinate virtual routers : 2

Interface : Vlan2 Master VRID : 1

Name : a Status : Backup

Subordinate virtual routers : 1

Interface : Vlan2 VRID : 4

Interface : -- Master VRID : --

Name : c Status : --

Subordinate virtual routers : 1

Interface : Vlan2 VRID : 5

Command output

| Field | Description |
| --- | --- |
| Total number of master virtual routers | Total number of master IPv6 VRRP groups. |
| Total number of subordinate virtual routers | Total number of subordinate IPv6 VRRP groups. |
| Interface | Interface to which the master IPv6 VRRP group belongs. If the master IPv6 VRRP group does not exist, this field displays two hyphens (--). |
| Master VRID | Virtual router ID of the master IPv6 VRRP group. If the master IPv6 VRRP group does not exist, this field displays two hyphens (--). |
| Name | Name of the master IPv6 VRRP group. |
| Status | Status of the router in the master IPv6 VRRP group:   * + - * Master.       * Backup.       * Initialize.       * Inactive.   If the master IPv6 VRRP group does not exist, this field displays two hyphens (--). |
| Subordinate virtual routers | Number of subordinate IPv6 VRRP groups. |
| Interface | Interface to which the subordinate IPv6 VRRP group belongs. |
| VRID | Virtual router ID of the subordinate IPv6 VRRP group. |

Related commands

vrrp ipv6 vrid follow

vrrp ipv6 vrid name

### display vrrp ipv6 statistics

Use display vrrp ipv6 statistics to display statistics for IPv6 VRRP groups.

Syntax

display vrrp ipv6 statistics [ interface interface-type interface-number [ vrid virtual-router-id ] ]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface interface-type interface-number: Specifies an interface by its type and number.

vrid virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

Usage guidelines

If no interface or VRRP group is specified, this command displays statistics for all IPv6 VRRP groups.

If only an interface is specified, this command displays statistics for all IPv6 VRRP groups on the specified interface.

If both an interface and an IPv6 VRRP group are specified, this command displays statistics for the specified IPv6 VRRP group on the specified interface.

Examples

# Display statistics for all IPv6 VRRP groups when VRRP operates in standard mode.

<Sysname> display vrrp ipv6 statistics

Interface : Vlan-interface2

VRID : 1

CheckSum Errors : 0 Version Errors : 0

Invalid Pkts Rcvd : 0 Unexpected Pkts Rcvd : 0

Hop Limit Errors : 0 Advertisement Interval Errors : 0

Invalid Auth Type : 0 Auth Failures : 0

Packet Length Errors : 0 Auth Type Mismatch : 0

Become Master : 1 Address List Errors : 0

Adver Rcvd : 0 Priority Zero Pkts Rcvd : 0

Adver Sent : 425 Priority Zero Pkts Sent : 0

IP Owner Conflicts : 0

Global statistics

CheckSum Errors : 0

Version Errors : 0

VRID Errors : 0

# Display statistics for all IPv6 VRRP groups when VRRP operates in load balancing mode.

<Sysname> display vrrp ipv6 statistics

Interface : Vlan-interface2

VRID : 1

CheckSum Errors : 0 Version Errors : 0

Invalid Pkts Rcvd : 0 Unexpected Pkts Rcvd : 0

Hop Limit Errors : 0 Advertisement Interval Errors : 0

Invalid Auth Type : 0 Auth Failures : 0

Packet Length Errors : 0 Auth Type Mismatch : 0

Become Master : 39 Address List Errors : 0

Become AVF : 13 Packet Option Errors : 0

Adver Rcvd : 2562 Priority Zero Pkts Rcvd : 1

Adver Sent : 16373 Priority Zero Pkts Sent : 49

Request Rcvd : 2 Reply Rcvd : 10

Request Sent : 12 Reply Sent : 2

Release Rcvd : 0 VF Priority Zero Pkts Rcvd : 1

Release Sent : 0 VF Priority Zero Pkts Sent : 11

Redirect Timer Expires : 1 Time-out Timer Expires : 0

Global statistics

CheckSum Errors : 0

Version Errors : 0

VRID Errors : 0

Command output (in standard mode)

| Field | Description |
| --- | --- |
| Interface | Interface where the VRRP group is configured. |
| VRID | VRRP group number. |
| CheckSum Errors | Number of packets with checksum errors. |
| Version Errors | Number of packets with version errors. |
| Invalid Pkts Rcvd | Number of received packets of invalid packet types. |
| Unexpected Pkts Rcvd | Number of received unexpected packets. |
| Advertisement Interval Errors | Number of packets with advertisement interval errors. |
| Hop Limit Errors | Number of packets with hop limit errors. |
| Auth Failures | Number of packets with authentication failures. |
| Invalid Auth Type | Number of packets with authentication failures because of invalid authentication types. |
| Auth Type Mismatch | Number of packets with authentication failures because of mismatching authentication types. |
| Packet Length Errors | Number of packets with VRRP packet length errors. |
| Address List Errors | Number of packets with virtual IP address list errors. |
| Become Master | Number of times that the router has been elected as the master. |
| Priority Zero Pkts Rcvd | Number of received advertisements with the router priority of 0. |
| Adver Rcvd | Number of received advertisements. |
| Priority Zero Pkts Sent | Number of sent advertisements with the router priority of 0. |
| Adver Sent | Number of sent advertisements. |
| IP Owner Conflicts | Number of VRRP packets that the local router (IP address owner) has received from conflicting IP address owners. |
| Global statistics | Global statistics for all IPv6 VRRP groups. |
| CheckSum Errors | Total number of packets with checksum errors. |
| Version Errors | Total number of packets with version errors. |
| VRID Errors | Total number of packets with VRID errors. |

Command output (in load balancing mode)

| Field | Description |
| --- | --- |
| Interface | Interface where the VRRP group is configured. |
| VRID | VRRP group number. |
| CheckSum Errors | Number of packets with checksum errors. |
| Version Errors | Number of packets with version errors. |
| Invalid Pkts Rcvd | Number of received packets of invalid packet types. |
| Unexpected Pkts Rcvd | Number of received unexpected packets. |
| Advertisement Interval Errors | Number of packets with advertisement interval errors. |
| Hop Limit Errors | Number of packets with hop limit errors. |
| Auth Failures | Number of packets with authentication failures. |
| Invalid Auth Type | Number of packets with authentication failures because of invalid authentication types. |
| Auth Type Mismatch | Number of packets with authentication failures because of mismatching authentication types. |
| Packet Length Errors | Number of packets with VRRP packet length errors. |
| Address List Errors | Number of packets with virtual IP address list errors. |
| Become Master | Number of times that the router has been elected as the master. |
| Redirect Timer Expires | Number of times that the redirect timer expired. |
| Become AVF | Number of times that the VF has been elected as the AVF. |
| Time-out Timer Expires | Number of times that the time-out timer expired. |
| Adver Rcvd | Number of received advertisements. |
| Request Rcvd | Number of received requests. |
| Adver Sent | Number of sent advertisements. |
| Request Sent | Number of sent requests. |
| Reply Rcvd | Number of received replies. |
| Release Rcvd | Number of received release packets. |
| Reply Sent | Number of sent replies. |
| Release Sent | Number of sent release packets. |
| Priority Zero Pkts Rcvd | Number of received advertisements with the router priority of 0. |
| VF Priority Zero Pkts Rcvd | Number of received advertisements with the VF priority of 0. |
| Priority Zero Pkts Sent | Number of sent advertisements with the router priority of 0. |
| VF Priority Zero Pkts Sent | Number of sent advertisements with the VF priority of 0. |
| Packet Option Errors | Number of packet option errors. |
| Global statistics | Global statistics for all IPv6 VRRP groups. |
| CheckSum Errors | Total number of packets with checksum errors. |
| Version Errors | Total number of packets with version errors. |
| VRID Errors | Total number of packets with VRID errors. |

Related commands

reset vrrp ipv6 statistics

### reset vrrp ipv6 statistics

Use reset vrrp ipv6 statistics to clear statistics for IPv6 VRRP groups.

Syntax

reset vrrp ipv6 statistics [ interface interface-type interface-number [ vrid virtual-router-id ] ]

Views

User view

Predefined user roles

network-admin

Parameters

interface interface-type interface-number: Specifies an interface by its type and number.

vrid virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

Usage guidelines

If no interface or VRRP group is specified, this command clears statistics for all IPv6 VRRP groups.

If only an interface is specified, this command clears statistics for all IPv6 VRRP groups on the specified interface.

If both an interface and an IPv6 VRRP group are specified, this command clears statistics for the specified IPv6 VRRP group on the specified interface.

Examples

# Clear statistics for all IPv6 VRRP groups on all interfaces.

<Sysname> reset vrrp ipv6 statistics

Related commands

display vrrp ipv6 statistics

### vrrp ipv6 dscp

Use vrrp ipv6 dscp to set a DSCP value for IPv6 VRRP packets.

Use undo vrrp ipv6 dscp to restore the default.

Syntax

vrrp ipv6 dscp dscp-value

undo vrrp ipv6 dscp

Default

The DSCP value for IPv6 VRRP packets is 56.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value for IPv6 VRRP packets, in the range of 0 to 63.

Usage guidelines

The DSCP value identifies the packet priority during transmission. A greater DSCP value means a higher packet priority.

Examples

# Set the DSCP value to 30 for IPv6 VRRP packets.

<Sysname> system-view

[Sysname] vrrp ipv6 dscp 30

### vrrp ipv6 mode

Use vrrp ipv6 mode to specify the operating mode for IPv6 VRRP.

Use undo vrrp ipv6 mode to restore the default.

Syntax

vrrp ipv6 mode load-balance

undo vrrp ipv6 mode

Default

IPv6 VRRP operates in standard mode.

Views

System view

Predefined user roles

network-admin

Parameters

load-balance: Specifies the load balancing mode.

Usage guidelines

For IPv6 VRRP to operate correctly in load balancing mode, make sure the virtual IPv6 address of an IPv6 VRRP group is not the IPv6 address of any interfaces in the VRRP group.

After you create IPv6 VRRP groups on the router, you can use this command to modify their operating mode. All IPv6 VRRP groups on the router operate in the specified mode.

Examples

# Specify the load balancing mode for IPv6 VRRP.

<Sysname> system-view

[Sysname] vrrp ipv6 mode load-balance

Related commands

display vrrp ipv6

### vrrp ipv6 send-nd

Use vrrp ipv6 send-nd to enable periodic sending of ND packets for IPv6 VRRP.

Use undo vrrp ipv6 send-nd to disable periodic sending of ND packets for IPv6 VRRP.

Syntax

vrrp ipv6 send-nd [ interval interval ]

undo vrrp ipv6 send-nd

Default

Periodic sending of ND packets is disabled for IPv6 VRRP.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the sending interval in the range of 30 to 1200 seconds. The default value is 120 seconds.

Usage guidelines

This command ensures that the MAC address entry for the virtual MAC address of an IPv6 VRRP group can be updated on downstream devices in a timely manner.

This command takes effect only in VRRP standard mode.

If you change the sending interval for ND packets, the configuration takes effect at the next sending interval.

The master sends the first ND packet at a random time in the second half of the set interval after you execute the vrrp ipv6 send-nd command. This prevents too many ND packets from being sent at the same time.

The sending interval for ND packets might be much longer than the set interval when the following conditions are met:

* Multiple IPv6 VRRP groups exist on the device.
* A short sending interval is set.

Examples

# Enable periodic sending of ND packets for IPv6 VRRP and set the sending interval to 200 seconds.

<Sysname> system-view

[Sysname] vrrp ipv6 send-nd interval 200

### vrrp ipv6 vrid

Use vrrp ipv6 vrid to create an IPv6 VRRP group and assign a virtual IPv6 address to it, or to assign a virtual IPv6 address to an existing IPv6 VRRP group.

Use undo vrrp ipv6 vrid to remove all configurations of an IPv6 VRRP group, or to remove a virtual IPv6 address from an IPv6 VRRP group.

Syntax

vrrp ipv6 vrid virtual-router-id virtual-ip virtual-address [ link-local ]

undo vrrp ipv6 vrid virtual-router-id [ virtual-ip [ virtual-address [ link-local ] ] ]

Default

No IPv6 VRRP groups exist.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

virtual-ip virtual-address: Specifies a virtual IPv6 address. If you do not specify this option, the undo vrrp ipv6 vrid command removes all virtual IPv6 addresses from the specified IPv6 VRRP group.

link-local: Specifies a link-local address as the virtual IPv6 address.

Usage guidelines

You can execute this command multiple times to assign multiple virtual IPv6 addresses to an IPv6 VRRP group. An IPv6 VRRP group can have a maximum of 16 virtual IPv6 addresses.

The first virtual IPv6 address that you assign to an IPv6 VRRP group must be a link-local address, and it must be removed last.

An IPv6 VRRP group can have only one link-local address as its virtual IPv6 address.

An IPv6 VRRP group without virtual IPv6 addresses configured can exist on a device provided that other settings (for example, priority and preemption mode) are available. Such a VRRP group stays in inactive state and does not function.

The virtual IPv6 address of an IPv6 VRRP group and the downlink interface IPv6 address of the VRRP group members must be in the same subnet. Otherwise, the hosts in the subnet might fail to access external networks.

Examples

# Create IPv6 VRRP group 1 and assign virtual IPv6 address fe80::10 to the VRRP group. Then assign virtual IPv6 address 1::10 to the VRRP group.

<Sysname> system-view

[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local

[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10

Related commands

display vrrp ipv6

### vrrp ipv6 vrid follow

Use vrrp ipv6 vrid follow to configure an IPv6 VRRP group to follow a master group.

Use undo vrrp ipv6 vrid follow to remove the configuration.

Syntax

vrrp ipv6 vrid virtual-router-id follow name

undo vrrp ipv6 vrid virtual-router-id follow

Default

An IPv6 VRRP group does not follow a master group.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

name: Specifies a master IPv6 VRRP group by its name, a case-sensitive string of 1 to 20 characters.

Usage guidelines

This command configures an IPv6 VRRP group as a subordinate VRRP group to follow a master group. A subordinate IPv6 VRRP group can forward service traffic.

An IPv6 VRRP group cannot be both a master group and a subordinate group.

An IPv6 VRRP group stays in Inactive state if it is configured to follow a nonexistent master VRRP group.

If an IPv6 VRRP group in Inactive or Initialize state follows a master group that is not in Inactive state, the state of the VRRP group does not change.

Examples

# Configure IPv6 VRRP group 1 to follow master group abc.

<Sysname> system-view

[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 follow abc

Related commands

display vrrp ipv6 binding

vrrp ipv6 vrid name

### vrrp ipv6 vrid name

Use vrrp ipv6 vrid name to configure an IPv6 VRRP group as a master group and assign a name to it.

Use undo vrrp ipv6 vrid name to remove the configuration.

Syntax

vrrp ipv6 vrid virtual-router-id name name

undo vrrp ipv6 vrid virtual-router-id name

Default

An IPv6 VRRP group does not act as a master group.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

name: Specifies a master IPv6 VRRP group name, a case-sensitive string of 1 to 20 characters.

Usage guidelines

This command configures an IPv6 VRRP group as a master group through assigning a master group name to it. An IPv6 VRRP group that follows the master group is a subordinate VRRP group. The master VRRP group exchanges VRRP packets among member devices. The subordinate group does not exchange VRRP packets and follows the state of the master group. Both the master and subordinate VRRP groups can forward service traffic.

You cannot assign the same master VRRP group name to different IPv6 VRRP groups on a device.

Examples

# Configure IPv6 VRRP group 1 as a master VRRP group and assign master group name abc to it.

<Sysname> system-view

[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 name abc

Related commands

display vrrp ipv6 binding

vrrp ipv6 vrid follow

### vrrp ipv6 vrid preempt-mode

Use vrrp ipv6 vrid preempt-mode to enable the preemptive mode for the router in an IPv6 VRRP group and set the preemption delay.

Use undo vrrp ipv6 vrid preempt-mode to disable the preemptive mode for the router in an IPv6 VRRP group.

Use undo vrrp ipv6 vrid preempt-mode delay to restore the default preemption delay.

Syntax

vrrp ipv6 vrid virtual-router-id preempt-mode [ delay delay-value ]

undo vrrp ipv6 vrid virtual-router-id preempt-mode [ delay ]

Default

The router operates in preemptive mode and the preemption delay is 0 centiseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

delay delay-value: Specifies the preemption delay in the range of 0 to 180000 in centiseconds.

Usage guidelines

In non-preemptive mode, the master router acts as the master as long as it operates correctly, even if a backup is assigned a higher priority later. The non-preemptive mode helps avoid frequent switchover between the master and backups.

In preemptive mode, a backup sends VRRP advertisements when it detects that it has a higher priority than the master. Then the backup takes over as the master and the previous master becomes a backup. This mechanism ensures that the master is always the router with the highest priority.

You can configure the VRRP preemption delay for the following purposes:

* Avoid frequent state changes among members in a VRRP group.
* Provide the backups with enough time to collect information (such as routing information).

A backup does not immediately become the master after it receives an advertisement with a lower priority than the local priority. Instead, it waits for a period of time before taking over.

Examples

# Enable the preemptive mode for VRRP group 1, and set the preemption delay to 5000 centiseconds.

<Sysname> system-view

[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] vrrp ipv6 vrid 10 preempt-mode delay 5000

Related commands

display vrrp ipv6

### vrrp ipv6 vrid priority

Use vrrp ipv6 vrid priority to set the priority of the router in an IPv6 VRRP group.

Use undo vrrp ipv6 vrid priority to restore the default.

Syntax

vrrp ipv6 vrid virtual-router-id priority priority-value

undo vrrp ipv6 vrid virtual-router-id priority

Default

The priority of a router in an IPv6 VRRP group is 100.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

priority-value: Specifies a priority value in the range of 1 to 254. A higher value indicates a higher priority.

Usage guidelines

VRRP determines the role (master or backup) of each router in a VRRP group by priority. A router with a higher priority is more likely to become the master.

Priorities 1 to 254 are configurable. Priority 0 is reserved for special uses, and priority 255 is for the IP address owner. The IP address owner in a VRRP group always has a running priority of 255 and acts as the master as long as it operates correctly.

Examples

# Set the priority of the switch to 150 in VRRP group 1 on VLAN-interface 2.

<Sysname> system-view

[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 priority 150

Related commands

display vrrp ipv6

### vrrp ipv6 vrid shutdown

Use vrrp ipv6 vrid shutdown to disable an IPv6 VRRP group.

Use undo vrrp ipv6 vrid shutdown to enable an IPv6 VRRP group.

Syntax

vrrp ipv6 vrid virtual-router-id shutdown

undo vrrp ipv6 vrid virtual-router-id shutdown

Default

An IPv6 VRRP group is enabled.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

Usage guidelines

You can use this command to temporarily disable an IPv6 VRRP group. After this command is configured, the VRRP group stays in Initialize state, and its configurations remain unchanged. You can change the configuration of the VRRP group, and your changes take effect when you enable the VRRP group again.

Examples

# Disable IPv6 VRRP group 1.

<Sysname> system-view

[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 shutdown

### vrrp ipv6 vrid timer advertise

Use vrrp ipv6 vrid timer advertise to set the interval at which the master in an IPv6 VRRP group sends VRRP advertisements.

Use undo vrrp ipv6 vrid timer advertise to restore the default.

Syntax

vrrp ipv6 vrid virtual-router-id timer advertise adver-interval

undo vrrp ipv6 vrid virtual-router-id timer advertise

Default

The master in an IPv6 VRRP group sends VRRP advertisements at an interval of 100 centiseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

adver-interval: Specifies an interval for the master in the specified IPv6 VRRP group to send VRRP advertisements, in the range of 100 to 4095 centiseconds.

Usage guidelines

The master in an IPv6 VRRP group periodically sends VRRP advertisements to declare its presence. You can use this command to set the interval at which the master sends VRRP advertisements.

As a best practice to maintain system stability, set the VRRP advertisement interval to be greater than 100 centiseconds.

The routers in an IPv6 VRRP group can have different intervals for sending VRRP advertisements. The master in the VRRP group sends VRRP advertisements at the specified interval and carries the interval attribute in the advertisements. After a backup receives the advertisement, it records the interval in the advertisement. If the backup does not receive any VRRP advertisement when the timer (3 × VRRP advertisement sending interval + Skew\_Time) expires, it regards the master as failed and takes over.

Large network traffic might disable a backup from receiving VRRP advertisements from the master within the specified timer and trigger an unexpected master switchover. To solve this problem, you can use this command to configure a larger interval.

Examples

# Configure the master in IPv6 VRRP group 1 to send VRRP advertisements at an interval of 500 centiseconds.

<Sysname> system-view

[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 timer advertise 500

Related commands

display vrrp ipv6

### vrrp ipv6 vrid track

Use vrrp ipv6 vrid track to associate an IPv6 VRRP group or the VFs in an IPv6 VRRP group with a track entry.

Use undo vrrp ipv6 vrid track to remove the association between an IPv6 VRRP group or the VFs in an IPv6 VRRP group and a track entry.

Syntax

vrrp ipv6 vrid virtual-router-id track track-entry-number { forwarder-switchover member-ip ipv6-address | priority reduced [ priority-reduced ] | switchover | weight reduced [ weight-reduced ] }

undo vrrp ipv6 vrid virtual-router-id track [ track-entry-number ] [ forwarder-switchover | priority reduced | switchover | weight reduced ] ]

Default

An IPv6 VRRP group and the VFs in an IPv6 VRRP group are not associated with any track entries.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group number in the range of 1 to 255.

track-entry-number: Specifies a track entry by its number in the range of 1 to 1024.

forwarder-switchover member-ip ipv6-address: Enables the LVF on the router to take over the role of the AVF at the specified IPv6 address immediately after the specified track entry changes to the Negative state. The ipv6-address argument specifies the IPv6 address of a member router. You can use the display vrrp ipv6 verbose command to view the IPv6 addresses of the members.

priority reduced [ priority-reduced ]: Reduces the priority of the router in the VRRP group by the specified value when the state of the specified track entry changes to Negative. The value range for the priority-reduced argument is 1 to 255, and the default value is 10.

switchover: Enables the router in backup state to take over as the master immediately after the specified track entry changes to the Negative state.

weight reduced [ weight-reduced ]: Reduces the weight of all VFs on the router in the VRRP group by the specified value when the state of the specified track entry changes to Negative. The value range for the weight-reduced argument is 1 to 255, and the default value is 30.

Usage guidelines

When the associated track entry changes to the Negative state, one of the following events occurs depending on your configuration:

* The priority of the router in the VRRP group decreases by a specified value.
* The weight of VFs decreases by a specified value.
* The router immediately takes over as the master if it is a backup.
* The LVF on the router immediately takes over the role of the AVF at the specified IPv6 address.

When the track entry changes from Negative to Positive or NotReady, one of the following events occurs:

* The router automatically restores its priority or VF weight.
* The failed master router becomes the master again.
* The failed AVF becomes active again.

Before executing this command, create an IPv6 VRRP group on the interface and assign a virtual IPv6 address to the IPv6 VRRP group.

You can create a track entry by using the track command before or after you associate it with an IPv6 VRRP group or the VFs in an IPv6 VRRP group. For more information about configuring track entries, see High Availability Configuration Guide.

If no track entry is specified, the undo vrrp ipv6 vrid track command removes all associations between track entries and the IPv6 VRRP group or VFs in the IPv6 VRRP group.

The vrrp ipv6 vrid track priority reduced command and the vrrp ipv6 vrid track switchover command do not take effect on an IP address owner. If you configure the command on an IP address owner, the configuration takes effect after the router changes to be a non-IP address owner.

The following parameters take effect only when the IPv6 VRRP group is operating in load balancing mode:

* The forwarder-switchover member-ip ip-address option.
* The weight reduced weight-reduced option.
* The weight reduced keyword.

The weight of a VF is 255, and its lower limit of failure is 10.

When the weight of a VF owner is higher than or equal to the lower limit of failure, its priority is always 255. The priority does not change with the weight. When the upstream link of the VF owner fails, an LVF must take over as the AVF. The switchover happens when the weight of the VF owner drops below the lower limit of failure. This requires that the reduced weight for the VF owner be higher than 245.

Examples

# Associate IPv6 VRRP group 1 on VLAN-interface 2 with track entry 1 and decrease the router priority by 50 when the state of track entry 1 changes to Negative.

<Sysname> system-view

[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 track 1 priority reduced 50

# Associate the VFs of IPv6 VRRP group 1 on VLAN-interface 2 with track entry 1. Enable the LVF to take over the role of the AVF at the IPv6 address of 1::3 immediately when the state of track entry 1 changes to Negative.

<Sysname> system-view

[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 track 1 forwarder-switchover member-ip 1::3

# Associate the VFs of IPv6 VRRP group 1 on VLAN-interface 2 with track entry 1. Decrease the weight of all VFs on the router in the VRRP group by 50 when the state of track entry 1 changes to Negative.

<Sysname> system-view

[Sysname] interface vlan-interface2

[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 track 1 weight reduced 50

Related commands

display vrrp ipv6

1. Release 3208

This release has the following changes:

* New feature: MAC address information display for 802.1X users in 802.1X VLANs of a specific type
* New feature: Authorization CAR action for an ISP domain
* New feature: 802.1X client
* New feature: MAC address information display for MAC authentication users in MAC authentication VLANs of a specific type
* Modified feature: Configuring the hash seed for global link aggregation load sharing
* Modified feature: Specifying a RADIUS or HWTACACS server

# New feature: MAC address information display for 802.1X users in 802.1X VLANs of a specific type

## Displaying MAC address information of 802.1X users in 802.1X VLANs of a specific type

Execute display commands in any view.

| Task | Command |
| --- | --- |
| Display MAC address information of 802.1X users in 802.1X VLANs of a specific type. | display dot1x mac-address { auth-fail-vlan | critical-vlan | guest-vlan } [ interface interface-type interface-number ] |

## Command reference

### display dot1x mac-address

Use display dot1x mac-address to display MAC address information of 802.1X users in 802.1X VLANs of a specific type.

Syntax

display dot1x mac-address { auth-fail-vlan | critical-vlan | guest-vlan } [ interface interface-type interface-number ]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

auth-fail-vlan: Specifies the 802.1X Auth-Fail VLAN.

critical-vlan: Specifies the 802.1X critical VLAN.

guest-vlan: Specifies the 802.1X guest VLAN.

interface interface-type interface-number: Specifies a port by its type and number. If you do not specify a port, this command displays MAC address information of 802.1X users in the specified 802.1X VLAN on all ports.

Usage guidelines

This command displays rough statistics. It might not fully display the specified information when a large number of 802.1X users perform authentication frequently.

Examples

# Display MAC address information of 802.1X users in the 802.1X Auth-Fail VLAN on all ports.

<Sysname> display dot1x mac-address auth-fail-vlan

Total MAC addresses: 10

Interface: Auth-Fail VLAN: 3 Aging time: N/A

MAC addresses: 8

0800-2700-9427 0800-2700-2341 0800-2700-2324 0800-2700-2351

0800-2700-5627 0800-2700-2251 0800-2700-8624 0800-2700-3f51

Interface: Auth-Fail VLAN: 5 Aging time: 30 sec

MAC addresses: 2

0801-2700-9427 0801-2700-2341

Command output

| Field | Description |
| --- | --- |
| Total MAC addresses | Total number of MAC addresses in the specified VLAN on the specified port or all ports. |
| Interface | Access port of 802.1X users. |
| Type VLAN | VLAN information for 802.1X users. The Type argument has the following values:   * + - * Auth-Fail VLAN.       * Critical VLAN.       * Guest VLAN. |
| Aging time | MAC address aging time in seconds.  This field displays N/A if the MAC addresses do not age out. |
| MAC addresses | Number of matching MAC addresses on a port. |
| xxxx-xxxx-xxxx | MAC address. |

Related commands

dot1x auth-fail vlan

dot1x critical vlan

dot1x guest-vlan

# New feature: Authorization CAR action for an ISP domain

## Configuring an authorization CAR action for an ISP domain

The CAR action attribute controls the traffic flows of authenticated users.

If the server does not authorize a CAR action to an authenticated user, the device assigns the domain's authorization CAR action to the user.

For portal users, you can configure an authorization CAR action in their preauthentication domain to control their traffic flows before they pass authentication.

To configure an authorization CAR action for an ISP domain:

| Step | Command | Remarks |
| --- | --- | --- |
| 1. Enter system view. | system-view | N/A |
| 1. Enter ISP domain view. | domain isp-name | N/A |
| 1. Configure an authorization CAR action for the ISP domain. | authorization-attribute car inbound cir committed-information-rate [ pir peak-information-rate ] outbound cir committed-information-rate [ pir peak-information-rate ] | By default, no authorization CAR action is configured for an ISP domain. |

## Command reference

### authorization-attribute car

Use authorization-attribute car to configure an authorization CAR action for an ISP domain.

Use undo authorization-attribute car to restore the default.

Syntax

authorization-attribute car inbound cir committed-information-rate [ pir peak-information-rate ] outbound cir committed-information-rate [ pir peak-information-rate ]

undo authorization-attribute car

Default

No authorization CAR action is configured for an ISP domain.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

inbound: Specifies the upload rate of users.

outbound: Specifies the download rate of users.

cir committed-information-rate: Specifies the committed information rate in kbps, in the range of 1 to 4194303.

pir peak-information-rate: Specifies the peak information rate in kbps, in the range of 1 to 4194303. If you do not specify this option, the CAR action does not restrict users by peak information rate.

Usage guidelines

If the server does not authorize a CAR action to an authenticated user, the device assigns the domain's authorization CAR action to the user.

For portal users, you can configure an authorization CAR action in their preauthentication domain to control their traffic flows before they pass authentication.

Examples

# Configure an authorization CAR action for ISP domain test. In the CAR action attribute, the CIR for upload rate of users is 1111 kbps, and the CIR for download rate of users is 2222 kbps.

<Sysname> system-view

[Sysname] domain test

[Sysname-isp-test] authorization-attribute car inbound cir 1111 outbound cir 2222

Related commands

display domain

# New feature: 802.1X client

## Configuring 802.1X client

As shown in Figure 1, the 802.1X client feature allows the access device to act as the supplicant in the 802.1X architecture. For information about the 802.1X architecture, see "802.1X overview."

802.1X client network diagram



### 802.1X client configuration task list

| Tasks at a glance |
| --- |
| (Required.) Enabling the 802.1X client feature |
| (Required.) Configuring an 802.1X client username and password |
| (Optional.) Configuring an 802.1X client MAC address |
| (Required.) Specifying an 802.1X client EAP authentication method |
| (Optional.) Configuring an 802.1X client anonymous identifier |
| (Optional.) Specifying an SSL client policy |

### Enabling the 802.1X client feature

Before enabling the 802.1X client feature, make sure you have configured 802.1X authentication on the authenticator. For information about 802.1X configuration, see "Configuring 802.1X."

To enable the 802.1X client feature on an interface:

| Step | Command | Remarks |
| --- | --- | --- |
| 1. Enter system view. | system-view | N/A |
| 1. Enter Ethernet interface view. | interface interface-type interface-number | N/A |
| 1. Enable the 802.1X client feature. | dot1x supplicant enable | By default, the 802.1X client feature is disabled. |

### Configuring an 802.1X client username and password

An 802.1X client-enabled device uses the configured username and password for 802.1X authentication.

Make sure the username and password configured on the device is consistent with the username and password configured on the authentication server. If any inconsistency occurs, the device cannot pass 802.1X authentication to access the network.

To configure an 802.1X client username and password on an interface:

| Step | Command | Remarks |
| --- | --- | --- |
| 1. Enter system view. | system-view | N/A |
| 1. Enter Ethernet interface view. | interface interface-type interface-number | N/A |
| 1. Configure an 802.1X client username. | dot1x supplicant username username | By default, no 802.1X client username exists. |
| 1. Set an 802.1X client password. | dot1x supplicant password { cipher | simple } string | By default, no 802.1X client password exists. |

### Configuring an 802.1X client MAC address

The authenticator adds the MAC address of an authenticated 802.1X client to the MAC address table and then assigns access rights to the client.

You can use either of the following methods to configure a unique MAC address for each interface:

* Execute the mac-address command in Ethernet interface view. For information about this command, see Layer 2—LAN Switching Command Reference.
* Configure an 802.1X client MAC address.

To configure an 802.1X client MAC address on an interface:

| Step | Command | Remarks |
| --- | --- | --- |
| 1. Enter system view. | system-view | N/A |
| 1. Enter Ethernet interface view. | interface interface-type interface-number | N/A |
| 1. Configure an 802.1X client MAC address. | dot1x supplicant mac-address mac-address | By default, an Ethernet interface uses the interface's MAC address for 802.1X client authentication. If the interface's MAC address is unavailable, the interface uses the device's MAC address for 802.1X client authentication. |

### Specifying an 802.1X client EAP authentication method

An 802.1X client-enabled device supports the following EAP authentication methods:

* MD5-Challenge.
* PEAP-MSCHAPv2.
* PEAP-GTC.
* TTLS-MSCHAPv2.
* TTLS-GTC.

An 802.1X authenticator supports both the EAP relay and EAP termination modes. Support of the EAP authentication methods for the two modes varies.

* The MD5-Challenge EAP authentication supports both modes.
* Other EAP authentication methods support only the EAP relay mode.

For information about EAP relay and EAP termination, see "Configuring 802.1X."

To specify an 802.1X client EAP authentication method on an interface:

| Step | Command | Remarks |
| --- | --- | --- |
| 1. Enter system view. | system-view | N/A |
| 1. Enter Ethernet interface view. | interface interface-type interface-number | N/A |
| 1. Specify an 802.1X client EAP authentication method. | dot1x supplicant eap-method { md5 | peap-gtc | peap-mschapv2 | ttls-gtc | ttls-mschapv2 } | By default, an 802.1X client-enabled interface uses the MD5-Challenge EAP authentication.  Make sure the specified 802.1X client EAP authentication method is supported by the authentication server. |

### Configuring an 802.1X client anonymous identifier

At the first authentication phase, packets sent to the authenticator are not encrypted. The use of an 802.1X client anonymous identifier prevents the 802.1X client username from being disclosed at the first phase. The 802.1X client-enabled device sends the anonymous identifier to the authenticator instead of the 802.1X client username. The 802.1X client username will be sent to the authenticator in encrypted packets at the second phase.

If no 802.1X client anonymous identifier is configured, the device sends the 802.1X client username at the first authentication phase.

The configured 802.1X client anonymous identifier takes effect only if one of the following EAP authentication methods is used:

* PEAP-MSCHAPv2.
* PEAP-GTC.
* TTLS-MSCHAPv2.
* TTLS-GTC.

If the MD5-Challenge EAP authentication is used, the configured 802.1X client anonymous identifier does not take effect. The device uses the 802.1X client username at the first authentication phase.

Do not configure the 802.1X client anonymous identifier if the vendor-specific authentication server cannot identify anonymous identifiers.

To configure an 802.1X client anonymous identifier on an interface:

| Step | Command | Remarks |
| --- | --- | --- |
| 1. Enter system view. | system-view | N/A |
| 1. Enter Ethernet interface view. | interface interface-type interface-number | N/A |
| 1. Configure an 802.1X client anonymous identifier. | dot1x supplicant anonymous identify identifier | By default, no 802.1X client anonymous identifier exists. |

### Specifying an SSL client policy

If the PEAP-MSCHAPv2, PEAP-GTC, TTLS-MSCHAPv2, or TTLS-GTC authentication is used, the 802.1X client authentication process is as follows:

* The first phase—The device acts as an SSL client to negotiate with the SSL server.

The SSL client uses the SSL parameters defined in the specified SSL client policy to establish a connection with the SSL server for negotiation. The SSL parameters include a PKI domain, supported cipher suites, and the SSL version. For information about SSL client policy configuration, see "Configuring SSL."

* The second phase—The device uses the negotiated result to encrypt and transmit the interchanged authentication packets.

If the MD5-Challenge authentication is used, the device does not use an SSL client policy during the authentication process.

To specify an SSL client policy on an interface:

| Step | Command | Remarks |
| --- | --- | --- |
| 1. Enter system view. | system-view | N/A |
| 1. Enter Ethernet interface view. | interface interface-type interface-number | N/A |
| 1. Specify an SSL client policy. | dot1x supplicant ssl-client-policy policy-name | By default, an 802.1X client-enabled interface uses the default SSL client policy. |

### Displaying and maintaining 802.1X client

Execute display commands in any view.

| Task | Command |
| --- | --- |
| Display 802.1X client information. | display dot1x supplicant [ interface interface-type interface-number ] |

## 802.1X client commands

### display dot1x supplicant

Use display dot1x supplicant to display 802.1X client authentication information.

Syntax

display dot1x supplicant [ interface interface-type interface-number ]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays 802.1X client authentication information for all interfaces.

Examples

# Display 802.1X client authentication information on .

<Sysname> display dot1x supplicant interface

Username : aaa

EAP method : PEAP-MSCHAPv2

Dot1x supplicant : Enabled

Anonymous identifier : bbb

SSL client policy : policy\_1

FSM state : Init

EAPOL-Start packets : 0

Command output

| Field | Description |
| --- | --- |
| Username | 802.1X client username. |
| EAP method | 802.1X client EAP authentication method:   * + - * MD5.       * PEAP-GTC.       * PEAP-MSCHAPv2.       * TTLS-GTC.       * TTLS-MSCHAPv2. |
| Dot1x supplicant | Status of the 802.1X client feature:   * + - * Enabled.       * Disabled. |
| Anonymous identifier | 802.1X client anonymous identifier. |
| SSL client policy | SSL client policy used by the 802.1X client feature. |
| FSM state | 802.1X client authentication state:   * + - * Init—The authentication process starts.       * Connecting—The 802.1X client is connecting to the authenticator.       * Authenticating—The 802.1X client is being authenticated.       * Authenticated—The 802.1X client has been authenticated.       * Held—The 802.1X client is waiting for authentication. |
| EAPOL-Start packets | Number of sent EAPOL-Start packets. |

### dot1x supplicant anonymous identify

Use dot1x supplicant anonymous identify to configure an 802.1X client anonymous identifier.

Use undo dot1x supplicant anonymous identify to restore the default.

Syntax

dot1x supplicant anonymous identify identifier

undo dot1x supplicant anonymous identify

Default

No 802.1X client anonymous identifier exists.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

identifier: Specifies an 802.1X client anonymous identifier, a case-sensitive string of 1 to 253 characters.

Usage guidelines

At the first authentication phase, packets sent to the authenticator are not encrypted. The use of an 802.1X client anonymous identifier prevents the 802.1X client username from being disclosed at the first phase. The 802.1X client-enabled device sends the anonymous identifier to the authenticator instead of the 802.1X client username. The 802.1X client username will be sent to the authenticator in encrypted packets at the second phase.

If no 802.1X client anonymous identifier is configured, the device sends the 802.1X client username in the first phase.

The configured 802.1X client anonymous identifier takes effect only if one of the following EAP authentication methods is used:

* PEAP-MSCHAPv2.
* PEAP-GTC.
* TTLS-MSCHAPv2.
* TTLS-GTC.

If the MD5-Challenge EAP authentication is used, the configured 802.1X client anonymous identifier does not take effect. The device uses the 802.1X client username at the first authentication phase.

Do not configure the 802.1X client anonymous identifier if the vendor-specific authentication server cannot identify anonymous identifiers.

Examples

# Configure the 802.1X client anonymous identifier as bbb on a port.

<Sysname> system-view

[Sysname] interface

[Sysname-] dot1x supplicant anonymous identify bbb

Related commands

display dot1x supplicant

dot1x supplicant enable

dot1x supplicant username

### dot1x supplicant eap-method

Use dot1x supplicant eap-method to specify an 802.1X client EAP authentication method.

Use undo dot1x supplicant eap-method to restore the default.

Syntax

dot1x supplicant eap-method { md5 | peap-gtc | peap-mschapv2 | ttls-gtc | ttls-mschapv2 }

undo dot1x supplicant eap-method

Default

The MD5-Challenge authentication is used as the 802.1X client EAP authentication method.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

md5: Specifies the MD5-challenge EAP authentication method.

peap-gtc: Specifies the PEAP-GTC EAP authentication method.

peap-mschapv2: Specifies the PEAP-MSCHAPv2 EAP authentication method

ttls-gtc: Specifies the TTLS-GTC EAP authentication method.

ttls-mschapv2: Specifies the TTLS-MSCHAPv2 EAP authentication method.

Usage guidelines

Make sure the specified 802.1X client EAP authentication method is supported by the authentication server.

Examples

# Specify PEAP-GTC as the 802.1X client EAP authentication method on a port.

<Sysname> system-view

[Sysname] interface

[Sysname-] dot1x supplicant eap-method peap-gtc

Related commands

display dot1x supplicant

dot1x supplicant enable

### dot1x supplicant enable

Use dot1x supplicant enable to enable the 802.1X client feature.

Use undo dot1x supplicant enable to disable the 802.1X client feature.

Syntax

dot1x supplicant enable

undo dot1x supplicant enable

Default

The 802.1X client feature is disabled.

Views

Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

Make sure you have configured 802.1X authentication on the authenticator before you use this command.

Examples

# Enable the 802.1X client feature on a port.

<Sysname> system-view

[Sysname] interface

[Sysname-] dot1x supplicant enable

Related commands

display dot1x supplicant

### dot1x supplicant mac-address

Use dot1x supplicant mac-address to configure an 802.1X client MAC address used for 802.1X client authentication.

Use undo dot1x supplicant mac-address to restore the default.

Syntax

dot1x supplicant mac-address mac-address

undo dot1x supplicant mac-address

Default

An Ethernet interface uses the interface's MAC address for 802.1X client authentication. If the interface's MAC address is unavailable, the interface uses the device's MAC address for 802.1X client authentication.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a MAC address in the format of H-H-H, excluding multicast, all-zero, and all-F MAC addresses. When entering a MAC address, you can omit the leading zeros in each H section. For example, enter f-e2-1 for 000f-00e2-0001.

Usage guidelines

When the device acts as an 802.1X client and has multiple Ethernet interfaces to seek MACsec protection, each interface requires a unique MAC address to pass 802.1X client authentication.

You can use either of the following methods to configure a unique MAC address for each 802.1X client-enabled interface:

* Execute the mac-address command in Ethernet interface view.
* Execute the dot1x supplicant mac-address command.

For information about MACsec, see Security Configuration Guide.

Examples

# Configure the 802.1X client MAC address for 802.1X client authentication as 0001-0001-0001.

<Sysname> system-view

[Sysname] interface

[Sysname-] dot1x supplicant mac-address 1-1-1

### dot1x supplicant password

Use dot1x supplicant password to set an 802.1X client password.

Use undo dot1x supplicant password to restore the default.

Syntax

dot1x supplicant password { cipher | simple } string

undo dot1x supplicant password

Default

No 802.1X client password exists.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 127 characters. Its encrypted form is a case-sensitive string of 1 to 201 characters.

Examples

# Set the 802.1X client password to 123456 in plaintext form on a port.

<Sysname> system-view

[Sysname] interface

[Sysname-] dot1x supplicant password simple 123456

Related commands

display dot1x supplicant

dot1x supplicant enable

### dot1x supplicant ssl-client-policy

Use dot1x supplicant ssl-client-policy to specify an SSL client policy for an 802.1X client-enabled device.

Use undo dot1x supplicant ssl-client-policy to restore the default.

Syntax

dot1x supplicant ssl-client-policy policy-name

undo dot1x supplicant ssl-client-policy policy-name

Default

An 802.1X client-enabled device uses the default SSL client policy.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

policy-name: Specifies an SSL client policy by its name, a case-insensitive string of 1 to 31 characters. Make sure the specified SSL client policy already exists.

Usage guidelines

If the PEAP-MSCHAPv2, PEAP-GTC, TTLS-MSCHAPv2, or TTLS-GTC authentication is used, the 802.1X client authentication process is as follows:

* The first phase—The device acts as an SSL client to negotiate with the SSL server.

The SSL client uses the SSL parameters specified in the specified SSL client policy to establish a connection to the SSL server for negotiation. The SSL parameters include a PKI domain, supported cipher suites, and the SSL version. For information about SSL client policies, see Security Configuration Guide.

* The second phase—The device uses the negotiated result to encrypt and transmit the interchanged authentication packets.

If the MD5-Challenge authentication is used, the device does not use an SSL client policy during the authentication process.

Examples

#Specify SSL client policy policy\_1 to be used by an 802.1X client-enabled device on .

<Sysname> system-view

[Sysname] interface

[Sysname-] dot1x supplicant ssl-client-policy policy\_1

Related commands

display dot1x supplicant

dot1x supplicant enable

ssl client-policy

### dot1x supplicant username

Use dot1x supplicant username to configure an 802.1X client username.

Use undo dot1x supplicant username to restore the default.

Syntax

dot1x supplicant username username

undo dot1x supplicant username

Default

No 802.1X client username exists.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

username: Specifies the 802.1X client username, a case-sensitive string of 1 to 253 characters.

Usage guidelines

802.1X client usernames can include domain names. The supported domain name delimiters include the at sign (@), backslash (\), dot (.), and forward slash (/). Usernames that include domain names can use the format of username@domain-name, domain-name\username, username.domain-name, or username/domain-name.

If you want to use backslash (\) as the domain name delimiter, you must enter the escape character (\) along with the backslash (\) sign.

If a username string includes multiple configured delimiters, the device takes the rightmost delimiter in the username string as the domain name delimiter. For more information about the domain name delimiters, see the dot1x domain-delimiter command.

Examples

# Configure the 802.1X client username as aaa on a port.

<Sysname> system-view

[Sysname] interface

[Sysname-] dot1x supplicant username aaa

Related commands

display dot1x supplicant

dot1x domain-delimiter

dot1x supplicant enable

# New feature: MAC address information display for MAC authentication users in MAC authentication VLANs of a specific type

## Displaying MAC address information of MAC authentication users in MAC authentication VLANs of a specific type

Execute display commands in any view.

| Task | Command |
| --- | --- |
| Display MAC address information of MAC authentication users in MAC authentication VLANs of a specific type. | display mac-authentication mac-address { critical-vlan | guest-vlan } [ interface interface-type interface-number ] |

## Command reference

### display mac-authentication mac-address

Use display mac-authentication mac-address to display MAC address information of MAC authentication users in MAC authentication VLANs of a specific type.

Syntax

display mac-authentication mac-address { critical-vlan | guest-vlan } [ interface interface-type interface-number ]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

critical-vlan: Specifies the MAC authentication critical VLAN.

guest-vlan: Specifies the MAC authentication guest VLAN.

interface interface-type interface-number: Specifies a port by its type and number. If you do not specify a port, this command displays MAC address information of MAC authentication users in the specified MAC authentication VLAN on all ports.

Usage guidelines

This command displays rough statistics. It might not fully display the specified information when a large number of MAC authentication users perform authentication frequently.

Examples

# Display MAC address information of MAC authentication users in the MAC authentication guest VLAN on all ports.

<Sysname> display mac-authentication mac-address guest-vlan

Total MAC addresses: 10

Interface: Guest VLAN: 3 Aging time: N/A

MAC addresses: 8

0800-2700-9427 0800-2700-2341 0800-2700-2324 0800-2700-2351

0800-2700-5627 0800-2700-2251 0800-2700-8624 0800-2700-3f51

Interface: Guest VLAN: 5 Aging time: 30 sec

MAC addresses: 2

0801-2700-9427 0801-2700-2341

Command output

| Field | Description |
| --- | --- |
| Total MAC addresses | Total number of MAC addresses in the specified VLAN on the specified port or all ports. |
| Interface | Access port of MAC authentication users. |
| Type VLAN | VLAN information for MAC authentication users. The Type argument has the following values:   * + - * Critical VLAN.       * Guest VLAN. |
| Aging time | MAC address aging time in seconds.  This field displays N/A if the MAC addresses do not age out. |
| MAC addresses | Number of matching MAC addresses on a port. |
| xxxx-xxxx-xxxx | MAC address. |

Related commands

mac-authentication critical vlan

mac-authentication guest-vlan

# Modified feature: Configuring the hash seed for global link aggregation load sharing

## Feature change description

The value range for the hash seed was modified for global link aggregation load sharing.

## Command changes

### Modified command: link-aggregation global load-sharing seed

Syntax

link-aggregation global load-sharing seed seed-number

undo link-aggregation global load-sharing seed

Views

System view

Change description

Before modification: The value range for the seed-number argument is 1 to 7FFFFFFF.

After modification: The value range for the seed-number argument is 1 to FFFFFFFF.

# Modified feature: Specifying a RADIUS or HWTACACS server

## Feature change description

Support for specifying a RADIUS or HWTACACS server by its host name was added.

## Command changes

### Modified commands in RADIUS scheme view: primary accounting, primary authentication, secondary accounting, secondary authentication, state secondary

Old syntax

primary accounting { ipv4-address | ipv6 ipv6-address } [ port-number | key { cipher | simple } string | weight weight-value ] \*

primary authentication { ipv4-address | ipv6 ipv6-address } [ port-number | key { cipher | simple } string | test-profile profile-name | weight weight-value ] \*

secondary accounting { ipv4-address | ipv6 ipv6-address } [ port-number | key { cipher | simple } string | weight weight-value ] \*

undo secondary accounting [ { ipv4-address | ipv6 ipv6-address } [ port-number ] \* ]

secondary authentication { ipv4-address | ipv6 ipv6-address } [ port-number | key { cipher | simple } string | test-profile profile-name | weight weight-value ] \*

undo secondary authentication [ { ipv4-address | ipv6 ipv6-address } [ port-number ] \* ]

state secondary { accounting | authentication } [ { ipv4-address | ipv6 ipv6-address } [ port-number ] \* ] { active | block }

New syntax

primary accounting { host-name | ipv4-address | ipv6 ipv6-address } [ port-number | key { cipher | simple } string | weight weight-value ] \*

primary authentication { host-name | ipv4-address | ipv6 ipv6-address } [ port-number | key { cipher | simple } string | test-profile profile-name | weight weight-value ] \*

secondary accounting { host-name | ipv4-address | ipv6 ipv6-address } [ port-number | key { cipher | simple } string | weight weight-value ] \*

undo secondary accounting [ { host-name | ipv4-address | ipv6 ipv6-address } [ port-number ] \* ]

secondary authentication { host-name | ipv4-address | ipv6 ipv6-address } [ port-number | key { cipher | simple } string | test-profile profile-name | weight weight-value ] \*

undo secondary authentication [ { host-name | ipv4-address | ipv6 ipv6-address } [ port-number ] \* ]

state secondary { accounting | authentication } [ { host-name | ipv4-address | ipv6 ipv6-address } [ port-number ] \* ] { active | block }

Views

RADIUS scheme view

Change description

The host-name argument was added. This argument specifies a RADIUS server by its host name.

### Modified commands in HWTACACS scheme view: primary accounting, primary authentication, primary authorization, secondary accounting, secondary authentication, secondary authorization

Old syntax

primary accounting { ipv4-address | ipv6 ipv6-address } [ port-number | key { cipher | simple } string | single-connection ] \*

primary authentication { ipv4-address | ipv6 ipv6-address } [ port-number | key { cipher | simple } string | single-connection ] \*

primary authorization { ipv4-address | ipv6 ipv6-address } [ port-number | key { cipher | simple } string | single-connection ] \*

secondary accounting { ipv4-address | ipv6 ipv6-address } [ port-number | key { cipher | simple } string | single-connection ] \*

undo secondary accounting [ { ipv4-address | ipv6 ipv6-address } [ port-number ] \* ]

secondary authentication { ipv4-address | ipv6 ipv6-address } [ port-number I key { cipher | simple } string | single-connection ] \*

undo secondary authentication [ { ipv4-address | ipv6 ipv6-address } [ port-number ] \* ]

secondary authorization { ipv4-address | ipv6 ipv6-address } [ port-number I key { cipher | simple } string | single-connection ] \*

undo secondary authorization [ { ipv4-address | ipv6 ipv6-address } [ port-number ] \* ]

New syntax

primary accounting { host-name | ipv4-address | ipv6 ipv6-address } [ port-number | key { cipher | simple } string | single-connection ] \*

primary authentication { host-name | ipv4-address | ipv6 ipv6-address } [ port-number | key { cipher | simple } string | single-connection ] \*

primary authorization { host-name | ipv4-address | ipv6 ipv6-address } [ port-number | key { cipher | simple } string | single-connection ] \*

secondary accounting { host-name | ipv4-address | ipv6 ipv6-address } [ port-number | key { cipher | simple } string | single-connection ] \*

undo secondary accounting [ { host-name | ipv4-address | ipv6 ipv6-address } [ port-number ] \* ]

secondary authentication { host-name | ipv4-address | ipv6 ipv6-address } [ port-number I key { cipher | simple } string | single-connection ] \*

undo secondary authentication [ { host-name | ipv4-address | ipv6 ipv6-address } [ port-number ] \* ]

secondary authorization { host-name | ipv4-address | ipv6 ipv6-address } [ port-number I key { cipher | simple } string | single-connection ] \*

undo secondary authorization [ { host-name | ipv4-address | ipv6 ipv6-address } [ port-number ] \* ]

Views

HWTACACS scheme view

Change description

The host-name argument was added. This argument specifies an HWTACACS server by its host name.

1. Release 3207

This release has the following changes:

* New features: Fundamentals features
* New features: IRF features
* New features: Layer 2—LAN switching features
* New features: Layer 3—IP services features
* New features: Layer 3—IP routing features
* New features: IP multicast features
* New features: ACL and QoS features
* New features: Security features
* New features: High availability features
* New features: Network management and monitoring features
* New features: OpenFlow features
* Modified feature: Configuring a command alias
* Modified feature: Displaying command aliases
* Modified feature: Configuring a hotkey
* Modified feature: Maximum length for a configuration file name
* Modified feature: BFD MAD collision handling process
* Modified feature: Support for commands on IRF physical interfaces
* Modified feature: Excluding a service interface from the IRF MAD shutdown action by the system
* Modified feature: Displaying information about packets dropped on an interface
* Modified feature: Displaying MAC address move records
* Modified feature: MAC address move notifications
* Modified feature: Setting the voice VLAN aging timer
* Modified feature: Creating a VLAN
* Modified feature: Displaying history about ports that are blocked by spanning tree protection features
* Modified feature: Setting the LLDP frame transmission interval
* Modified feature: Displaying ARP entries
* Modified feature: Displaying the aging time of dynamic ARP entries
* Modified feature: Default source IP address in packets relayed to the DHCP server
* Modified feature: Specifying gateways on the DHCP server for DHCP clients
* Modified feature: Displaying information for DHCP snooping trusted ports
* Modified feature: Setting the MTU of IPv4 packets sent over an interface
* Modified feature: Setting the TCP buffer size
* Modified feature: Configuring prefix to be advertised in RA messages
* Modified feature: Setting the MTU of IPv6 packets sent over an interface
* Modified feature: Displaying PBR configuration
* Modified feature: Displaying IPv6 PBR configuration
* Modified feature: Creating an ACL
* Modified feature: Copying an ACL to create a new ACL
* Modified feature: Displaying ACL configuration and match statistics
* Modified feature: Displaying packet filtering statistics
* Modified feature: Displaying accumulated packet filtering statistics for an ACL
* Modified feature: Displaying ACL application details for packet filtering
* Modified feature: Applying an ACL to an interface for packet filtering
* Modified feature: Specify the applicable scope of packet filtering on a VLAN interface
* Modified feature: Clearing statistics for ACLs
* Modified feature: Clearing the packet filtering statistics and accumulated statistics for an ACL
* Modified feature: Specifying an ACL match criterion
* Modified feature: Displaying predefined control plane QoS policies of cards
* Modified feature: Length range for an ISP domain
* Modified feature: Displaying local user configuration
* Modified feature: Displaying user group configuration
* Modified feature: Enabling the RADIUS server load sharing feature
* Modified feature: Setting the real-time accounting interval
* Modified feature: Displaying 802.1X information
* Modified feature: Port-specific mandatory 802.1X authentication domain
* Modified feature: Removing users from the MAC authentication critical VLAN on a port
* Modified feature: Port security's limit on the number of secure MAC addresses on a port
* Modified feature: Enabling the SSH server to support SSH1 clients
* Modified feature: Creating an SSH user and specifying the service type and authentication method
* Modified feature: Predefined user roles for SSH and FTP client commands
* Modified feature: Setting the number of ARP blackhole route probes for each unresolved IP address
* Modified feature: Displaying information about SNMPv1 or SNMPv2c communities
* Modified feature: Displaying information about SNMP groups
* Modified feature: Displaying SNMPv3 user information
* Modified feature: Configuring an SNMPv1 or SNMPv2c community
* Modified feature: Creating an SNMP group
* Modified feature: Creating an SNMPv1 or SNMPv2c user
* Modified feature: Creating an SNMPv3 user
* Modified feature: Configuration locking BY NETCONF
* Modified feature: Value range for the interval for an OpenFlow instance to reconnect to a controller
* Removed features

# New features: Fundamentals features

Table 1 describes the fundamental features added in this software version. For more information about the features and commands, see HPE 5130 EI Switch Series Fundamentals Configuration Guide-R3207 and HPE 5130 EI Switch Series Fundamentals Command Reference-R3207.

Fundamentals features added in version R3207

| Feature | Command changes |
| --- | --- |
| CLI: Repeating commands in the command history buffer for the current CLI session | The repeat [ number ] [ count times ] [ delay seconds ] command was added. |
| Login management: Associating a Telnet redirect listening port with an IP address | The ip alias command was added. |
| Login management: Specifying an ACL by its name to apply the ACL to the HTTP or HTTPS service | The name acl-name option was added to the following commands:   * + - * ip http acl       * ip https acl |
| Login management: Enabling RESTful access | The following commands were added:   * + - * restful http enable       * restful https enable |
| Login management: Setting the user line locking key | The lock-key key-string command was added. |
| Login management: Locking the current user line and enabling unlocking authentication | The lock reauthentication command was added. |
| Login management: Specifying a source IPv6 address or source interface for outgoing Telnet packets | The source { interface interface-type interface-number | ipv6 ipv6-address } option was added to the telnet ipv6 command. |
| Login management: Enabling logging for Telnet login attempts that are denied by the Telnet login control ACL | The telnet server acl-deny-log enable command was added. |
| Login management: Applying a Layer 2 ACL to filter Telnet logins | The mac keyword was added to the following commands:   * + - * telnet server ipv6 acl       * telnet server acl |
| Login management: Enabling Web operation logging | The webui log enable command was added. |
| FTP: Enabling logging for FTP login attempts that are denied by the FTP login control ACL | The ftp server acl-deny-log enable command was added. |
| FTP: Associating an SSL server policy with the FTP server | The ftp server ssl-server-policy command was added. |
| Configuration file management: Committing the settings configured after the configuration commit delay timer was set | The configuration commit command was added. |
| Configuration file management: Starting the configuration commit delay timer | The configuration commit delay delay-time command was added. |
| Configuration file management: Main next-startup configuration file backup to an IPv6 TFTP server or download from an IPv6 TFTP server | The ipv6 ipv6-server option was added to the following commands:   * + - * backup startup-configuration       * restore startup-configuration |
| Configuration file management: Displaying all running configuration or the running configuration for an IRF member device | The all and slot slot-number options were added to the display current-configuration command. |
| Configuration file management: Displaying all running configuration in the current view | The all keyword was added to the display this command. |
| Configuration file management: Overwriting the target configuration file with the running configuration if an inconsistency is detected between the settings | The changed keyword was added to the save command. |
| Software upgrade: Installing or uninstalling feature or patch images | The following commands were added:   * + - * display install active       * display install committed       * install activate       * install commit       * install deactivate |
| Device management: Displaying CPU usage statistics in table form | The summary keyword was added to the display cpu-usage command. |
| Device management: Displaying flash memory information | The flash keyword was added to the display device command. |
| Device management: Displaying brief memory usage information | The summary keyword was added to the display memory command. |
| Device management: Displaying system stability and status information | The display system stable state command was added. |
| Device management: Setting free-memory thresholds in percentage, and setting and displaying free-memory early-warning thresholds and sufficient-memory thresholds | * + - * The early-warning, secure, and ratio options were added to the memory-threshold command.       * The display memory-threshold command also displays early warning thresholds. |

# New features: IRF features

Table 2 describes the IRF features added in this software version. For more information about the features and commands, see HPE 5130 EI Switch Series IRF Configuration Guide-R3207 and HPE 5130 EI Switch Series IRF Command Reference-R3207.

IRF features added in version R3207

| Feature | Command changes |
| --- | --- |
| Bulk-configuring basic IRF settings | The easy-irf command was added. |

# New features: Layer 2—LAN switching features

Table 3 describes the Layer 2—LAN switching features added in this software version. For more information about the features and commands, see HPE 5130 EI Switch Series Layer 2—LAN Switching Configuration Guide-R3207 and HPE 5130 EI Switch Series Layer 2—LAN Switching Command Reference-R3207.

Layer 2—LAN switching features added in version R3207

| Feature | Command changes |
| --- | --- |
| Ethernet link aggregation: Configuring an aggregate interface as an edge aggregate interface | The lacp edge-port command was added. |
| Ethernet link aggregation: Configuring LACP to operate in passive mode on a port | The lacp mode passive command was added. |
| Ethernet link aggregation: Using the port speeds as the preferential criteria for selecting a reference port for a dynamic aggregation group | The lacp select speed command was added. |
| Ethernet link aggregation: Enabling the current interface to synchronize the attribute configurations from the aggregate interface when the interface was assigned to the aggregate interface | The force keyword was added to the port link-aggregation group command. |
| Spanning tree: Enabling SNMP notifications for new-root election events or spanning tree topology changes | The new-root and tc keywords were added to the snmp-agent trap enable stp command. |
| Spanning tree: Enabling dispute guard | The stp dispute-protection command was added. |
| Spanning tree: Disabling inconsistent PVID protection | The stp ignore-pvid-inconsistency command was added. |
| Spanning tree: Configuring BPDU guard on an interface | The stp port bpdu-protection { enable | disable } command was added. |
| Spanning tree: Disabling the device from reactivating edge ports shut down by BPDU guard | The stp port shutdown permanent command was added. |
| Spanning tree: Enabling PVST BPDU guard | The stp pvst-bpdu-protection command was added. |
| VLAN: Clearing statistics on a VLAN interface | The reset counters interface vlan-interface |
| VLAN: Associating a VLAN with the specified protocol template | The raw keyword was added to the protocol-vlan command. |
| L2PT: Enabling L2PT for UDLD | The udld keyword was added to the l2protocol tunnel dot1q command. |
| LLDP: Enabling advertisement of the management address TLV globally and setting the management address to be advertised | The lldp [ agent { nearest-customer | nearest-nontpmr } ] global tlv-enable basic-tlv management-address-tlv [ ipv6 ] { ip-address | interface loopback interface-number | interface vlan-interface interface-number } command was added. |

# New features: Layer 3—IP services features

Table 4 describes the Layer 3—IP services features added in this software version. For more information about the features and commands, see HPE 5130 EI Switch Series Layer 3—IP Services Configuration Guide-R3207 and HPE 5130 EI Switch Series Layer 3—IP Services Command Reference-R3207.

Layer 3—IP services features added in version R3207

| Feature | Command changes |
| --- | --- |
| Displaying the maximum number of ARP entries that a device supports | The display arp entry-limit command was added. |
| Setting the aging timer for dynamic ARP entries | The second aging-seconds option was added to the arp timer aging command. |
| Setting the times and the interval for retransmitting a gratuitous ARP packet for the device MAC address change | The gratuitous-arp mac-change retransmit times interval seconds command was added. |
| IP addressing: Displaying brief IP configuration for Layer 3 interfaces | The description keyword was added to the display ip interface brief command. |
| Enabling client offline detection on the DHCP server or relay agent | The dhcp client-detect command was added. |
| Enabling DHCP logging on the DHCP server | The dhcp log enable command was added. |
| Enabling the DHCP server proxy on the relay agent | The proxy keyword was added to the dhcp select command. |
| DHCP server: Specifying a DHCP address pool for a DHCP user class | The class ip-pool command was added. |
| DHCP server: Specifying a DHCP option group for a DHCP user class in a DHCP address pool | The class option-group command was added. |
| DHCP server: Specifying the default DHCP address pool | The default ip-pool command was added. |
| DHCP server: Applying a DHCP policy to an interface | The dhcp apply-policy command was added. |
| DHCP server: Creating a DHCP option group and entering its view | The dhcp option-group command was added. |
| DHCP server: Creating a DHCP policy | The dhcp policy command was added. |
| DHCP server: Enabling MAC address check on the DHCP server. | The dhcp server check mac-address command was added. |
| DHCP server: Configuring the DHCP server to back up the bindings to a file | The following commands were added:   * + - * dhcp server database filename       * dhcp server database update interval       * dhcp server database update now       * dhcp server database update stop       * display dhcp server database |
| DHCP server: Configuring a match rule for a DHCP user class | The following parameters were added to the if-match command:   * + - * hardware-address hardware-address       * mask hardware-address-mask       * ascii ascii-string       * offset offset       * partial       * relay-agent gateway-address |
| DHCP server: Setting the DHCP address pool usage threshold | The ip-in-use threshold command was added. |
| DHCP server: Customizing a DHCP option | The option command was added in DHCP option group view. |
| DHCP server: Configuring the DHCP server in DHCP policy view | The following commands were added in DHCP policy view:   * + - * class ip-pool       * default ip-pool |
| DHCP server: Adding DHCP user classes to the whitelist | The valid class command was added. |
| DHCP server: Enabling the DHCP user class whitelist | The verify class command was added. |
| DHCP relay agent: Setting the DHCP server response timeout time for DHCP server switchover | The dhcp relay dhcp-server timeout command was added. |
| DHCP relay agent: Specifying the DHCP relay agent address to be inserted in DHCP requests | The dhcp relay gateway command was added. |
| DHCP relay agent: Configuring the padding mode and padding format for the Circuit ID sub-option | The following keywords were added to the dhcp relay information circuit-id command:   * + - * bas       * interface |
| DHCP relay agent: Enabling the switchback to the master DHCP server and setting the delay time | The following commands were added:   * + - * dhcp relay master-server switch-delay       * master-server switch-delay |
| DHCP relay agent: Specifying the DHCP server selecting algorithm | The following commands were added:   * + - * dhcp relay server-address algorithm       * remote-server algorithm |
| DHCP relay agent: Specifying the source IP address for relayed DHCP requests | The dhcp relay source-address command was added. |
| DHCP relay agent: Enabling the DHCP smart relay feature | dhcp smart-relay enable |
| DHCP relay agent: Setting the DHCP server response timeout time for DHCP server switchover | The dhcp-server timeout command was added. |
| DHCP relay agent: Specifying DHCP servers for a DHCP address pool | The remote-server command was added. |
| DHCP snooping: Enabling the recording of DHCP snooping entries for a VLAN | The dhcp snooping binding record command was added in VLAN view. |
| DHCP snooping: Disabling DHCP snooping on an interface | The dhcp snooping disable command was added. |
| DHCP snooping: Enabling DHCP snooping for VLANs | The dhcp snooping enable vlan command was added. |
| DHCP snooping: Configuring an interface in a VLAN as a trusted port | The dhcp snooping trust interface command was added. |
| DHCP snooping: Displaying DHCP snooping entries | The verbose keyword was added to the display dhcp snooping binding command. |
| IP forwarding basics: Saving the IP forwarding entries to a file | The ip forwarding-table save filename filename command was added. |
| IP performance optimization: Enabling an interface to forward directed broadcasts destined for the directly connected network | The acl acl-number option was added to the ip forward-broadcast command. |
| IPv6 basics: Displaying the maximum number of ND entries that a device supports | The display ipv6 neighbors entry-limit command was added. |
| IPv6 basics: Specifying an IPv6 prefix for an interface to automatically generate an IPv6 global unicast address and advertising the prefix | The ipv6 address prefix-number command was added. |
| IPv6 basics: Configuring the default settings for prefixes advertised in RA messages | The ipv6 nd ra prefix default command was added. |
| IPv6 basics: Setting the interval for retransmitting an NS message for DAD | The ipv6 nd snooping dad retrans-timer interval command was added. |
| IPv6 basics: Setting timeout timers for ND snooping entries | The ipv6 nd snooping lifetime { invalid invalid-lifetime | valid valid-lifetime } command was added. |
| IPv6 basics: Configuring the port as an ND snooping uplink port which cannot learn ND snooping entries | The ipv6 nd snooping uplink command was added. |
| IPv6 basics: Enabling IPv6 local fragment reassembly | The ipv6 reassemble local enable command was added. |
| Enabling the DHCPv6 server or relay agent to advertise IPv6 prefixes | The ipv6 dhcp advertise pd-route command was added. |
| Enabling DHCPv6 logging on the DHCPv6 server | The ipv6 dhcp log enable command was added. |
| DHCPv6 server: Specifying a DHCPv6 address pool for a DHCPv6 user class | The class pool command was added. |
| DHCPv6 server: Specifying the default DHCPv6 address pool | The default pool command was added. |
| DHCPv6 server: Displaying information about a DHCPv6 option group | The display ipv6 dhcp option-group command was added. |
| DHCPv6 server: Configuring the DHCPv6 server in DHCPv6 option group view | The following commands were added in DHCPv6 option group view:   * + - * dns-server       * domain-name |
| DHCPv6 server: Configuring a match rule for a DHCPv6 user class | The if-match command was added. |
| DHCPv6 server: Applying a DHCPv6 policy to an interface | The ipv6 dhcp apply-policy command was added. |
| DHCPv6 server: Creating a DHCPv6 user class and entering DHCPv6 user class view | The ipv6 dhcp class command was added. |
| DHCPv6 server: Creating a static DHCPv6 option group | The ipv6 dhcp option-group command was added. |
| DHCPv6 server: Creating a DHCPv6 policy | The ipv6 dhcp policy command was added. |
| DHCPv6 server: Specifying a prefix for a DHCPv6 address pool | The prefix prefix-number option was added to the ipv6 dhcp prefix-pool command. |
| DHCPv6 server: Configuring the DHCPv6 server to back up the bindings to a file | The following commands were added:   * + - * ipv6 dhcp server database filename       * ipv6 dhcp server database update interval       * ipv6 dhcp server database update now       * ipv6 dhcp server database update stop       * display ipv6 dhcp server database |
| DHCPv6 server: Specifying an IPv6 subnet for dynamic allocation in a DHCPv6 address pool | The following options were added to the network command:   * + - * prefix prefix-number       * sub-prefix/sub-prefix-length |
| DHCPv6 server: Configuring the DHCPv6 server in DHCPv6 option group view | The following commands were added in DHCPv6 option group view:   * + - * option       * sip-server |
| DHCPv6 server: Specifying a DHCPv6 option group for a DHCPv6 address pool | The option-group command was added. |
| DHCPv6 relay agent: Displaying DHCPv6 relay entries that record clients' IPv6 address information | The display ipv6 dhcp relay client-information address command was added. |
| DHCPv6 relay agent: Displaying DHCPv6 relay entries that record clients' IPv6 prefix information | The display ipv6 dhcp relay client-information pd command was added. |
| DHCPv6 relay agent: Specifying gateway addresses for DHCPv6 clients in a DHCPv6 address pool | The gateway-list command was added. |
| DHCPv6 relay agent: Enabling client offline detection | The ipv6 dhcp client-detect command was added. |
| DHCPv6 relay agent: Enabling the DHCPv6 relay agent to record relay entries | The ipv6 dhcp relay client-information record command was added. |
| DHCPv6 relay agent: Specifying a gateway address for DHCPv6 clients | The ipv6 dhcp relay gateway command was added. |
| DHCPv6 relay agent: Specifying a padding mode for the Interface-ID option | The ipv6 dhcp relay interface-id command was added. |
| DHCPv6 relay agent: Enabling IPv6 release notification | The ipv6 dhcp relay release-agent command was added. |
| DHCPv6 relay agent: Specifying DHCPv6 servers for the DHCPv6 address pool | The remote-server command was added. |
| DHCPv6 relay agent: Clearing DHCPv6 relay entries that record clients' IPv6 address information | The reset ipv6 dhcp relay client-information address command was added. |
| DHCPv6 relay agent: Clearing DHCPv6 relay entries that record clients' IPv6 prefix information | The reset ipv6 dhcp relay client-information pd command was added. |
| DHCPv6 client: Configuring the interface to use DHCPv6 to obtain an IPv6 address and other configuration parameters | The option-group option-group-number option was added to the following commands:   * + - * ipv6 dhcp client pd       * ipv6 address dhcp-alloc |
| DHCPv6 client: Configuring the DHCPv6 client DUID | The ipv6 dhcp client duid command was added. |
| DHCPv6 client: Configuring the interface to use DHCPv6 to obtain an IPv6 address, an IPv6 prefix, and other configuration parameters | The ipv6 dhcp client stateful command was added. |

# New features: Layer 3—IP routing features

Table 5 describes the Layer 3—IP routing features added in this software version. For more information about the features and commands, see HPE 5130 EI Switch Series Layer 3—IP Routing Configuration Guide-R3207 and HPE 5130 EI Switch Series Layer 3—IP Routing Command Reference-R3207.

Layer 3—IP routing features added in version R3207

|  |  |
| --- | --- |
| Feature | Command changes |
| RIP: Displaying the GR status for a RIP process | The display rip graceful-restart command was added. |
| RIP: Displaying the NSR status for a RIP process | The display rip non-stop-routing command was added. |
| RIP: Setting the GR interval | The graceful-restart interval command was added. |
| RIP: Enabling RIP NSR | The non-stop-routing command was added. |
| RIP: Configuring RIP FRR | The fast-reroute command was added. |
| RIPng: Displaying the GR status for a RIPng process | The display ripng graceful-restart command was added. |
| RIPng: Displaying the NSR status for a RIPng process | The display ripng non-stop-routing command was added. |
| RIPng: Enabling RIPng FRR | The fast-reroute command was added. |
| RIPng: Setting the GR interval | The graceful-restart interval command was added. |
| RIPng: Enabling RIPng NSR | The non-stop-routing command was added. |
| RIPng: Enabling BFD single-hop echo detection for RIPng FRR | The ripng primary-path-detect bfd echo command was added. |

# New features: IP multicast features

Table 6 describes the IP multicast features added in this software version. For more information about the features and commands, see HPE 5130 EI Switch Series IP Multicast Configuration Guide-R3207 and HPE 5130 EI Switch Series IP Multicast Command Reference-R3207.

IP multicast features added in version R3207

| Feature | Command changes |
| --- | --- |
| IGMP snooping: Displaying information about dynamic IGMP snooping group entries for an interface | The interface interface-type interface-number option was added to the display igmp-snooping group command. |
| IGMP snooping: Displaying detailed information about dynamic router ports | The verbose keyword was added to the display igmp-snooping router-port command. |
| IGMP snooping: Displaying detailed information about static router ports | The verbose keyword was added to the display igmp-snooping static-router-port command. |
| IGMP snooping: Enabling IGMP snooping globally | The global-enable command was added. |
| IGMP snooping: Disabling IGMP snooping for a VLAN | The igmp-snooping disable command was added. |
| PIM snooping: Displaying detailed information about PIM snooping router ports | The verbose keyword was added to the display pim-snooping router-port command. |
| MLD snooping: Displaying information about dynamic MLD snooping group entries for an interface | The interface interface-type interface-number option was added to the display mld-snooping group command. |
| MLD snooping: Displaying detailed information about dynamic router ports | The verbose keyword was added to the display mld-snooping router-port command. |
| MLD snooping: Displaying detailed information about static router ports | The verbose keyword was added to the display mld-snooping static-router-port command. |
| MLD snooping: Enabling MLD snooping globally | The global-enable command was added. |
| MLD snooping: Disabling MLD snooping for a VLAN | The mld-snooping disable command was added. |
| IPv6 PIM snooping: Displaying detailed information about IPv6 PIM snooping router ports | The verbose keyword was added to the display ipv6 pim-snooping router-port command. |

# New features: ACL and QoS features

Table 7 describes the ACL and QoS features added in this software version. For more information about the features and commands, see HPE 5130 EI Switch Series ACL and QoS Configuration Guide-R3207 and HPE 5130 EI Switch Series ACL and QoS Command Reference-R3207.

ACL and QoS features added in version R3207

| Feature | Command changes |
| --- | --- |
| ACL: Enabling SNMP notifications for packet filtering and setting the interval | The acl trap interval command was added. |
| ACL: Setting a rule numbering step for an ACL | The start start-value option was added to the step command. |
| QoS: Configuring a description for a traffic class | The description command was added. |
| QoS: Associating a traffic behavior with a traffic class in a QoS policy | The insert-before before-classifier-name option was added to the classifier behavior command. |
| QoS: Displaying QoS policies applied to user profiles | display qos policy user-profile |
| QoS: Configuring queue scheduling profiles | The following commands were added:   * + - * display qos qmprofile configuration       * display qos qmprofile interface       * qos qmprofile       * bandwidth queue       * queue       * qos apply qmprofile |
| Data buffer: Configuring data buffer monitoring | The following commands were added:   * + - * display buffer usage interface       * buffer usage threshold |

# New features: Security features

Table 8 describes the security features added in this software version. For more information about the features and commands, see HPE 5130 EI Switch Series Security Configuration Guide-R3207 and HPE 5130 EI Switch Series Security Command Reference-R3207.

Security features added in version R3207

| Feature | Command changes |
| --- | --- |
| AAA: New authorization attributes for users | The following parameters were added in the authorization-attribute command in ISP domain view:   * + - * acl       * car       * igmp       * mld       * url       * user-group   The following parameters were added in the authorization-attribute command in local user view or user group view:   * + - * idle-cut       * session-timeout |
| AAA: Configuring the device to include the idle cut period in the user online duration sent to the server | The session-time include-idle-time command was added. |
| AAA: Configuring a description for a network access user | The description command was added in local user view. |
| AAA: Configuring the auto-delete feature of local users | The local-user auto-delete enable command was added. |
| AAA: Configuring the validity period for a network access user | The validity-datetime command was added. |
| AAA: Configuring the device ID | The aaa device-id command was added. |
| AAA: Enabling the extended accounting-on feature | The accounting-on extended command was added. |
| AAA: Configuring the device to interpret the RADIUS class attribute (attribute 25) as CAR parameters | The attribute 25 car command was added. |
| AAA: Configuring the MAC address format for RADIUS attribute 31 | The attribute 31 mac-format command was added. |
| AAA: Setting the data measurement unit for the Remanent\_Volume attribute | The attribute remanent-volume command was added. |
| AAA: Configuring the RADIUS attribute translation feature | The following commands were added:   * + - * attribute convert (RADIUS DAS view)       * attribute convert (RADIUS scheme view)       * attribute reject (RADIUS DAS view)       * attribute reject (RADIUS scheme view)       * attribute translate       * radius attribute extended |
| AAA: Configuring the DSCP priority of RADIUS packets | The radius dscp command was added. |
| AAA: Support for CoA messages to shut down or reboot the access port of users or reauthenticate users | N/A |
| AAA: Specifying a RADIUS session-control client | The radius session-control client command was added. |
| AAA: Configuring an LDAP attribute map | The following commands were added:   * + - * attribute-map       * ldap attribute-map       * map |
| AAA: Specifying the LDAP authorization server | The authorization-server command was added. |
| AAA: Broadcasting RADIUS accounting requests | The broadcast keyword was added to the following commands:   * + - * accounting lan-access       * accounting portal |
| AAA: Displaying the HWTACACS service statistics | The display hwtacacs scheme [ hwtacacs-scheme-name statistics ] command was added. |
| AAA: Configuring the RADIUS server feature | The following commands were added:   * + - * display radius-server active-client       * display radius-server active-user       * radius-server activate       * radius-server client |
| AAA: Support for RADIUS attribute 168 (Framed-IPv6-Address) to accept the IPv6 addresses assigned by the server to hosts | N/A |
| 802.1X: Redirect URL assignment | N/A |
| 802.1X: Displaying information about online 802.1X open users | The open keyword was added to the display dot1x connection command. |
| 802.1X: Displaying MAC address information of 802.1X users in specific VLANs | The display dot1x mac-address command was added. |
| 802.1X: Enabling logging for 802.1X users | The dot1x access-user log enable command was added. |
| 802.1X: Setting the maximum number of 802.1X authentication attempts for MAC authenticated users | The dot1x after-mac-auth max-attempt command was added. |
| 802.1X: Specifying supported domain name delimiters | The dot1x domain-delimiter command was added. |
| MAC authentication: Redirect URL assignment | N/A |
| MAC authentication: Displaying information about online MAC authentication open users | The open keyword was added to the display mac-authentication connection command. |
| MAC authentication: Displaying MAC address information of MAC authentication users in specific VLANs | The display mac-authentication mac-address command was added. |
| MAC authentication: Enabling logging for MAC authentication users | The mac-authentication access-user log enable command was added. |
| MAC authentication: Enabling the authorization VLAN auto-tag feature | The mac-authentication auto-tag [ ignore-config ] command was added. |
| MAC authentication: Including user IP addresses in MAC authentication requests | The mac-authentication carry user-ip command was added. |
| Port security: Redirect URL assignment for specific port security modes | N/A |
| Port security: Enabling open authentication mode | The following commands were added:   * + - * port-security authentication open       * port-security authentication open global |
| Port security: Setting the secure MAC aging timer in seconds | The second keyword was added to the port-security timer autolearn aging command. |
| Port security: Enabling logging for port security users | The port-security access-user log enable command was added. |
| Port security: Enabling the quiet timer function for the authorization-fail-offline feature | The quiet-period keyword was added to the port-security authorization-fail offline command. |
| Port security: Setting port security's limit on the number of MAC addresses for specific VLANs on a port | The port-security mac-limit command was added. |
| Port security: Setting port security's limit on the number of secure MAC addresses for specific VLANs on a port | The vlan [ vlan-id-list ] option was added to the port-security max-mac-count command. |
| Portal support for EAP | N/A |
| Portal: Displaying information about portal users | The following parameters were added in the display portal user command:   * + - * ip       * ipv6       * pre-auth       * verbose |
| Portal: Displaying information about Web redirect rules | The display web-redirect rule interface interface-type interface-number [ slot slot-number ] command was added. |
| Portal: Configuring a match rule for URL redirection | The if-match { original-url url-string redirect-url url-string [ url-param-encryption { aes | des } key { cipher | simple } string ] | user-agent string redirect-url url-string } command was added. |
| Portal: Setting the maximum number of portal users on an interface | The portal { ipv4-max-user | ipv6-max-user } max-number command was added. |
| Portal: Enabling strict checking on portal authorization information | The portal authorization { acl | user-profile } strict-checking command was added. |
| Portal: Specifying the Layer 3 interface on which an IP-based portal-free rule takes effect | The interface interface-type interface-number option was added to the portal free-rule command. |
| Portal: Configuring a destination-based portal-free rule | The portal free-rule rule-number destination host-name command was added. |
| Portal: Enabling logging for portal logins and logouts | The portal log enable command was added. |
| Portal: Specifying the format for the NAS-Port-Id attribute | The portal nas-port-id format { 1 | 2 | 3 | 4 } command was added. |
| Portal: Specifying a portal preauthentication domain | The portal [ ipv6 ] pre-auth domain domain-name command was added. |
| Portal: Enabling the Rule ARP or ND entry feature for portal clients | The portal refresh { arp | nd } enable command was added. |
| Portal: Allowing only users with DHCP-assigned IP addresses to pass portal authentication | The portal [ ipv6 ] user-dhcp-only command was added. |
| Portal: Specifying the port number of a Web proxy server | The portal web-proxy port port-number command was added. |
| Portal: Configuring the device to periodically register with the portal authentication server | The server-register [ interval interval-value ] command was added. |
| Portal: Specifying the type of a portal authentication server or portal Web server | The server-type { cmcc | imc } command was added. |
| Portal: Configuring the device to carry the user MAC address in encrypted form in the redirect URL | The [ encryption { aes | des } key { cipher | simple } string ] parameter was added to the url-parameter command. |
| Portal: Configuring Web redirect | The web-redirect [ ipv6 ] url url-string [ interval interval ] command was added. |
| Web authentication: Setting the redirection wait time | The redirect-wait-time period command was added. |
| Web authentication: Adding parameters to the redirection URL of the Web authentication server | The url-parameter parameter-name { original-url | source-address | source-mac | value expression } command was added. |
| PKI: Specifying an ECDSA key pair for certificate request | The public-key ecdsa name key-name [ secp256r1 | secp384r1 | secp521r1 ] command was added in FIPS mode. |
| IKE: Configuring a description for an IKE proposal | The description text command was added. |
| IKE: Displaying IKE statistics | The display ike statistics command was added. |
| IKEv2: Displaying IKEv2 statistics | The display ikev2 statistics command was added. |
| IKEv2: Clearing IKEv2 statistics | The reset ikev2 statistics command was added. |
| SSL: SSL server support for optional SSL client authentication | The optional keyword was added to the client-verify command. |
| SSL: Setting the timeout time for cached sessions | The timeout time option was added to the session command. |
| SSH: Releasing SSH connections | The free ssh { user-ip { ip-address | ipv6 ipv6-address } [ port port-number ] | user-pid pid-number | username username } command was added. |
| SSH: Enabling logging for SSH login attempts that are denied by the SSH login control ACL | The ssh server acl-deny-log enable command was added. |
| SSH: Specifying the SSH service port | The ssh server port port-number command was added. |
| SSH: Deleting server public keys saved in the public key file on the SSH client | The delete ssh client server-public-key [ server-ip ip-address ] command was added. |
| SSH: Displaying server public key information saved in the public key file of the SSH client | The display ssh client server-public-key [ server-ip ip-address ] command was added. |
| 802.1X client | All 802.1X client commands were newly added. |
| IP source guard: Displaying IPv4SG bindings dynamically generated based on ARP snooping or 802.1X | The arp-snooping and dot1x keywords were added to the display ip source binding command. |
| IP source guard: Displaying IPv6SG bindings dynamically generated based on DHCPv6 relay agent, 802.1X, or ND snooping | The following keywords were added to the display ipv6 source binding command:   * + - * dhcpv6-relay       * dot1x       * nd-snooping |
| ARP attack protection: Converting valid static ARP entries to dynamic ARP entries and deleting invalid static ARP entries | The undo arp fixup command was added. |
| ARP attack protection: Specifying the sender IP address range for ARP packet checking | The arp sender-ip-range command was added. |
| SAVI | All SAVI commands were newly added. |

# New features: High availability features

Table 9 describes the high availability features added in this software version. For more information about the features and commands, see HPE 5130 EI Switch Series High Availability Configuration Guide-R3207 and HPE 5130 EI Switch Series High Availability Command Reference-R3207.

High availability features added in version R3207

| Feature | Command changes |
| --- | --- |
| CFD: Enabling two-way DM | The dot1p dot1p-value and interval interval options were added to the cfd dm two-way command. |
| CFD: Enabling loss measurement | The dot1p dot1p-value and interval interval options were added to the cfd slm command. |
| DLDP: Setting the port shutdown mode | The hybrid keyword was added to the dldp unidirectional-shutdown command. |
| BFD: Creating a BFD session for detecting the local interface state | The bfd detect-interface source-ip command was added. |
| BFD: Enabling the echo packet mode | The receive and send keywords were added to the bfd echo enable command. |
| BFD: Enabling SNMP notifications for BFD | The snmp-agent trap enable bfd command was added. |
| Monitor Link: Configuring the uplink interface threshold for triggering monitor link group state switchover | The uplink up-port-threshold command was added. |
| Process placement | All process placement commands were newly added. |
| Track: Displaying track entry information | The negative, positive, and brief keywords were added to the display track command. |
| Track: Creating a track entry and associate it with the physical state of an interface | The track interface physical command was added. |
| Track: Creating a track entry and associate it with a route entry | The track ip route reachability command was added. |
| Track: Creating a track entry and associate it with the neighbor availability status of an LLDP interface | The track lldp neighbor command was added. |

# New features: Network management and monitoring features

Table 10 describes the network management and monitoring features added in this software version. For more information about the features and commands, see HPE 5130 EI Switch Series Network Management and Monitoring Configuration Guide-R3207 and HPE 5130 EI Switch Series Network Management and Monitoring Command Reference-R3207

Network management and monitoring features added in version R3207

| Feature | Command changes |
| --- | --- |
| NQA: Specifing a community name for the SNMP operation | The community read command was added. |
| NQA: Specifying a destination device by its host name for the UDP tracert operation | The destination host command was added. |
| NQA: Configuring the RADIUS template | The key command was added. |
| NQA: Specifying the next hop IP address for ICMP echo requests | The next-hop command was added |
| NQA: Configuring the TCP half open template | N/A |
| NQA: Configuring the SSL template | The ssl-client-policy command was added. |
| NQA: Configuring the HTTPS template | N/A |
| NTP: Configuring NTP authentication | The hmac-sha-1, hmac-sha-256, hmac-sha-384, and hmac-sha-512 keywords were added to the ntp-service authentication-keyid command. |
| NETCONF: Specifying a mandatory authentication domain for NETCONF users | The netconf soap domain command was added. |
| NETCONF: Applying an ACL to NETCONF over SOAP traffic | The netconf soap acl command was added. |
| NETCONF: Setting the DSCP value for outgoing NETCONF over SOAP packets | The netconf soap dscp command was added/ |
| NETCONF: Specifying a specific name space. | The netconf capability specific-namespace command was added. |
| NETCONF: Setting the NETCONF session idle timeout time | The netconf idle-timeout command was added. |
| NETCONF: Support for the OverWrite attribute for saving the running configuration | N/A |
| NETCONF: Subscribing to monitoring events and module report events | N/A |
| NETCONF: Retrieving NETCONF information | N/A |
| NETCONF: Retrieving YANG file content | N/A |
| NETCONF: Not support for the <edit-config> operation while the device is rolling back configuration. | N/A |
| VCF fabric | All VCF fabric commands were newly added. |
| SNMP: Calculating the encrypted form for a key in plaintext form | * + - * In non-FIPS mode: The aes192md5, aes192sha, aes256md5, and aes256sha keywords were added to the snmp-agent calculate-password command.       * In FIPs mode: The aes192sha and aes256sha keywords were added to the snmp-agent calculate-password command. |
| EAA: Configuring a member device join or leave event | The insert and remove keywords were added to the event hotplug command. |
| EAA: Configuring a track event for a CLI-defined monitor policy | The event track command was added. |
| EAA: Setting the size for the EAA-monitored log buffer | The rtm event syslog buffer-size command was added. |
| Process monitoring and maintenance: Specifying the action to be taken in response to a kernel thread deadloop | The monitor kernel deadloop action command was added. |
| Process monitoring and maintenance: Enabling kernel thread deadloop detection for a CPU core. | The core keyword was added to the monitor kernel deadloop enable command. |
| Information center: Setting the maximum number of log traps that can be stored in the log trap buffer | The info-center syslog trap command was added. |
| Information center: Enabling SNMP notifications for log messages | The snmp-agent trap enable syslog command was added. |

# New features: OpenFlow features

Table 11 describes the OpenFlow features added in this software version. For more information about the features and commands, see HPE 5130 EI Switch Series OpenFlow Configuration Guide-R3207 and HPE 5130 EI Switch Series OpenFlow Command Reference-R3207.

OpenFlow features added in version R3207

| Feature | Command changes |
| --- | --- |
| Displaying information of the client that connects to the server that is enabled for an OpenFlow instance in the controller information | The listened keyword was added to the display openflow command. |
| Adding the VLAN tagging and untagging flow tables | The ingress-vlan ingress-table-id and egress-vlan egress-table-id options were added to the flow-table command. |
| Clearing statistics on packets that a controller sends and receives for an OpenFlow instance | The reset openflow instance statistics command was added. |
| Adding the smart interruption mode | The smart keyword was added to the fail-open mode command. |

# Modified feature: Configuring a command alias

## Feature change description

The syntax of the command for configuring a command alias changed from command-alias mapping to alias.

## Command changes

### Modified command: command-alias mapping

Old syntax

command-alias mapping

New syntax

alias

Views

Any view

Change description

Before modification: The command syntax is command-alias mapping.

After modification: The command syntax is alias.

# Modified feature: Displaying command aliases

## Feature change description

The syntax of the command for displaying command aliases changed from display command-alias to display alias.

## Command changes

### Modified command: display command-alias

Old syntax

display command-alias

New syntax

display alias

Views

Any view

Change description

Before modification: The command syntax is display command-alias.

After modification: The command syntax is display alias.

# Modified feature: Configuring a hotkey

## Feature change description

More hotkeys can be modified.

## Command changes

### Modified command: hotkey

Old syntax

hotkey { ctrl\_g | ctrl\_l | ctrl\_o | ctrl\_t | ctrl\_u } command

New syntax

hotkey hotkey { command | function function | none }

Views

System view

Change description

Before modification: The command allows you to configure only five hotkeys.

After modification: The command allows you to configure all hotkeys.

# Modified feature: Maximum length for a configuration file name

## Feature change description

The maximum length was increased for a configuration file name.

## Command changes

### Modified command: configuration replace file

Syntax

configuration replace file filename

Views

System view

Change description

Before modification: The maximum length cannot exceed 191 characters for a configuration file name. The file name can include the file path.

After modification: The maximum length cannot exceed 255 characters for a configuration file name. The file name can include the file path.

### Modified command: restore startup-configuration

Syntax

restore startup-configuration from tftp-server src-filename

Views

User view

Change description

Before modification: The maximum length cannot exceed 191 characters for a configuration file name. The file name can include the file path.

After modification: The maximum length cannot exceed 255 characters for a configuration file name. The file name can include the file path.

### Modified command: save

Syntax

save file-url [ all | slot slot-number ]

Views

Any view

Change description

Before modification: The maximum length cannot exceed 191 characters for a configuration file name. The file name can include the file path.

After modification: The maximum length cannot exceed 255 characters for a configuration file name. The file name can include the file path.

### Modified command: startup saved-configuration

Syntax

startup saved-configuration cfgfile [ backup | main ]

Views

User view

Change description

Before modification: The maximum length cannot exceed 191 characters for a configuration file name. The file name can include the file path.

After modification: The maximum length cannot exceed 255 characters for a configuration file name. The file name can include the file path.

# Modified feature: BFD MAD collision handling process

## Feature change description

Before modification, BFD MAD uses the following process to handle a multi-active collision:

Compares the member IDs of the masters in the split IRF fabrics.

Sets all fabrics to the Recovery state except the one that has the lowest numbered master.

BFD MAD cannot be configured together with LACP MAD, because they handle collisions differently.

After modification, BFD MAD uses the following process to handle a multi-active collision:

Compares the number of members in each split IRF fabric.

Sets all fabrics to the Recovery state except the one that has the most members.

Compares the member IDs of the masters if all IRF fabrics have the same number of members.

Sets all fabrics to the Recovery state except the one that has the lowest numbered master.

BFD MAD can be configured together with LACP MAD.

## Command changes

None.

# Modified feature: Support for commands on IRF physical interfaces

## Feature change description

The following commands were added on IRF physical interfaces:

* MAC address table configuration commands, including the mac-address static source-check enable command. For information about this command, see HPE 5130 EI Switch Series Layer 2—LAN Switching Command Reference-R3207.
* The mirroring-group reflector-port command. Use this command to configure the reflector port for a remote source group. When you execute this command on an IRF physical interface, the binding between the physical interface and IRF port is removed. To avoid IRF split, do not configure a physical interface as a reflector port if that interface is the only member interface of an IRF port. For more information about the mirroring-group reflector-port command, see HPE 5130 EI Switch Series Network Management and Monitoring Command Reference-R3207.
* LLDP commands, including:
  + lldp admin-status
  + lldp check-change-interval
  + lldp enable
  + lldp encapsulation snap
  + lldp notification remote-change enable
  + lldp tlv-enable

Use these commands to view the connectivity and status of IRF links. For more information about LLDP commands, see HPE 5130 EI Switch Series Layer 2—LAN Switching Command Reference-R3207.

## Command changes

The following commands were added in IRF physical interface view:

* lldp admin-status
* lldp check-change-interval
* lldp enable
* lldp encapsulation snap
* lldp notification remote-change enable
* lldp tlv-enable
* mac-address static source-check enable
* mirroring-group reflector-port

# Modified feature: Excluding a service interface from the IRF MAD shutdown action by the system

## Feature change description

When the IRF fabric transits to the Recovery state, the system automatically excludes the following service interfaces from being shut down:

* Before modification:
  + IRF physical interfaces.
  + Member interfaces of an aggregate interface if the aggregate interface is excluded from being shut down.
* After modification:
  + IRF physical interfaces.
  + Interfaces used for BFD MAD.
  + Member interfaces of an aggregate interface if the aggregate interface is excluded from being shut down.

## Command changes

None.

# Modified feature: Displaying information about packets dropped on an interface

## Feature change description

Statistics about packets dropped due to insufficient data buffer were displayed.

## Command changes

### Modified command: display packet-drop

Syntax

display packet-drop { interface [ interface-type [ interface-number ] ] | summary }

Views

Any view

Change description

Before modification: The command cannot display statistics about packets dropped due to insufficient data buffer.

After modification: The command can display statistics about packets dropped due to insufficient data buffer as follows:

Packets dropped due to insufficient data buffer. Input dropped: 0 Output dropped:0

# Modified feature: Displaying MAC address move records

## Feature change description

The maximum number of MAC address move records the device can display changed from 20 to 200.

## Command changes

None.

# Modified feature: MAC address move notifications

## Feature change description

Before modification: Within a detection interval, an IRF member device can record MAC address move information for a maximum of 20 MAC addresses. The most recent record will override the oldest one.

After modification:

Within a detection interval, an IRF member device can record MAC address move information for a maximum of 20 MAC addresses. The records are ranked in descending order of MAC move counts. When the MAC move count of a new record is higher than the MAC move count of any existing record, the device performs the following operations:

* Discards the record that has the lowest MAC move count.
* Ranks the MAC address move records in descending order of MAC move count.

Then, in the next detection interval, the device discards all MAC address move records generated in the previous detection interval and starts another round of MAC move record generation.

## Command changes

None.

# Modified feature: Setting the voice VLAN aging timer

## Feature change description

You can configure voice VLANs not to age out in this version and later.

## Command changes

### Modified command: voice-vlan aging

Syntax

voice-vlan aging minutes

undo voice-vlan aging

Views

System view

Change description

Before modification: The value of voice VLAN aging timer is in the range of 5 to 43200 minutes.

After modification: The value of voice VLAN aging timer can be 0 minutes or in the range of 5 to 43200 minutes. If you set the voice VLAN aging timer to 0 minutes, the voice VLAN does not age out.

# Modified feature: Creating a VLAN

## Feature change description

When you create a VLAN, you can specify a space-separated list of up to 32 VLAN items in this version and later.

## Command changes

### Modified command: vlan

Old syntax

vlan { vlan-id1 [ to vlan-id2 ] | all }

undo vlan { vlan-id1 [ to vlan-id2 ] | all }

New syntax

vlan { vlan-id-list ] | all }

undo vlan { vlan-id-list | all }

Views

System view

Change description

Before modification: The vlan-id1 to vlan-id2 option specifies a VLAN range. This option can be specified only once.

After modification: The vlan-id-list argument specifies a space-separated list of up to 32 VLAN items.

# Modified feature: Displaying history about ports that are blocked by spanning tree protection features

## Feature change description

You can use the display stp abnormal-port command to display history about ports that are blocked by spanning tree protection features.

## Command changes

### Modified command: display stp abnormal-port

Syntax

display stp abnormal-port

Views

Any view

Change description

Before modification:

<Sysname> display stp abnormal-port

MST ID Blocked Port Reason

1 GigabitEthernet1/0/1 Root-Protected

2 GigabitEthernet1/0/2 Loop-Protected

12 GigabitEthernet1/0/3 Loopback-Protected

After modification:

<Sysname> display stp abnormal-port

---[GigabitEthernet1/0/1]---

MST ID BlockReason Time

0 Loopback-Protected 07:56:44 05/01/2017

0 Disputed 07:56:37 05/01/2017

0 Loop-Protected 06:56:13 05/01/2017

---[GigabitEthernet1/0/2]---

MST ID BlockReason Time

0 Loopback-Protected 07:55:51 05/01/2017

Modification:

* In an MSTI or VLAN, this command can display a maximum of three history records for a port that is blocked by spanning tree protection features.
* The following fields were added to the output from the display stp abnormal-port command:
  + BlockReason—Reason that the port was blocked.
  + Time—Protection feature trigger time.

# Modified feature: Setting the LLDP frame transmission interval

## Feature change description

The minimum LLDP frame transmission interval was changed from 5 seconds to 1 second.

## Command changes

### Modified command: lldp timer tx-interval

Syntax

lldp timer tx-interval interval

undo lldp timer tx-interval

Views

System view

Change description

Before modification: The value range for the interval argument was 5 to 32768 seconds.

After modification: The value range for the interval argument is 1 to 32768 seconds.

# Modified feature: Displaying ARP entries

## Feature change description

The unit of the displayed aging time for ARP entries was changed from minute to second, and Rule ARP entries were added to the output.

## Command changes

### Modified command: display arp

Syntax

display arp [ [ all | dynamic | multiport | static ] [ slot slot-number ] | vlan vlan-id | interface interface-type interface-number ] [ count | verbose ]

Views

Any view

Change description

Before modification:

# Display brief information about all ARP entries.

<Sysname> display arp all

Type: S-Static D-Dynamic O-Openflow M-Multiport I-Invalid

IP Address MAC Address VLAN Interface Aging Type

20.1.1.1 00e0-fc00-0001 N/A N/A N/A S

193.1.1.70 00e0-fe50-6503 100 GE1/0/1 N/A IS

192.168.0.115 000d-88f7-9f7d 1 GE1/0/2 18 D

192.168.0.39 0012-a990-2241 1 GE1/0/3 20 D

22.1.1.1 010c-299d-c041 10 N/A N/A M

# Display detailed information about all ARP entries.

<Sysname> display arp all verbose

Type: S-Static D-Dynamic O-Openflow M-Multiport I-Invalid

IP Address MAC Address VLAN Interface Aging Type

Vpn Instance

20.1.1.1 00e0-fc00-0001 N/A N/A N/A S

[No Vrf]

193.1.1.70 00e0-fe50-6503 100 GE1/0/1 N/A IS

[No Vrf]

192.168.0.115 000d-88f7-9f7d 1 GE1/0/2 18 D

[No Vrf]

192.168.0.39 0012-a990-2241 1 GE1/0/3 20 D

[No Vrf]

22.1.1.1 010c-299d-c041 10 N/A N/A M

[No Vrf]

After modification:

# Display brief information about all ARP entries.

<Sysname> display arp all

Type: S-Static D-Dynamic O-Openflow R-Rule M-Multiport I-Invalid

IP Address MAC Address VID Interface/Link ID Aging Type

1.1.1.1 02e0-f102-0023 1 GE1/0/1 N/A S

1.1.1.2 00e0-fc00-0001 12 GE1/0/2 960 D

1.1.1.3 00e0-fe50-6503 12 Tunnel1 960 D

1.1.1.4 000d-88f7-9f7d 12 0x1 960 D

# Display detailed information about all ARP entries.

<Sysname> display arp all verbose

Type: S-Static D-Dynamic O-Openflow R-Rule M-Multiport I-Invalid

IP Address : 1.1.1.1 VID : 1 Aging : N/A

MAC Address : 02e0-f102-0023 Type: S Nickname: 0x0000

Interface/Link ID:

VPN Instance : [No Vrf]

VXLAN ID : N/A

VSI Name : N/A

VSI Interface : N/A

IP Address : 1.1.1.2 VID : 12 Aging : 960 sec

MAC Address : 0015-e944-adc5 Type: D Nickname: 0x0000

Interface/Link ID:

VPN Instance : [No Vrf]

VXLAN ID : N/A

VSI Name : N/A

VSI Interface : N/A

IP Address : 1.1.1.3 VID : 12 Aging : 960 sec

MAC Address : 0013-1234-0001 Type: D Nickname: 0x0000

Interface/Link ID: Tunnel1

VPN Instance : [No Vrf]

VXLAN ID : N/A

VSI Name : N/A

VSI Interface : N/A

IP Address : 1.1.1.4 VID : 12 Aging : 960 sec

MAC Address : 0012-1234-0002 Type: D Nickname: 0x0000

Interface/Link ID: 0x1

VPN Instance : [No Vrf]

VXLAN ID : N/A

VSI Name : N/A

VSI Interface : N/A

The following changes were added to the command output:

* The R-Rule field was added.
* The unit of the displayed aging time for ARP entries was changed from minute to second.

# Modified feature: Displaying the aging time of dynamic ARP entries

## Feature change description

The unit of the displayed aging time of dynamic ARP entries was changed from minute to second.

## Command changes

### Modified command: display arp timer aging

Syntax

display arp timer aging

Views

Any view

Change description

Before modification: The unit of the displayed aging time of dynamic ARP entries was minute.

# Display the aging time of dynamic ARP entries.

<Sysname> display arp timer aging

Current ARP aging time is 20 minute(s)

After modification: The unit of the displayed aging time of dynamic ARP entries was changed from minute to second.

# Display the aging time of dynamic ARP entries.

<Sysname> display arp timer aging

Current ARP aging time is 1200 seconds

# Modified feature: Default source IP address in packets relayed to the DHCP server

## Feature change description

For the default source IP address in packets that the DHCP relay agent forwards to the DHCP server, the following changes have been made:

* In software versions earlier than Release 3207, the default source IP address is the IP address of the interface through which the DHCP relay agent connects the DHCP client.
* In Release 3207 and later, the default source IP address is the IP address of the output interface through which the DHCP relay agent forwards the packets to the DHCP server. You can use the dhcp relay source-address command to modify the source IP address for these relayed packets.

## Command changes

None.

# Modified feature: Specifying gateways on the DHCP server for DHCP clients

## Feature change description

The maximum number of gateways that can be specified on the DHCP server for DHCP clients was changed from 8 to 64.

## Command changes

### Modified command: gateway-list

Syntax

gateway-list ip-address&<1-64>

undo gateway-list [ ip-address&<1-64> ]

Views

DHCP address pool view

DHCP secondary subnet view

Change description

Before modification: A maximum of eight gateways can be specified on the DHCP server for DHCP clients.

After modification: A maximum of 64 gateways can be specified on the DHCP server for DHCP clients.

# Modified feature: Displaying information for DHCP snooping trusted ports

## Feature change description

From this version, you can display VLAN information for DHCP snooping trusted ports.

## Command changes

### Modified command: display dhcp snooping trust

Syntax

display dhcp snooping trust

Views

Any view

Change description

Before modification:

# Display information about trusted ports.

<Sysname> display dhcp snooping trust

DHCP snooping is enabled.

Interface Trusted

========================= ============

GigabitEthernet1/0/1 Trusted

After modification:

# Display information about trusted ports.

<Sysname> display dhcp snooping trust

DHCP snooping is enabled.

Interface Trusted VLAN

========================= ============ =======

GigabitEthernet1/0/1 Trusted

GigabitEthernet1/0/2 - 100

GigabitEthernet1/0/3 - 100, 200

The following changes were added to the command output:

* Trusted—For a DHCP snooping trusted port configured in system view, this field displays Trusted. For a trusted port configured in VLAN view, this field displays a hyphen (-).
* VLAN—VLANs in which the port is configured as trusted. If a trusted port is configured after DHCP snooping is enabled globally, this field is empty.

# Modified feature: Setting the MTU of IPv4 packets sent over an interface

## Feature change description

The value range for the MTU of IPv4 packets sent over an interface was changed.

## Command changes

### Modified command: ip mtu

Syntax

ip mtu mtu-size

undo ip mtu

Views

Interface view

Change description

Before modification: The value range for the mtu-size argument is 128 to 2000 bytes.

After modification: The value range for the mtu-size argument is 128 to 1500 bytes.

# Modified feature: Setting the TCP buffer size

## Feature change description

The default size of the TCP receive/send buffer was changed from 64 KB to 63 KB.

## Command changes

### Modified command: tcp window

Syntax

tcp window window-size

undo tcp window

Views

System view

Change description

Before modification: The default size of the TCP receive/send buffer is 64 KB.

After modification: The default size of the TCP receive/send buffer is 63 KB.

# Modified feature: Configuring prefix to be advertised in RA messages

## Feature change description

The following changes were added to the ipv6 nd ra prefix command:

* The no-advertise keyword was added.
* The valid-lifetime, preferred-lifetime, and no-advertise parameters in this command were changed from required to optional.

## Command changes

### Modified command: ipv6 nd ra prefix

Old syntax

ipv6 nd ra prefix { ipv6-prefix prefix-length | ipv6-prefix/prefix-length } valid-lifetime preferred-lifetime [ no-autoconfig | off-link ] \*

New syntax

ipv6 nd ra prefix { ipv6-prefix prefix-length | ipv6-prefix/prefix-length } [ valid-lifetime preferred-lifetime [ no-autoconfig | off-link ] \* | no-advertise ]

Views

Interface view

Change description

Before modification:

* The device always advertises the prefix in RA messages.
* When configuring the ipv6 nd ra prefix command, you must specify the valid-lifetime and preferred-lifetime parameters.

After modification:

* The no-advertise keyword was added to disable the device from advertising the prefix specified in the ipv6 nd ra prefix command.
* The valid-lifetime and preferred-lifetime parameters become optional. If you do not configure optional parameters for this command, the prefix uses the default settings configured by the ipv6 nd ra prefix default command.

# Modified feature: Setting the MTU of IPv6 packets sent over an interface

## Feature change description

The value range for the MTU of IPv6 packets sent over an interface was changed.

## Command changes

Syntax

ipv6 mtu size

undo ipv6 mtu

Views

Interface view

Change description

Before modification: The value range for the size argument is 1280 to 10240 bytes.

After modification: The value range for the size argument is 1280 to 1500 bytes.

# Modified feature: Displaying PBR configuration

## Feature change description

In this release, the display ip policy-based-route setup command can display the type of the policies.

## Command changes

### Modified command: display ip policy-based-route setup

Syntax

display ip policy-based-route setup

Views

Any view

Change description

Before modification: The command displays applied policies and interfaces to which the policies are applied.

<Sysname> display ip policy-based-route setup

Policy Name Interface Name

pr01 Vlan-interface 1

After modification: The command displays applied policies, interfaces to which the policies are applied, and type of the policies.

<Sysname> display ip policy-based-route setup

Policy name Type Interface

pr01 Forward Vlan-interface2

aaa Local N/A

Command output

|  |  |
| --- | --- |
| Field | Description |
| Type | Type of the PBR:   * + - * Forward—Interface PBR.       * Local—Local PBR. |

# Modified feature: Displaying IPv6 PBR configuration

## Feature change description

In this release, the display ipv6 policy-based-route setup command can display the type of the policies.

## Command changes

### Modified command: display ipv6 policy-based-route setup

Syntax

display ipv6 policy-based-route setup

Views

Any view

Change description

Before modification: The command displays applied IPv6 policies and interfaces to which the IPv6 policies are applied.

<Sysname> display ipv6 policy-based-route setup

Policy Name Interface Name

pr01 Vlan-interface 1

After modification: The command displays applied IPv6 policies, interfaces to which the IPv6 policies are applied, and type of the IPv6 policies.

<Sysname> display ipv6 policy-based-route setup

Policy name Type Interface

pr01 Forward Vlan-interface 2

pr02 Local N/A

Command output

|  |  |
| --- | --- |
| Field | Description |
| Type | Type of the IPv6 PBR:   * + - * Forward—Interface IPv6 PBR.       * Local—Local IPv6 PBR. |

# Modified feature: Creating an ACL

## Feature change description

The syntax of the acl command was changed.

## Command changes

### Modified command: acl

Old syntax

acl [ ipv6 ] number acl-number [ name acl-name ] [ match-order { auto | config } ]

undo acl [ ipv6 ] { all | name acl-name | number acl-number }

New syntax

acl [ ipv6 ] { advanced | basic } { acl-number | name acl-name } [ match-order { auto | config } ]

acl mac { acl-number | name acl-name } [ match-order { auto | config } ]

acl [ ipv6 ] number acl-number [ match-order { auto | config } ]

undo acl [ ipv6 ] { all | { advanced | basic } { acl-number | name acl-name } }

undo acl mac { all | acl-number | name acl-name }

undo acl [ ipv6 ] number acl-number

Views

System view

Change description

After modification:

* You can use the acl [ ipv6 ] number acl-number command to create an ACL or enter the view of an existing ACL.
* If an ACL is created by using the name acl-name option, you can use only the acl [ ipv6 | mac ] name acl-name command to enter the ACL view.

# Modified feature: Copying an ACL to create a new ACL

## Feature change description

The syntax of the acl copy command was changed.

## Command changes

### Modified command: acl copy

Old syntax

acl [ ipv6 ] copy { source-acl-number | name source-acl-name } to { dest-acl-number | name dest-acl-name }

New syntax

acl [ ipv6 | mac ] copy { source-acl-number | name source-acl-name } to { dest-acl-number | name dest-acl-name }

Views

System view

Change description

After modification, the mac keyword was required to specify a Layer 2 ACL.

# Modified feature: Displaying ACL configuration and match statistics

## Feature change description

The syntax of the display acl command was changed.

## Command changes

### Modified command: display acl

Old syntax

display acl [ ipv6 ] { acl-number | all | name acl-name }

New syntax

display acl [ ipv6 | mac ] { acl-number | all | name acl-name }

Views

Any view

Change description

After modification:

* The mac keyword was required to specify a Layer 2 ACL.
* The start rule ID was added in the command output.

# Modified feature: Displaying packet filtering statistics

## Feature change description

The syntax of the display packet-filter statistics command was changed.

## Command changes

### Modified command: display packet-filter statistics

Old syntax

display packet-filter statistics interface interface-type interface-number { inbound | outbound } [ [ ipv6 ] { acl-number | name acl-name } ] [ brief ]

New syntax

display packet-filter statistics interface interface-type interface-number { inbound | outbound } [ [ ipv6 | mac ] { acl-number | name acl-name } ] [ brief ]

Views

Any view

Change description

After modification, the mac keyword was required to specify a Layer 2 ACL.

# Modified feature: Displaying accumulated packet filtering statistics for an ACL

## Feature change description

The syntax of the display packet-filter statistics sum command was changed.

## Command changes

### Modified command: display packet-filter statistics sum

Old syntax

display packet-filter statistics sum { inbound | outbound } [ ipv6 ] { acl-number | name acl-name } [ brief ]

New syntax

display packet-filter statistics sum { inbound | outbound } [ ipv6 | mac ] { acl-number | name acl-name } [ brief ]

Views

Any view

Change description

After modification, the mac keyword was required to specify a Layer 2 ACL.

# Modified feature: Displaying ACL application details for packet filtering

## Feature change description

The syntax of the display packet-filter verbose command was changed.

## Command changes

### Modified command: display packet-filter verbose

Old syntax

display packet-filter verbose interface interface-type interface-number { inbound | outbound } [ [ ipv6 ] { acl-number | name acl-name } ] [ slot slot-number ]

New syntax

display packet-filter verbose interface interface-type interface-number { inbound | outbound } [ [ ipv6 | mac ] { acl-number | name acl-name } ] [ slot slot-number ]

Views

Any view

Change description

After modification, the mac keyword was required to specify a Layer 2 ACL.

# Modified feature: Applying an ACL to an interface for packet filtering

## Feature change description

The syntax of the packet-filter command was changed.

## Command changes

### Modified command: packet-filter

Old syntax

packet-filter [ ipv6 ] { acl-number | name acl-name } { inbound | outbound } [ hardware-count ]

undo packet-filter [ ipv6 ] { acl-number | name acl-name } { inbound | outbound }

New syntax

packet-filter [ ipv6 | mac ] { acl-number | name acl-name } { inbound | outbound } [ hardware-count ]

undo packet-filter [ ipv6 | mac ] { acl-number | name acl-name } { inbound | outbound }

Views

Layer 2 Ethernet interface view

VLAN interface view

Change description

After modification, the mac keyword was required to specify a Layer 2 ACL.

# Modified feature: Specify the applicable scope of packet filtering on a VLAN interface

## Feature change description

The syntax of the packet-filter filter command was changed.

## Command changes

### Modified command: packet-filter filter

Old syntax

packet-filter filter [ route | all ]

New syntax

packet-filter filter { route | all }

Views

VLAN interface view

Change description

After modification, you must specify the application scope for packet filtering on a VLAN interface.

# Modified feature: Clearing statistics for ACLs

## Feature change description

The syntax of the reset acl counter command was changed.

## Command changes

### Modified command: reset acl counter

Old syntax

reset acl [ ipv6 ] counter { acl-number | all | name acl-name }

New syntax

reset acl [ ipv6 | mac ] counter { acl-number | all | name acl-name }

Views

User view

Change description

After modification, the mac keyword was required to specify a Layer 2 ACL.

# Modified feature: Clearing the packet filtering statistics and accumulated statistics for an ACL

## Feature change description

The syntax of the reset packet-filter statistics command was changed.

## Command changes

### Modified command: reset packet-filter statistics

Old syntax

reset packet-filter statistics interface [ interface-type interface-number ] { inbound | outbound } [ [ ipv6 ] { acl-number | name acl-name } ]

New syntax

reset packet-filter statistics interface [ interface-type interface-number ] { inbound | outbound } [ [ ipv6 | mac ] { acl-number | name acl-name } ]

Views

User view

Change description

After modification, the mac keyword was required to specify a Layer 2 ACL.

# Modified feature: Specifying an ACL match criterion

## Feature change description

The syntax for specifying an ACL match criterion was changed.

## Command changes

### Modified command: if-match acl

Old syntax

if-match acl [ ipv6 ] { acl-number | name acl-name }

New syntax

if-match acl [ ipv6 | mac ] { acl-number | name acl-name }

Views

Traffic class view

Change description

The mac keyword was added to the if-match acl command for specifying a Layer 2 ACL.

# Modified feature: Displaying predefined control plane QoS policies of cards

## Feature change description

The display qos policy control-plane pre-defined command output was changed.

## Command changes

### Modified command: display qos policy control-plane pre-defined

Syntax

display qos policy control-plane pre-defined [ slot slot-number ]

Views

Any view

Change description

Command output before modification:

<Sysname> display qos policy control-plane pre-defined slot 1

Pre-defined policy information slot 1

Protocol Priority Bandwidth (kbps) Group

IS-IS 4 512 critical

VRRP 5 768 important

IGMP 3 256 important

VRRPv6 3 768 important

ARP 1 256 normal

DHCP Snooping 3 256 redirect

DHCP 3 256 normal

802.1x 1 128 important

STP 6 256 critical

LACP 5 64 critical

MVRP 3 256 critical

BGP 3 256 critical

ICMP 1 640 monitor

IPOPTION 2 64 normal

BGPv6 3 256 critical

IPOPTIONv6 2 64 normal

LLDP 3 128 important

DLDP 3 64 critical

TELNET 1 512 management

SSH 1 512 management

HTTP 1 64 management

HTTPS 1 64 management

ARP Snooping 1 256 redirect

ICMPv6 1 512 monitor

DHCPv6 3 256 normal

Command output after modification:

<Sysname> display qos policy control-plane pre-defined slot 1

Pre-defined policy information slot 1

Protocol Priority Bandwidth Group

Default N/A 0 (kbps) N/A

IS-IS 4 512 (kbps) critical

VRRP 35 768 (kbps) important

IGMP 3 256 (kbps) important

VRRPv6 35 768 (kbps) important

ARP 1 128 (kbps) normal

DHCP Snooping 3 256 (kbps) redirect

DHCP 3 256 (kbps) normal

802.1x 1 128 (kbps) important

STP 6 256 (kbps) critical

LACP 5 64 (kbps) critical

MVRP 3 256 (kbps) critical

BGP 3 256 (kbps) critical

ICMP 1 640 (kbps) monitor

IPOPTION 2 64 (kbps) normal

BGPv6 3 256 (kbps) critical

IPOPTIONv6 2 64 (kbps) normal

LLDP 3 128 (kbps) important

DLDP 3 64 (kbps) critical

TELNET 1 512 (kbps) management

SSH 1 512 (kbps) management

TACACS 1 512 (kbps) management

RADIUS 1 512 (kbps) management

HTTP 1 64 (kbps) management

HTTPS 1 64 (kbps) management

ARP Snooping 1 256 (kbps) redirect

ICMPv6 1 512 (kbps) monitor

DHCPv6 3 256 (kbps) normal

# Modified feature: Length range for an ISP domain

## Feature change description

The length range for an ISP domain name was changed.

## Command changes

### Modified commands: display domain, domain, domain default enable, domain if-unknown

Syntax

Any view:

display domain [ isp-name ]

System view:

domain isp-name

domain default enable isp-name

domain if-unknown isp-name

Views

Any view

System view

Change description

Before modification: The isp-name argument is a string of 1 to 24 characters.

After modification: The isp-name argument is a string of 1 to 255 characters.

# Modified feature: Displaying local user configuration

## Feature change description

Syntax was changed for the display local-user command to display local user configuration.

## Command changes

### Modified command: display local-user

Old syntax

display local-user [ class { manage | network } | service-type { ftp | http | https | lan-access | portal | ssh | telnet | terminal } | state { active | block } | user-name user-name | vlan vlan-id ]

New syntax

display local-user [ class { manage | network } | idle-cut { disable | enable } | service-type { ftp | http | https | lan-access | portal | ssh | telnet | terminal } | state { active | block } | user-name user-name class { manage | network } | vlan vlan-id ]

Views

Any view

Change description

Before modification:

* You cannot specify local users by the status of the idle cut feature.
* The user-name user-name option specifies all local users that have the specified username.

After modification:

* The idle-cut { disable | enable } option was added. This option specifies local users by the status of the idle cut feature.
* The class { manage | network } option was added before the user-name user-name option to specify device management users or network access users that have the specified username.

# Modified feature: Displaying user group configuration

## Feature change description

Syntax was changed for the display user-group command to display user group configuration.

## Command changes

### Modified command: display user-group

Old syntax

display user-group [ group-name ]

New syntax

display user-group { all | name group-name }

Views

Any view

Change description

Before modification: The group-name argument is optional. If you do not specify a user group, this command displays configuration for all user groups.

After modification:

* The all keyword was added. This keyword specifies all user groups.
* The name keyword was added before the group-name argument to specify a user group.
* You must specify either all or name group-name.

# Modified feature: Enabling the RADIUS server load sharing feature

## Feature change description

Syntax was changed for the command that enables the RADIUS server load sharing feature.

## Command changes

### Modified command: server-load-sharing enable

Old syntax

algorithm loading-share enable

undo algorithm loading-share enable

New syntax

server-load-sharing enable

undo server-load-sharing enable

Views

RADIUS scheme view

Change description

The syntax of this command was change from algorithm loading-share enable to server-load-sharing enable.

# Modified feature: Setting the real-time accounting interval

## Feature change description

Syntax was changed for the command that sets the real-time accounting interval, and the value range for the argument in this command was also changed.

## Command changes

### Modified command: timer realtime-accounting

Old syntax

timer realtime-accounting minutes

New syntax

timer realtime-accounting interval [ second ]

Views

RADIUS scheme view

Change description

Before modification:

* The value range for the minutes argument is 0 to 60.
* The real-time accounting interval is in minutes.

After modification:

* The value range for the interval argument is 0 to 71582.
* The second keyword was added. This keyword specifies the real-time accounting interval, in seconds. If you do not specify this keyword, the real-time accounting interval is in minutes.

# Modified feature: Displaying 802.1X information

## Feature change description

The Max 802.1X users field was removed from the output of the display dot1x command.

## Command changes

### Modified command: display dot1x

Syntax

display dot1x [ sessions | statistics ] [ interface interface-type interface-number ]

Views

Any view

Change description

Before modification: The Max 802.1X users field in the command output indicates the maximum number of online 802.1X users each device supports.

After modification: The Max 802.1X users field is removed from the command output. The output does not include the information about the maximum number of online 802.1X users each device supports.

# Modified feature: Port-specific mandatory 802.1X authentication domain

## Feature change description

The length range was changed for the ISP domain name string when you specify a mandatory 802.1X authentication domain on a port.

## Command changes

### Modified command: dot1x mandatory-domain

Syntax

dot1x mandatory-domain domain-name

Views

Layer 2 Ethernet interface view

Change description

Before modification: The value range for the domain-name argument is 1 to 24 characters.

After modification: The value range for the domain-name argument is 1 to 255 characters.

# Modified feature: Removing users from the MAC authentication critical VLAN on a port

## Feature change description

The syntax was changed for the command that removes users from the MAC authentication critical VLAN on a port.

## Command changes

### Modified command: reset mac-authentication critical vlan

Old syntax

reset mac-authentication critical-vlan interface interface-type interface-number [ mac-address mac-address ]

New syntax

reset mac-authentication critical vlan interface interface-type interface-number [ mac-address mac-address ]

Views

User view

Change description

The critical-vlan keyword was changed to critical vlan.

# Modified feature: Port security's limit on the number of secure MAC addresses on a port

## Feature change description

The value range was changed for setting the maximum number of secure MAC addresses that port security allows on a port.

## Command changes

### Modified command: port-security max-mac-count

Syntax

port-security max-mac-count max-count

Views

Layer 2 Ethernet interface view

Change description

Before modification: The value range for the max-count argument is 1 to 4294967295.

After modification: The value range for the max-count argument is 1 to 2147483647.

# Modified feature: Enabling the SSH server to support SSH1 clients

## Feature change description

From this release, the SSH server does not support SSH1 clients by default.

## Command changes

### Modified command: ssh server compatible-ssh1x

Syntax

ssh server compatible-ssh1x enable

undo ssh server compatible-ssh1x [ enable ]

Views

System view

Change description

Before modification: The SSH server supports SSH1 clients by default.

After modification: The SSH server does not support SSH1 clients by default.

# Modified feature: Creating an SSH user and specifying the service type and authentication method

## Feature change description

Support for specifying multiple SSH client public keys was added for an SSH user.

## Command changes

### Modified command: ssh user

Old syntax

In non-FIPS mode:

ssh user username service-type { all | netconf | scp | sftp | stelnet } authentication-type { password | { any | password-publickey | publickey } [ assign { pki-domain domain-name | publickey keyname } ] }

In FIPS mode:

ssh user username service-type { all | netconf | scp | sftp | stelnet } authentication-type { password | password-publickey [ assign { pki-domain domain-name | publickey keyname } ] }

New syntax

In non-FIPS mode:

ssh user username service-type { all | netconf | scp | sftp | stelnet } authentication-type { password | { any | password-publickey | publickey } [ assign { pki-domain domain-name | publickey keyname&<1-6> } ] }

In FIPS mode:

ssh user username service-type { all | netconf | scp | sftp | stelnet } authentication-type { password | password-publickey [ assign { pki-domain domain-name | publickey keyname&<1-6> } ] }

Views

System view

Change description

After modification, you can specify multiple SSH client public keys for client verification.

# Modified feature: Predefined user roles for SSH and FTP client commands

## Feature change description

The predefined user roles for the following SSH and FTP client commands were changed:

* bye
* exit
* help
* quit

## Command changes

### Modified command: bye

Syntax

bye

Views

SFTP client view

FTP client view

Change description

Before modification, the predefined user role for this command is network-admin.

After modification, the predefined user roles for this command are network-admin and network-operator.

### Modified command: exit

Syntax

exit

Views

SFTP client view

Change description

Before modification, the predefined user role for this command is network-admin.

After modification, the predefined user roles for this command are network-admin and network-operator.

### Modified command: help

Syntax

help

Views

SFTP client view

FTP client view

Change description

Before modification, the predefined user role for this command is network-admin.

After modification, the predefined user roles for this command are network-admin and network-operator.

### Modified command: quit

Syntax

quit

Views

SFTP client view

FTP client view

Change description

Before modification, the predefined user role for this command is network-admin.

After modification, the predefined user roles for this command are network-admin and network-operator.

# Modified feature: Setting the number of ARP blackhole route probes for each unresolved IP address

## Feature change description

The default value of ARP blackhole route probes for each unresolved IP address was changed from one to three.

## Command changes

### Modified command: arp resolving-route probe-count

Syntax

arp resolving-route probe-count count

undo arp resolving-route probe-count

Views

System view

Change description

Before modification: The device performs one ARP blackhole route probe for each unresolved IP address by default.

After modification: The device performs three ARP blackhole route probes for each unresolved IP address by default.

# Modified feature: Displaying information about SNMPv1 or SNMPv2c communities

## Feature change description

The ACL name field was added to the output from the display snmp-agent community command.

## Command changes

### Modified command: display snmp-agent community

Syntax

display snmp-agent community [ read | write ]

Views

Any view

Change description

Before modification:

<Sysname> display snmp-agent community

Community name: aa

Group name: aa

ACL:2001

Storage-type: nonVolatile

Context name: con1

After modification:

<Sysname> display snmp-agent community

Community name: aa

Group name: aa

ACL:2001

Storage-type: nonVolatile

Context name: con1

Community name: cc

Group name: cc

ACL name: testacl

Storage-type: nonVolatile

The ACL name field appears only when an ACL name is specified for the SNMPv1 or SNMPv2c community. It is exclusive with the ACL field.

# Modified feature: Displaying information about SNMP groups

## Feature change description

The ACL name field was added to the output from the display snmp-agent group command.

## Command changes

### Modified command: display snmp-agent group

Syntax

display snmp-agent group [ group-name ]

Views

Any view

Change description

Before modification:

<Sysname> display snmp-agent group

Group name: groupv3

Security model: v3 noAuthnoPriv

Readview: ViewDefault

Writeview: <no specified>

Notifyview: <no specified>

Storage-type: nonVolatile

After modification:

<Sysname> display snmp-agent group

Group name: groupv3

Security model: v3 noAuthnoPriv

Readview: ViewDefault

Writeview: <no specified>

Notifyview: <no specified>

Storage-type: nonVolatile

ACL name: testacl

The ACL name field appears only when an ACL name is specified for the SNMP group. It is exclusive with the ACL field.

# Modified feature: Displaying SNMPv3 user information

## Feature change description

The ACL name field was added to the output from the display snmp-agent usm-user command.

## Command changes

### Modified command: display snmp-agent usm-user

Syntax

display snmp-agent usm-user [ engineid engineid | group group-name | username user-name ] \*

Views

Any view

Change description

Before modification:

<Sysname> display snmp-agent usm-user

Username: userv3

Group name: mygroupv3

Engine ID: 800063A203000FE240A1A6

Storage-type: nonVolatile

UserStatus: active

After modification:

<Sysname> display snmp-agent usm-user

Username: userv3

Group name: mygroupv3

Engine ID: 800063A203000FE240A1A6

Storage-type: nonVolatile

UserStatus: active

ACL: 2000

Username: userv3

Group name: mygroupv3

Engine ID: 8000259503000BB3100A508

Storage-type: nonVolatile

UserStatus: active

ACL name: testacl

The ACL name field appears only when an ACL name is specified for the SNMPv3 user. It is exclusive with the ACL field.

# Modified feature: Configuring an SNMPv1 or SNMPv2c community

## Feature change description

The name ipv4-acl-name and name ipv6-acl-name options and advanced ACLs were supported for configuring an SNMP community.

## Command changes

### Modified command: snmp-agent community

Old syntax

In VACM mode:

snmp-agent community { read | write } [ simple | cipher ] community-name [ mib-view view-name ] [ acl acl-number | acl ipv6 ipv6-acl-number ] \*

In RBAC mode:

snmp-agent community [ simple | cipher ] community-name user-role role-name [ acl acl-number | acl ipv6 ipv6-acl-number ] \*

New syntax

In VACM mode:

snmp-agent community { read | write } [ simple | cipher ] community-name [ mib-view view-name ] [ acl { ipv4-acl-number | name ipv4-acl-name } | acl ipv6 { ipv6-acl-number | name ipv6-acl-name } ] \*

In RBAC mode:

snmp-agent community [ simple | cipher ] community-name user-role role-name [ acl { ipv4-acl-number | name ipv4-acl-name } | acl ipv6 { ipv6-acl-number | name ipv6-acl-name } ] \*

Views

System view

Change description

Before modification: You can specify a basic IPv4/IPv6 ACL by its number for an SNMP community.

After modification:

* You can specify a basic or advanced IPv4/IPv6 ACL by its number for an SNMP community.
* You can specify a basic or advanced IPv4/IPv6 ACL by its name for an SNMP community.

# Modified feature: Creating an SNMP group

## Feature change description

The name ipv4-acl-name and name ipv6-acl-name options and advanced ACLs were supported for creating an SNMP group.

## Command changes

### Modified command: snmp-agent group

Old syntax

SNMPv1 and SNMP v2c:

snmp-agent group { v1 | v2c } group-name [ read-view view-name ] [ write-view view-name ] [ notify-view view-name ] [ acl acl-number | acl ipv6 ipv6-acl-number ] \*

SNMPv3 (in non-FIPS mode):

snmp-agent group v3 group-name [ authentication | privacy ] [ read-view read-view ] [ write-view write-view ] [ notify-view notify-view ] [ acl acl-number | acl ipv6 ipv6-acl-number ] \*

SNMPv3 (in FIPS mode):

snmp-agent group v3 group-name { authentication | privacy } [ read-view read-view ] [ write-view write-view ] [ notify-view notify-view ] [ acl acl-number | acl ipv6 ipv6-acl-number ] \*

New syntax

SNMPv1 and SNMP v2c:

snmp-agent group { v1 | v2c } group-name [ read-view view-name ] [ write-view view-name ] [ notify-view view-name ] [ acl { ipv4-acl-number | name ipv4-acl-name } | acl ipv6 { ipv6-acl-number | name ipv6-acl-name } ] \*

SNMPv3 (in non-FIPS mode):

snmp-agent group v3 group-name [ authentication | privacy ] [ read-view read-view ] [ write-view write-view ] [ notify-view notify-view ] [ acl { ipv4-acl-number | name ipv4-acl-name } | acl ipv6 { ipv6-acl-number | name ipv6-acl-name } ] \*

SNMPv3 (in FIPS mode):

snmp-agent group v3 group-name { authentication | privacy } [ read-view read-view ] [ write-view write-view ] [ notify-view notify-view ] [ acl { ipv4-acl-number | name ipv4-acl-name } | acl ipv6 { ipv6-acl-number | name ipv6-acl-name } ] \*

Views

System view

Change description

Before modification: You can specify a basic IPv4/IPv6 ACL by its number for an SNMP group.

After modification:

* You can specify a basic or advanced IPv4/IPv6 ACL by its number for an SNMP group.
* You can specify a basic or advanced IPv4/IPv6 ACL by its name for an SNMP group.

# Modified feature: Creating an SNMPv1 or SNMPv2c user

## Feature change description

The name ipv4-acl-name and name ipv6-acl-name options and advanced ACLs were supported for creating an SNMPv1/SNMPv2c user.

## Command changes

### Modified command: snmp-agent usm-user { v1 | v2c }

Old syntax

snmp-agent usm-user { v1 | v2c } user-name group-name [ acl acl-number | acl ipv6 ipv6-acl-number ] \*

New syntax

snmp-agent usm-user { v1 | v2c } user-name group-name [ acl { ipv4-acl-number | name ipv4-acl-name } | acl ipv6 { ipv6-acl-number | name ipv6-acl-name } ] \*

Views

System view

Change description

Before modification: You can specify a basic IPv4/IPv6 ACL by its number for an SNMPv1/SNMPv2c user.

After modification:

* You can specify a basic or advanced IPv4/IPv6 ACL by its number for an SNMPv1/SNMPv2c user.
* You can specify a basic or advanced IPv4/IPv6 ACL by its name for an SNMPv1/SNMPv2c user.

# Modified feature: Creating an SNMPv3 user

## Feature change description

The name ipv4-acl-name and name ipv6-acl-name options and advanced ACLs were supported for creating an SNMPv3 user.

The following encryption algorithms were added for creating an SNMPv3 user:

* In FIPS mode—aes192 and aes256 encryption algorithms.
* In non-FIPS mode—3des, aes192, and aes256 encryption algorithms in VACM mode and aes192 and aes256 encryption algorithms in RBAC mode.

## Command changes

### Modified command: snmp-agent usm-user v3

Old syntax

In non-FIPS mode (in VACM mode):

snmp-agent usm-user v3 user-name group-name [ remote { ip-address | ipv6 ipv6-address } ] [ { cipher | simple } authentication-mode { md5 | sha } auth-password [ privacy-mode { aes128 | des56 } priv-password ] ] [ acl acl-number | acl ipv6 ipv6-acl-number ] \*

In non-FIPS mode (in RBAC mode):

snmp-agent usm-user v3 user-name user-role role-name [ remote { ip-address | ipv6 ipv6-address } ] [ { cipher | simple } authentication-mode { md5 | sha } auth-password [ privacy-mode { aes128 | 3des | des56 } priv-password ] ] [ acl acl-number | acl ipv6 ipv6-acl-number ] \*

In FIPS mode (in VACM mode):

snmp-agent usm-user v3 user-name group-name [ remote { ip-address | ipv6 ipv6-address } ] { cipher | simple } authentication-mode sha auth-password [ privacy-mode aes128 priv-password ] [ acl acl-number | acl ipv6 ipv6-acl-number ] \*

In FIPS mode (in RBAC mode):

snmp-agent usm-user v3 user-name user-role role-name [ remote { ip-address | ipv6 ipv6-address } ] [ { cipher | simple } authentication-mode sha auth-password [ privacy-mode aes128 priv-password ] ] [ acl acl-number | acl ipv6 ipv6-acl-number ] \*

New syntax

In non-FIPS mode (in VACM mode):

snmp-agent usm-user v3 user-name group-name [ remote { ipv4-address | ipv6 ipv6-address }] [ { cipher | simple } authentication-mode { md5 | sha } auth-password [ privacy-mode { 3des | aes128 | aes192 | aes256 | des56 } priv-password ] ] [ acl { ipv4-acl-number | name ipv4-acl-name } | acl ipv6 { ipv6-acl-number | name ipv6-acl-name } ] \*

In non-FIPS mode (in RBAC mode):

snmp-agent usm-user v3 user-name user-role role-name [ remote { ipv4-address | ipv6 ipv6-address } ] [ { cipher | simple } authentication-mode { md5 | sha } auth-password [ privacy-mode { 3des | aes128 | aes192 | aes256 | des56 } priv-password ] ] [ acl { ipv4-acl-number | name ipv4-acl-name } | acl ipv6 { ipv6-acl-number | name ipv6-acl-name } ] \*

In FIPS mode (in VACM mode):

snmp-agent usm-user v3 user-name group-name [ remote { ipv4-address | ipv6 ipv6-address } ] { cipher | simple } authentication-mode sha auth-password [ privacy-mode { aes128 | aes192 | aes256 } priv-password ] [ acl { ipv4-acl-number | name ipv4-acl-name } | acl ipv6 { ipv6-acl-number | name ipv6-acl-name } ] \*

In FIPS mode (in RBAC mode):

snmp-agent usm-user v3 user-name user-role role-name [ remote { ipv4-address | ipv6 ipv6-address } ] [ { cipher | simple } authentication-mode sha auth-password [ privacy-mode { aes128 | aes192 | aes256 } priv-password ] ] [ acl { ipv4-acl-number | name ipv4-acl-name } | acl ipv6 { ipv6-acl-number | name ipv6-acl-name } ] \*

Views

System view

Change description

Before modification: You can specify a basic IPv4/IPv6 ACL by its number for an SNMPv3 user.

After modification:

* You can specify a basic or advanced IPv4/IPv6 ACL by its number for an SNMPv3 user user.
* You can specify a basic or advanced IPv4/IPv6 ACL by its name for an SNMPv3 user.

The following parameters were added to the command:

* In FIPS mode—The name ipv4-acl-name and name ipv6-acl-name options and the aes192 and aes256 keywords.
* In non-FIPS mode—The name ipv4-acl-name and name ipv6-acl-name options and the 3des, aes192, and aes256 keywords in VACM mode and aes192 and aes256 keywords in RBAC mode.

# Modified feature: Configuration locking BY NETCONF

## Feature change description

Before modification: After a user uses NETCONF to lock the configuration, other users cannot use NETCONF to configure the device but can use other configuration methods, such as CLI and SNMP.

After modification: After a user uses NETCONF to lock the configuration, other users cannot use NETCONF or any other methods to configure the device.

## Command changes

None.

# Modified feature: Value range for the interval for an OpenFlow instance to reconnect to a controller

## Feature change description

The value range changed for the interval for an OpenFlow instance to reconnect to a controller.

## Command changes

### Modified command: controller connect interval

Syntax

controller connect interval interval

undo controller connect interval

Views

OpenFlow instance view

Change description

Before modification: The value range for the interval argument is 10 to 120 seconds.

After modification: The value range for the interval argument is 1 to 120 seconds.

# Removed features

Removed features in version R3207

| Feature | Removed commands |
| --- | --- |
| IPv6 basics: Enabling a device to discard IPv6 packets that contain extension headers | The ipv6 option drop enable command was removed from system view. |
| QoS: Configuring traffic policing for all traffic on inbound interface by using the non-MQC approach | * + - * The following commands were removed from Layer 2 Ethernet interface view:         + qos car inbound any cir committed-information-rate [ cbs committed-burst-size [ ebs excess-burst-size ] ] [ green action | red action | yellow action ]         + qos car inbound any cir committed-information-rate [ cbs committed-burst-size ] pir peak-information-rate [ ebs excess-burst-size ] [ green action | red action | yellow action ]       * The display qos car interface [ interface-type interface-number ] command was removed from any view. |
| QoS: Configuring the bandwidth guaranteeing group | * + - * The qos nni bandwidth bandwidth-value command was removed from system view.       * The qos uni enable command was removed from Layer 2 Ethernet interface view.       * The following commands were removed from any view:         + display qos nni bandwidth         + display qos uni interface [ interface-type interface-number ] |
| AAA: Specifying a security policy server for a RADIUS scheme | The security-policy-server { ipv4-address | ipv6 ipv6-address } command was removed from RADIUS scheme view. |
| IKE: Specifying a DH group for key negotiation in phase 1 | In FIPS mode, the group24 keyword was removed from the dh command in IKE proposal view. |

1. Related documentation

This document introduces software feature changes between HPE 5130EI-CMW710-R3207 and later versions. For information about software feature changes between software versions earlier than HPE 5130EI-CMW710-R3207, see HPE 5130EI-CMW710-R3115P08 Release Notes (Software Feature Changes).