Hewlett Packard Enterprise

HPE A5500EI-CMW520-R2222P12 Release Notes

Contents

List of tables

Introduction

This document describes the features, restrictions and guidelines, open problems, and workarounds for version A5500EI-CMW520-R2222P12. Before you use this version on a live network, back up the configuration and test the version to avoid software upgrade affecting your live network.

Use this document in conjunction with *HPE A5500EI-CMW520-R2222P12 Release Notes (Software Feature Changes)* and the documents listed in "Related documents."

Version information

Version number

Comware software, Version 5.20.99, Release 2222P12

Note: You can see the version information with the command **display version** in any view. See **Note①.**

Version history

IMPORTANT:

The software feature changes listed in the version history table for each version are not complete. To obtain complete information about all software feature changes in each version, see the *Software Feature Changes* document for this release notes.

Table 1 Version history

Version number	Last version	Release Date	Release type	Remarks
A5500EI-CMW520-R2222P12	A5500EI-CMW520-R2222P09	2019-01-21	Release version	Fixed bugs
A5500EI-CMW520-R2222P09	A5500EI-CMW520-R2222P08	2018-04-11	Release version	This version fixed bugs and introduced feature changes. Modified feature include: • RADIUS Calling-Station-ID attribute value for the login service • Port security need to know feature
A5500EI-CMW520-R2222P08	A5500EI-CMW520-R2222P07	2017-10-16	Release version	Fixed bugs.
A5500EI-CMW520-R2222P07	A5500EI-CMW520-R2222P05	2017-08-03	Release version	This version fixed bugs and introduced feature changes. New features include: • Configuring the action a port takes after it receives an Ethernet OAM event from the

				remote end
A5500EI-CMW520-R2222P05	A5500EI-CMW520-R2222P02	2017-03-31	Release version	Fixed bugs.
A5500EI-CMW520-R2222P02	A5500EI-CMW520-R2221P30	2017-01-10	Release version	• New features: • Modified feature: 1. Uploading IPv6 addresses for 802.1X and MAC authentication users • Fixed bugs
A5500EI-CMW520-R2221P30	A5500EI-CMW520-R2221P25	2016-08-31	Release version	• New features: 1. Including user IP addresses in realtime accounting packets for MAC authentication users with dynamic IP addresses 2．Ignoring the ingress ports of ARP packets during user validity check 3．Authorization VLAN auto-tagging for MAC authentication • Modified feature: 1．Specifying file name for storing DHCP snooping entries on a remote server 2．Confining RADIUS Vendor-Specific extended attributes to a specific vendor • Fixed bugs
A5500EI-CMW520-R2221P25	A5500EI-CMW520-R2221P22	2016-03-31	Release version	• New features: 1. Configuring periodic MAC re-authentication messages • Modified feature: • Fixed bugs
A5500EI-CMW520-R2221P22	A5500EI-CMW520-R2221P20	2016-01-31	Release version	• New features: 1. Enabling sending of ICMPv6 redirect messages • Modified feature: 1. Disabling advertising prefix information in RA messages • Fixed bugs
A5500EI-CMW520-R2221P20	A5500EI-CMW520-R2221P19	2015-10-31	Release version	• New features: 1.MAC authentication voice VLAN 2.Generating the random number entropy and saving it to a file • Fixed bugs

A5500EI-CMW520-R2221P19	A5500EI-CMW520-R2221P18	2015-09-31	Release version	• Fixed bugs
A5500EI-CMW520-R2221P18	A5500EI-CMW520-R2221P15	2015-08-31	Release version	• New features: 1.Sending EAP-Success packets to 802.1X users in critical VLAN • Modified feature: 1.VPN instance support for NQA server configuration • Fixed bugs
A5500EI-CMW520-R2221P15	A5500EI-CMW520-R2221P12	2015-07-09	Release version	• Fixed bugs
A5500EI-CMW520-R2221P12	A5500EI-CMW520-R2221P10	2015-06-22	Release version	• New features: 1.Login delay 2. IPv6 address with a 127-bit prefix length • Fixed bugs
A5500EI-CMW520-R2221P10	A5500EI-CMW520-R2221P08	2015-04-28	Release version	• New features: 1.Support for NTP configuration in IPv6 networks • Fixed bugs
A5500EI-CMW520-R2221P08	A5500EI-CMW520-R2221P07	2015-02-03	Release version	• New features: 1.Applicable scope of packet filtering on a VLAN interface 2.SNMP notifications for PVST topology changes 3.Disabling SSL 3.0 • Fixed bugs
A5500EI-CMW520-R2221P07	A5500EI-CMW520-R2221P06	2014-12-22	Release version	• New features: 1.802.1X MAC address binding 2.Automatic PI reset • Fixed bugs
A5500EI-CMW520-R2221P06	A5500EI-CMW520-R2221P05	2014-10-31	Release version	• Fixed bugs

A5500EI-CMW520-R2221P05	A5500EI-CMW520-R2221P04	2014-08-29	Release version	• New features: 1.Telnet/SSH user connection control 2.Packet rate-limiting for the table-miss flow entry • Modified feature: 1.Including time zone information in the timestamp of system information sent to a log host 2. Configuring physical state change suppression on an Ethernet interface 3. Configuring a tag and description for an IPv6 static route • Fixed bugs
A5500EI-CMW520-R2221P04	A5500EI-CMW520-R2221P02	2014-07-15	Release version	• New features: 1.802.1X voice VLAN 2.Configuring the uplink port to permit multiple isolate-user-VLANs 3.TCP fragment attack protection 4.Portal roaming • Modified feature: 1.Username request timeout timer for 802.1X authentication 2.Default configuration • Fixed bugs
A5500EI-CMW520-R2221P02	A5500EI-CMW520-R2221P01	2014-04-30	Release version	• New features: 1.Support for BPDU guard configuration in interface or port group view; 2. MAC re-authentication timer for users in guest VLAN; 3. Specifying the IPv4/IPv6 VRRP version; 4. MAC and port uniqueness check by the DHCP snooping device; • Modified feature: 1. Auto status transition of dynamic secure MAC addresses 2.The maximum number of gateways supported in MFF automatic mode • Fixed bugs
A5500EI-CMW520-R2221P01	A5500EI-CMW520-R2221	2014-02-28	Release version	• New features: Discarding IPv6 packets that contain extension headers • Fixed bugs

A5500EI-CMW520-R2221	A5500EI-CMW520-R2220P11	2013-12-31	Release version	• New features: 1. SSL server policy association with the FTP service; 2. OpenFlow; • Modified features: 1. Setting the device name; 2. Displaying brief IP configuration for Layer 3 interfaces; 3. Configuring static multicast MAC address entries; 4. Specifying the username and password to log in to the SCP server; 5. Disabling an untrusted port from recording clients' IP-to-MAC bindings; 6. Customizing DHCP options; • Fixed bugs
A5500EI-CMW520-R2220P11	A5500EI-CMW520-R2220P10	2013-12-06	Release version	• Fixed bugs
A5500EI-CMW520-R2220P10	A5500EI-CMW520-R2220P09	2013-10-30	Release version	• New features: 1. Specifying multiple public keys for an SSH user; • Fixed bugs
A5500EI-CMW520-R2220P09	A5500EI-CMW520-R2220P02P07	2013-09-30	Release version	• Modified features: 1.Specifying multiple secondary HWTACACS servers; • Fixed bugs
A5500EI-CMW520-R2220P07	A5500EI-CMW520-R2220P02L06	2013-06-30	Release version	• New features: 1.Configuring the ARP detection logging function • Modified features: 1.CWMP; • Fixed bugs
A5500EI-CMW520-R2220L06	A5500EI-CMW520-R2220P02	2013-04-22	Release version	• New features: 1.802.1X-based dynamic IPv4 source guard binding entries 2.Multicast ND 3.Configuring packet capture 4.Enabling MAC authentication multi-VLAN mode 5.Binding IP, MAC, and port on Web • Modified features: 1.Configuring system

				information for the SNMP agent • Fixed bugs
A5500EI-CMW520-R2220P02	A5500EI-CMW520-R2220	2013-04-10	Release version	• New features: None • Modified features: 1.Enabling/disabling FIPS mode; 2.Setting the IRF link down report delay; 3.Setting the minimum password length; 4.Switching the user privilege level; 5.Implementing ACL-based IPsec; 6.Cluster management; 7.Upgrading a subordinate member; • Fixed bugs
A5500EI-CMW520-R2220	A5500EI-CMW520-F2218L02	2013-01-09	Release version	• New features: 1.Disabling password recovery capacity; 2.Configuring a port to forward 802.1X EAPOL packets untagged; 3.Enabling source IP conflict prompt; 4.Delaying the MAC authentication; 5.Disabling MAC entry aging timer refresh based on destination MAC address; 6.Setting the deletion delay time for SAVI; • Fixed bugs
A5500EI-CMW520-F2218L02	A5500EI-CMW520-F2218P01	2012-11-09	Feature version	• New features:None • Modified features: 1.changing the VRF instances per VLAN interface from 128 to 1023; • Fixed bugs
A5500EI-CMW520-F2218P01	A5500EI-CMW520-F2218	2012-10-24	Feature version	• Modified features: 1. Default configuration. • Fixed bugs
A5500EI-CMW520-F2218	A5500EI-CMW520-F2217	2012-09-28	Feature version	• New features: 1.Supporting using a self-signed certificate for HTTPS; 2.Setting the maximum number of 802.1X authentication attempts for MAC authentication users; 3.Support of 802.1X for

				issuing VLAN groups; 4.Enabling MAC address migration log notifying; • Modified features: 1.Cluster management; • Removed features: 1.WiNet; • Fixed bugs
A5500EI-CMW520-F2217	A5500EI-CMW520-R2215	2012-08-31	Feature version	• New features: 1.Automatic configuration file backup for software downgrading; 2.FIPS; 3.Configuring ACL-based IPsec; 4.IKE; 5.Verifying the correctness and integrity of the file; • Modified features: 1.Configuring a password for the local user; 2.Clearing all users from the password control blacklist; 3.802.1X critical VLAN; 4.MAC authentication critical VLAN; 5.Modifying CLI configuration commands executed in FIPS mode for CC evaluation; 6.Modifying login management commands executed in FIPS mode for CC evaluation; 7.Modifying software upgrade commands executed in FIPS mode for CC evaluation; 8.Modifying security commands executed in FIPS mode for CC evaluation; 9.Modifying SNMP commands executed in FIPS mode for CC evaluation; • Fixed bugs
A5500EI-CMW520-R2215	A5500EI-CMW520-F2212	2012-04-28	Release version	• New features: 1. Interface range configuration; 2. NTPv4; 3. Changing the brand name; 4. Remaining POE power display by slot for IRF; 5. Configuring LLDP to advertise a specific voice

				VLAN; 6. Set the maximum number of Selected ports for the aggregation group; • Fixed bugs
A5500EI-CMW520-F2212	A5500EI-CMW520-F2211	2012-02-24	Feature version	• New features: 1.Setting the DSCP value for multiple types of protocol packets; 2.Portal authentication in IPv6 networks; • Modified features: 1. Modified password/key related configuration. For more information, see Feature and Command Change History for HP A5500EI-CMW520-F2212; • Fixed bugs
A5500EI-CMW520-F2211	A5500EI-CMW520-R2210	2011-11-30	Feature version	• New features: 1.Critical VLAN ; 2.SCP(Secure copy) ; 3.Configuring a source interface for DNS packets; 4.MVRP(Multiple VLAN Registration Protocol) ; 5.Enabling LLDP to automatically discover IP phones;
A5500EI-CMW520-R2210	A5500EI-CMW520-R2208	2011-9-16	Release version	• New features: 1.SAVI (Source Address Validation) ; 2.Global IP address binding ; 3.Layer-3 Combo port ; 4.PVST+ ; 5.Configuring secure addresses to age without being triggered by traffic 6.Set Sticky MAC addresses as dynamic secure MAC addresses 7.Dot1dTpFdbTable of RFC 1493 8.Encryption of shared keys for HWTACACS packets 9.DHCP snooping option 82 support for sub-option 9 10.Obtaining receiving power of optical modules through MIB 11.Obtaining utilization of H3C device ACL resources through MIB 12.Super VLAN for IPv6

				13.Local proxy ND 14.Easy configuration for Isolate-user-VLAN 15.CWMP (CPE WAN Management Protocol) 16.PIM Snooping 17.IPv6 PIM Snooping 18.STP TC-Snooping 19.IPv6 routing protocols for MCE 20.Configurable Jumbo frame size 21.Restore port-based default settings 22.WFQ support for SP/WRR/DRR 23.WEB based Triple authentication configuration 24.Collaboration between Smart Link and CFD CC detection 25.PoE power negotiation through Power Via MDI TLV 26.Port aggregation priority effective in static aggregation groups 27.OSPFv3 BFD 28.ISISv6 BFD 29.PIM BFD 30.IPv6 PIM BFD 31.SSH2 IPv6 32.SFTP IPv6 33.MAC address roaming 34.Loose URPF 35.Configurable minimum number of ports in an aggregation group 36.Keyword vpn-instance added for the telnet ipv6 command 37.Keyword vpn-instance added for the ftp ipv6 command 38.Keyword vpn-instance added for the tftp ipv6 command 39.Restoring the default operating mode for CDP-compatible LLDP 40.DHCP snooping support for packet rate limit
A5500EI-CMW520-R2208	S5500EI-CMW520-R2208	2011-6-17	Release version	• New features: 1. ipv6 neighbor stale-aging;

Hardware and software compatibility matrix

△ **CAUTION:**

To avoid an upgrade failure, use Table 3 to verify the hardware and software compatibility before performing an upgrade.

Before HP A5500EI family, there were another 2 product families, i.e. 3Com 4800G and H3C S5500EI, shipped to market. All of these three product families have same hardware and software specification except brand. The product matrix is as following. In brief, the HP A5500EI will be the representation to all of them in subsequent document.

Table 2 Product family matrix

HP A5500EI	3Com 4800G	H3C S5500EI
HP A5500-24G EI	Switch 4800G 24-Port	H3C S5500-28C-EI
HP A5500-48G EI	Switch 4800G 48-Port	H3C S5500-52C-EI
HP A5500-24G-PoE+ EI	Switch 4800G 24-Port PWR	H3C S5500-28C-PWR-EI
HP A5500-48G-PoE+ EI	Switch 4800G 48-Port PWR	H3C S5500-52C-PWR-EI
HP A5500-24G-SFP EI	Switch 4800G 24-Port SFP	H3C S5500-28F-EI
HP A5500-24G EI TAA	Switch 4800G 24-Port	H3C S5500-28C-EI
HP A5500-48G EI TAA	Switch 4800G 48-Port	H3C S5500-52C-EI
HP A5500-24G-SFP EI TAA	Switch 4800G 24-Port SFP	H3C S5500-28F-EI
HP A5500-24G-PoE+ EI TAA	Switch 4800G 24-Port PWR	H3C S5500-28C-PWR-EI
HP A5500-48G-PoE+ EI TAA	Switch 4800G 48-Port PWR	H3C S5500-52C-PWR-EI

Table 3 Hardware and software compatibility matrix

Item	Specifications
Product family	HP A5500 EI series H3C S5500-EI series 3Com Switch 4800G series

Item	Specifications
Hardware platform	HP A5500-24G EI Switch with 2 Interface Slots HP A5500-48G EI Switch with 2 Interface Slots HP A5500-24G-PoE+ EI Switch with 2 Interface Slots HP A5500-48G-PoE+ EI Switch with 2 Interface Slots HP A5500-24G-SFP EI Switch with 2 Interface Slots HP A5500-24G EI TAA Switch with 2 Interface Slots HP A5500-48G EI TAA Switch with 2 Interface Slots HP A5500-24G-SFP EI TAA Switch with 2 Interface Slots HP A5500-24G-PoE+ EI TAA Switch with 2 Interface Slots HP A5500-48G-PoE+ EI TAA Switch with 2 Interface Slots H3C S5500-28C-EI H3C S5500-52C-EI H3C S5500-28C-PWR-EI H3C S5500-52C-PWR-EI H3C S5500-28C-EI-DC H3C S5500-28F-EI Switch 4800G 24-Port Switch 4800G 48-Port Switch 4800G 24-Port PWR Switch 4800G 48-Port PWR Switch 4800G 24-Port SFP
Minimum memory requirements	256 MB
Minimum Flash requirements	32 MB
Boot ROM version	Version 721 or higher (See **Note②**)
System software image	A5500EI-CMW520-R2222P12.bin
IMC	iMC BIMS 7.3 (E0501) iMC EAD 7.3 (E0502) iMC TAM 7.3 (E0503) iMC UAM 7.3 (E0503) iMC NTA 7.3（E0502) iMC PLAT 7.3 (E0504) iMC QoSM 7.3 (E0502) iMC RAM 7.3 (E0501) iMC SHM 7.3 (E0502)
iNode	iNode PC7.3 (E0504)

Display version information on the A5500EI switch:

```
<HPE>display version
HPE Comware Platform Software
Comware Software, Version 5.20.99, Release 2222P12    ---------------Note①
Comware Platform Software Version COMWAREV500R002B99D077
HP A5500-48G EI Switch with 2 Interface Slots Software Version V200R002B07D077
```

```
Copyright (c) 2010-2018 Hewlett Packard Enterprise Development LP
Compiled Dec 26 2018 17:19:16, RELEASE SOFTWARE
HP A5500-48G EI Switch with 2 Interface Slots uptime is 0 week, 0 day, 18 hours,
14 minutes

HP A5500-48G EI Switch with 2 Interface Slots with 1 Processor
256M    bytes SDRAM
32768K  bytes Flash Memory

Hardware Version is REV.C
CPLD Version is 002
Bootrom Version is 721          ---------------------------------Note②
[SubSlot 0] 48GE+4SFP Hardware Version is REV.C
[SubSlot 1] 2 CX4 Hardware Version is REV.A
[SubSlot 2] 2 SFP+ Hardware Version is REV.A
```

Table 4 ISSU compatibility matrix

Current version	History version	ISSU compatibility
A5500EI-CMW520-R2222P12	A5500EI-CMW520-R2222P09	Incompatible
	A5500EI-CMW520-R2222P08	Incompatible
	A5500EI-CMW520-R2222P07	Incompatible
	A5500EI-CMW520-R2222P05	Incompatible
	A5500EI-CMW520-R2222P02	Incompatible
	A5500EI-CMW520-R2221P30	Incompatible
	A5500EI-CMW520-R2221P25	Incompatible
	A5500EI-CMW520-R2221P22	Incompatible
	A5500EI-CMW520-R2221P20	Incompatible
	A5500EI-CMW520-R2221P19	Incompatible
	A5500EI-CMW520-R2221P18	Incompatible
	A5500EI-CMW520-R2221P15	Incompatible
	A5500EI-CMW520-R2221P12	Incompatible
	A5500EI-CMW520-R2221P10	Incompatible
	A5500EI-CMW520-R2221P08	Incompatible
	A5500EI-CMW520-R2221P07	Incompatible
	A5500EI-CMW520-R2221P06	Incompatible
	A5500EI-CMW520-R2221P05	Incompatible
	A5500EI-CMW520-R2221P04	Incompatible
	A5500EI-CMW520-R2221P02	Incompatible
	A5500EI-CMW520-R2221P01	Incompatible
	A5500EI-CMW520-R2221	Incompatible
	A5500EI-CMW520-R2220P11	Incompatible

Current version	History version	ISSU compatibility
	A5500EI-CMW520-R2220P10	Incompatible
	A5500EI-CMW520-R2220P09	Incompatible
	A5500EI-CMW520-R2220P07	Incompatible
	A5500EI-CMW520-R2220L06	Incompatible
	A5500EI-CMW520-R2220P02	Incompatible
	A5500EI-CMW520-R2220	Incompatible
	A5500EI-CMW520-F2218L02	Incompatible
	A5500EI-CMW520-F2218P01	Incompatible
	A5500EI-CMW520-F2218	Incompatible
	A5500EI-CMW520-F2217	Incompatible
	A5500EI-CMW520-R2215	Incompatible
	A5500EI-CMW520-F2212	Incompatible
	A5500EI-CMW520-F2211	Incompatible
	A5500EI-CMW520-R2210	Incompatible
	A5500EI-CMW520-R2208	Incompatible

Upgrade restrictions and guidelines

Before performing a software upgrade, it is important to refer to the *Software Feature Changes* document for any feature changes in the new version. Also check the most recent version of the related documents (see "Related documents") available on the HPE website for more information about feature configuration and commands.

Release F2212 or later adopts a new password encryption algorithm. The password saved in the configuration file has been processed by the new algorithm. If you roll back the software from Release F2212 or later to a version before F2212, the password cannot be restored, and login will fail.

Hardware feature updates

Hardware feature updates in R2222P12

None

Hardware feature updates in R2222P09

None

Hardware feature updates in R2222P08

None

Hardware feature updates in R2222P07

None

Hardware feature updates in R2222P05

None

Hardware feature updates in R2222P02

None

Hardware feature updates in R2221P30

None

Hardware feature updates in R2221P25

None

Hardware feature updates in R2221P22

None

Hardware feature updates in R2221P20

None

Hardware feature updates in R2221P19

None

Hardware feature updates in R2221P18

None

Hardware feature updates in R2221P15

None

Hardware feature updates in R2221P12

None

Hardware feature updates in R2221P10

None

Hardware feature updates in R2221P08

None

Hardware feature updates in R2221P07

None

Hardware feature updates in R2221P06

None

Hardware feature updates in R2221P05

None

Hardware feature updates in R2221P04

None

Hardware feature updates in R2221P02

None

Hardware feature updates in R2221P01

None

Hardware feature updates in R2221

None

Hardware feature updates in R2220P11

None

Hardware feature updates in R2220P10

None

Hardware feature updates in R2220P09

None

Hardware feature updates in R2220P07

None

Hardware feature updates in R2220L06

None

Hardware feature updates in R2220P02

New Features:

1. Add 10G-BASE-T module

Hardware feature updates in R2220

None

Hardware feature updates in F2218L02

None

Hardware feature updates in F2218P01

None

Hardware feature updates in F2218

None

Hardware feature updates in F2217

None

Hardware feature updates in R2215

None

Hardware feature updates in F2212

None

Hardware feature updates in F2211

None

Hardware feature updates in R2210

None

Hardware feature updates in R2208

None

Software feature and command updates

For more information about the software feature and command update history, see *HPE A5500EI-CMW520-R2222P12 Release Notes (Software Feature Changes)*.

MIB updates

Table 5 MIB updates

Item	MIB file	Module	Description
A5500EI-CMW520-R2222P12			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-R2222P09			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-R2222P08			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-R2222P07			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-R2222P05			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-R2222P02			

Item	MIB file	Module	Description
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-R2221P30			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-R2221P25			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-R2221P22			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-R2221P20			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-R2221P19			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-R2221P18			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-R2221P15			
New	New	New	New
Modified	Modified	Modified	Modified
A5500EI-CMW520-R2221P12			
New	New	New	New
Modified	Modified	Modified	Modified
A5500EI-CMW520-R2221P10			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-R2221P08			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-R2221P07			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-R2221P06			
New	None	None	None

Item	MIB file	Module	Description
Modified	None	None	None
A5500EI-CMW520-R2221P05			
New	rfc2096-ip-forward.mib	IP-FORWARD-MIB	Added inetCidrRouteTable.
Modified	None	None	None
A5500EI-CMW520-R2221P04			
New	hh3c-ifqos2.mib	HH3C-IFQOS2-MIB	Added descriptions and support for the following MIBs: 1.hh3cIfQoSQSModeTable 2.hh3cIfQoSQSWeightTable 3.hh3cIfQoSPortPriorityTable 4.hh3cIfQoSPortPirorityTrustTable
Modified	rfc4292-ip-forward.mib	IP-FORWARD-MIB	Support full RFC 4292
A5500EI-CMW520-R2221P04			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-R2221P01			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-R2221			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-R2220P11			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-R2220P10			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-R2220P09			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-R2220P07			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-R2220L06			
New	None	None	None
Modified	rfc1213.mib rfc3418-snmpv2.mib	RFC1213-MIB	The maximum character string length allowed by the sysLocation and sysContact nodes was changed from 200 to 255.

Item	MIB file	Module	Description
A5500EI-CMW520-R2220P02			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-R2220			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-F2218L02			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-F2218P01			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-F2218			
New	None	None	None
Modified	hh3c-radius.mib	HH3C-RADIUS-MIB	Changed the value returned by the following MIBs from a plaintext or ciphertext password to empty or "******": (1)hh3cUserPassword (2)hh3cRdKey (3)hh3cRdSecKey (4)hh3cRdAccKey (5)hh3cRdSecAccKey (6)hh3cRadiusSchAuthPrimKey (7)hh3cRadiusSchAuthSecKey (8)hh3cRadiusSchAccPrimKey (9)hh3cRadiusSchAccSecKey (10)hh3cDot11SrvSecurityPskKeyString (11)hh3cSecureRalmAuthPassword (12)hh3cDot11SecurityPskKeyString
A5500EI-CMW520-F2217			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-R2215			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-F2212			
New	None	None	None
Modified	None	None	None
A5500EI-CMW520-F2211			
New		hh3cCfgLogTable	HH3C-CONFIG-MAN-MIB

Item	MIB file	Module	Description
		hh3cCfgOperateTable	HH3C-CONFIG-MAN-MIB
Modified		None	None
A5500EI-CMW520-R2210			
New		rfc1493-bridge.mib	BRIDGE-MIB
		rfc1493-bridge.mib	BRIDGE-MIB
		hh3c-acl.mib	ACL-MIB
		hh3c-transceiver-info.mib	TRANSCEIVER-MIB
		savi-mib.mib	SAVI-MID
Modified		rfc2011-ip-icmp.mib	IP-MIB
		rfc2465-ipv6.mib	IPV6-MIB
A5500EI-CMW520-R2208			
New	None	None	None
Modified	None	None	None
S5500EI-CMW520-R2208			
New	None	None	None
Modified	None	None	None

Operation changes

Operation changes in R2222P12

None

Operation changes in R2222P09

None

Operation changes in R2222P08

None

Operation changes in R2222P07

None

Operation changes in R2222P05

None

Operation changes in R2222P02

None

Operation changes in R2221P30

None

Operation changes in R2221P25

1. The maximum number of DHCP snooping entries was changed from 2 K to 6 K for each interface.

Operation changes in R2221P22

1. Modified the output destination of MemRatio log messages

Before modification, MemRatio log messages are not output to the log buffer when the switch fails to issue ACLs for lack of memory.

After modification, MemRatio log messages are output to the log buffer when the switch fails to issue ACLs for lack of memory.

Operation changes in R2221P20

None

Operation changes in R2221P19

None

Operation changes in R2221P18

1. Change to the count of IfInDiscards for an IRF physical interface

Before modification, the counted dropped packets include the packets that fail to find the egress port.

After modification, the counted dropped packets do not include the packets that fail to find the egress port.

2. Change to VLAN assignment for voice users and data users when the server is unreachable

Before modification: When the server is unreachable, both voice users and data users join the critical VLAN.

After modification: When the server is unreachable, voice users join the voice VLAN and data users join the critical VLAN.

Operation changes in R2221P15

1. Added traps for master PoE DIMM module failures:

Before modification, no traps are generated when a PoE switch fails to supply power over PoE because its master PoE DIMM module becomes faulty.

After modification, power failure traps are generated for the preceding situation.

Operation changes in R2221P12

1. Increased the number of supported syslog hosts from 4 to 20.

Operation changes in R2221P10

1. Change to the logout threshold for offline detect of MAC authentication

Before modification: The switch logs out a user if it has not received traffic from the user within two offline detect intervals.

After modification: The switch logs out a user if it has not received traffic from the user within one offline detect interval.

2. Change to route learning after the **ipv6 address dhcp-alloc** command is configured

Before modification, the switch can learn only IPv6 addresses with the prefix as 128 and cannot generate network routes after the **ipv6 address dhcp-alloc** command is configured on an interface.

After modification, the switch can actively send RS messages and RA learning is enabled after the **ipv6 address dhcp-alloc** command is configured on an interface. Then, the following events occur on the switch:

- The switch can request addresses from a DHCPv6 server and can learn IPv6 addresses with the prefix as 64.
- The switch can learn the default gateway based on RA messages and add the default gateway to routes.
- The switch can learn a prefix based on RA messages and add the prefix to routes.

Operation changes in R2221P08

1. Change to the LED for a loop detection-enabled port

Before modification, when a loop is detected on a loop detection-enabled port, the LED status for the port does not change.

After modification, when a loop is detected on a loop detection-enabled port, the LED for the port is flashing green.

Operation changes in R2221P07

None

Operation changes in R2221P06

None

Operation changes in R2221P05

1. Changed the OpenFlow packet-in rate limit from 200 PPS to 500 PPS.
2. Change to ACL limit for FP_RANGE_CHECK

Before modification, the FP_RANGE_CHECK register supports a maximum of 32 ACLs. The system prompts failure information when the maximum number is exceeded.

After modification, the FP_RANGE_CHECK register supports a maximum of more than 32 ACLs, which depends on the available ACL resources.

Operation changes in R2221P04

1. Added a controller+normal action for the OpenFlow flow table.
2. Added L2/L3 forwarding support for OpenFlow packet out normal.
3. Added a "to controller" action for OpenFlow packet out.

Operation changes in R2221P02

1. Changed the maximum number of gateways in a VLAN from 20 to 64 for auto-mode MFF.

Operation changes in R2221P01

None

Operation changes in R2221

1. Changed the maximum ARP rate on a port that is enabled with ARP detection from 50 pps to 400 pps.

Operation changes in R2220P11

None

Operation changes in R2220P10

None

Operation changes in R2220P09

1. Before modification, the CPE only supports using HTTP to upload/download files to/from the ACS.

After modification, if the CPE passes authentication on the ACS, the CPE can use either HTTP or HTTPS to upload/download files to/from the ACS.

Operation changes in R2220P07

1. Changed the flow control configuration policy:

Before modification, enabling or disabling flow control does not bring up or down the physical port.

After modification, enabling or disabling flow control brings down and up the physical port to apply the new configuration.

Operation changes in R2220L06

1. In this version and later versions, multicast MAC addresses starting with 01005e can be configured.

Operation changes in R2220P02

1. Operation changes to the port security mode UserloginWithOui when multicast trigger is disabled and unicast trigger is enabled:

Before modification, packets with an unknown source MAC address that does not contain a permitted OUI are discarded without triggering authentication.

After modification, packets with an unknown source MAC address that does not contain a permitted OUI can trigger authentication.

2. Operation changes to the port security mode UserloginWithOui when multicast trigger is enabled:

Before modification, the device continues multicasting authentication requests after a PC passes authentication, resulting in re-authentication of the PC.

After modification, the device stops multicasting authentication packets after a PC passes authentication.

3. This release permits IP camera packets that have a Power consumption TLV longer than 6 bytes to pass.

Operation changes in R2220

1. Added the following attributes for CDP packets sent by the device: Addresses, Capabilities, Software Version, Platform, Duplex, MTU and System Name.

2. The ARP rate limit is enabled by default with a value of 50 packets per second.

3. Before modification, the system does not provide log information for ARP attacks found by ARP detection.

After modification, the system provides log information for ARP attacks found by ARP detection.

Operation changes in F2218L02

The maximum number of VPN instances supported by the switch was changed from 63 to 1023, and the maximum number of VLAN interfaces supported by a VPN instance was changed from 128 to 1023.

Operation changes in F2218P01

Default configuration changes: disable all the TCP/UDP port by default (For example: TCP ports including 23/80,UDP ports including 1812/3318/3799).

Operation changes in F2218

1. The cluster management feature provides a simple method to manage multiple units using a single IP address, however it does use some protocols that are not considered totally secure. In this release, the cluster management protocols, including NDP, NTDP, and Cluster, are disabled by default to avoid any possible security risks.

If cluster management is required it is necessary to re-enable the required protocols with the following commands: ndp enable, ntdp enable, and cluster enable. In addition, HPE recommends that a separate management VLAN for the cluster should be established. Only the access ports that are used to link the cluster members should belong to this VLAN so the inter-switch protocol will not be accessible to insecure devices, including PCs and other network devices.

The Winet feature is removed in this release as it is not considered totally secure. The Winet functionality is available through other management methods.

2. Changed the maximum number of Free IP networks for 802.1X authentication from 4 to 16.

3. Suffix requirement change for execute batch files

(1)Before modification, execute batch files must have a suffix of ".bat".

(2)After modification, execute batch files can have any suffix.

4. Modified the value of node hh3cUserPassword in HH3C-USER-MIB due to security concerns. When read, hh3cUserPassword always returns a zero-length OCTET STRING.

Operation changes in F2217

1. Change the maximum online time from 65535 seconds to 2147483647 seconds for MAC authentication users in the RADIUS authentication approach.

2. Change the MAC authentication delay setting:

(1)Before: On a port where both 802.1X authentication and MAC authentication are enabled, MAC authentication starts after a delay of 30 seconds.

(2)After: By default, MAC authentication is not delayed. The following command is provided to enable MAC authentication delay and set the delay time.

mac-authentication timer auth-delay *time*

undo mac-authentication timer auth-delay

3. Change the maximum number of sub VLANs in an Isolate-user-VLAN from 64 to 192.

4. Patch operation change:

In earlier versions, when a patch is installed on a switch that has been installed with another patch, the switch replaces the existing patch with the new patch without any prompt. This creates risks. This version prompts a message "Another patch loaded, please uninstall it first."

5. Operation change for whether a port leaves the critical VLAN after the silent timer expires:

After a port is assigned to the critical VLAN, the RADIUS server state changes to "blocked", and the silent timer of the RADIUS server starts (this timer is configurable and defaults to 5 minutes).

In earlier versions:

(1) If the port uses 802.1X authentication, it leaves the critical VLAN when the silent timer expires. If the port is configured with the dot1x critical recovery-action command, its leaving triggers new 802.1X authentication.

(2)If the port uses MAC authentication, it leaves the critical VLAN when the silent timer expires.

In this version:

(1)If the port uses 802.1X authentication, it remains in the critical VLAN when the silent timer expires. If the port is configured with the dot1x critical recovery-action command, the silent timer expiration triggers new 802.1X authentication.

(2)If the port uses MAC authentication, it remains in the critical VLAN and triggers new MAC authentication when the silent timer expires.

6. If a save operation is performed on a switch where a software version of F2217 or later is running and the version number in the current startup configuration file is lower than F2212, the system first backs up the startup configuration file and then saves the current configuration. For example, suppose the startup configuration file is a.cfg. When a save operation is performed, the system first backs up a.cfg into _a_bak.cfg and then saves the current configuration into a.cfg.

Operation changes in R2215

Forwarded ARP packets are not rate limited.

Operation changes in F2212

None

Operation changes in F2211

None

Operation changes in R2210

1. Added the function of redistributing default routes into RIPng.

2. In earlier versions, if you specify both the output interface and next hop for an IPv6 static route, the specified next hop must be a link-local address. This version removes the limitation and allows you to specify a global unicast address as the next hop.

3. Added Root protection on the edge port.

4. Changed the maximum number of loopback interfaces to 1023.

5. Changed the maximum number of BGP peers from 40 to 64.

6. Changed the maximum number of VRRP groups to 255.

7. Changed the maximum number of OSPFv3 processes to 64.

8. Changed the maximum number of VTY users from 5 to 16.

9. Changed the maximum number of BFD sessions from 8 to 20.

9. Changed the maximum number of 10G aggregated ports from 4 to 8.

10. Changed the user-bind { ip-address X.X.X.X | mac-address H-H-H } [vlan INTEGER<1-4094>] command in port view to ip source binding { ip-address X.X.X.X | mac-address H-H-H } [vlan INTEGER<1-4094>].

11. Changed the ip check source { ip-address | mac-address } command in port view to ip verify source { ip-address | mac-address }.

12. Change the command of {ipsec-policy } to {enable ipsec-policy }.

Operation changes in R2208

None

Operation changes in R2208

First Release

Restrictions and cautions

1. Due to implementation limitation, VLAN ACLs do not take effect on QinQ-enabled ports.

2. Port isolation group configuration takes precedence over traffic redirect configuration. For example, add GE1/0/1 and GE1/0/2 to a port isolation group, and configure GE1/0/1 to redirect specific traffic to GE1/0/2. The redirect configuration does not take effect because the two ports have been isolated.

3. The display diagnostic-information command creates a very large amount of data. The output from this command is quite likely to exceed the flash storage limits of the device and fail. To avoid this possibility, please select the command option to display the output from the command and save the displayed results to an external file.

4. Multi-port loopback detection is available on a single device only.

5. Multicast ARP is supported only on A5500-24G EI / A5500-24G-PoE+ EI / A5500-24G-SFP EI, the output ports of a multicast ARP entry must reside on the same device.

6. Release F2212 or later adopts a new password encryption algorithm. The password saved in the configuration file has been processed by the new algorithm. If you roll back the software from Release F2212 or later to a version before F2212, the password cannot be restored, and login will fail.

7. The port type of OpenFlow can't support the link-aggregation.

8. OpenFlow can't support IRF.

9. Software auto-update function might fail to synchronize the software of subordinate devices from a version earlier than R2220P10 to R2220P10 or a later version. You must manually upgrade the software for the devices.

10. If the software is upgraded for a switch that runs a version earlier than release R2221P10 and has the portal roaming configuration modified, the switch will be rebooted to complete the upgrade and then be rebooted again to update the device configuration.

Open problems and workarounds

LSD074215

- Symptom: After two member devices in an IRF fabric reboot, all users fail to log in.
- Conditions: Two devices form an IRF fabric. Enable the password control function, configure users, and format the flash of the slave device. Then, copy a startup configuration file to the slave device and specify the startup configuration file, save the configuration, and perform a master/standby switchover.
- Workaround: After the flash is formatted, configure the passwords for all users again before performing a master/standby switchover.

LSD67923

- Symptom: In this version of code, the password encryption within configuration files has been enhanced and cannot be interpreted by earlier revisions of the agent code. This means that if a unit is downgraded to earlier code, it may no longer be possible to login and manage the device.
- Condition: This symptom might occur after the software is downgraded to a version before F2212.
- Workarounds:
  - Before upgrading to the new code, it is necessary to ensure password control is disabled. Execute the "*undo password-control enable*" and then save this configuration file as a backup in case you need to downgrade the software again. If it is later necessary to downgrade to earlier software, force the switch to use this backup configuration file by executing a "*startup saved-configuration (filename)" c*ommand before rebooting to the old code. Then, after the code has been downgraded, the device can be logged in from the console or by Telnet, but not SSH. The SSH authentication details will need to be reset.
  - If no backup configuration has been saved but it is still possible to access the device management via some method while running the old code (e.g. Console, Telnet or SSH), then you can redefine all the device management passwords as required.
  - If after a downgrade it is impossible to login to the device via any method, then there are two ways to recover the switch:
    - From the BOOT menu, set the new code to run again and reboot the device. Disable Telnet authentication:
    - User-interface vty 0 4
    - Authentication mode none
    - Then save the configuration and downgrade the code again, login via Telnet and reset all the passwords as required.
  - From the BOOT menu. On boot-up, use Ctrl+B to enter the Boot menu and then force the unit to use the factory default configuration (bypassing the user configuration). The unit will then need to be fully reconfigured.

201603300317

- Symptom: The files in the flash might be corrupted if the DHCP snooping entry file is frequently updated to flash and can cause the switch image loading to fail after a reboot.
- Condition: This symptom occurs if the DHCP snooping entry backup function is configured with a short DHCP snooping entry update interval, set by using the **dhcp-snooping binding database update interval** command.
- Workaround: It is recommended to write the DHCP snooping entry file to a remote file server by using the command: **dhcp snooping binding database filename { filename | url url [username username [password { cipher | simple } string]] }**.

List of resolved problems

Resolved problems in R2222P12

201712050157

- Symptom: An IRF fabric splits.
- Condition: This symptom occurs if the following operations are performed:
  - **a.** Assign interfaces numbered 1 on the IRF fabric to an aggregation group.
  - **b.** Configure the qinq transparent-vlan command on the aggregate interface corresponding to the aggregation group to enable transparent transmission for a list of VLANs.

201808090430

- Symptom: When the device is connected to a peer through an SFP-XG-LX220-MM1310 transceiver module, the switch generates the LLDP_DUPLEX_INCONSISTENT log frequently.
- Condition: This symptom might occur if the device is connected to a peer through an SFP-XG-LX220-MM1310 transceiver module.

201811050058

- Symptom: On an IRF fabric, the **undo snmp-agent trap enable system** setting is lost after the IRF master reboots.
- Condition: This symptom might occur if the **undo snmp-agent trap enable system** command is executed and the IRF master is rebooted.

201812250053

- Symptom: The switch reboots unexpectedly after receiving an 802.1X Response/Identity packet from an iNode client.
- Condition: This symptom might occur if the IP address in the extended information of the 802.1X Response/Identity packet triggers a refresh of static IPv4SG bindings from version R2222P02 to R2222P10.

201805300583

- Symptom: The device reboots unexpectedly.
- Condition: This symptom occurs if a VPN private network interface on the device receives an abnormal packet carrying option 131 (Loose Source Route) without an address (the length in the option is 3 bytes).

201804280589

- Symptom: BFD sessions flap when the local device receives BFD packets from the peer device.
- Condition: This symptom occurs if the value of the remote discriminator in the received BFD packets exceeds the maximum value supported by the local device.

201712050157

- Symptom: An IRF fabric splits.
- Condition: This symptom occurs if the following operations are performed:
    - Assign interfaces numbered 1 on the IRF fabric to an aggregation group.
    - Configure the **qinq transparent-vlan** command on the aggregate interface corresponding to the aggregation group to enable transparent transmission for a list of VLANs.

201804190493

- Symptom: The CLI of a subordinate IRF member device does not respond during its reboot.
- Condition: This symptom occurs if an ISSU reboot is performed for an IRF fabric.

Resolved problems in R2222P09

201712190289

- Symptom: CVE-2017-12190
- Condition: Local attacker can exploit these issues to obtain sensitive information that may lead to further attacks.

201801030312

- Symptom: The role of a device in a VRRP group might frequently switch between Master and Backup.

- Condition: This symptom occurs if the device has been continuously running for 355 weeks.

Resolved problems in R2222P08

201706200187

- Symptom: CVE-2010-3864
- Condition: Successfully exploiting this issue may allow attackers to execute arbitrary code in the context of applications that use the affected library, but this has not been confirmed. Failed exploit attempts may crash applications, denying service to legitimate users.

201706200187

- Symptom: CVE-2010-4252
- Condition: A successful exploit may allow attackers to authenticate without the shared secret, aiding in further attacks.

201706200187

- Symptom: CVE-2011-4109
- Condition: An attacker may leverage these issues to obtain sensitive information, cause a denial-of-service condition and perform unauthorized actions.

201706200187

- Symptom: CVE-2012-2110
- Condition: Successfully exploiting this issue may allow an attacker to execute arbitrary code in the context of the application using the vulnerable library. Failed exploit attempts will result in a denial-of-service condition.

201708140543

- Symptom: In the output from the **display saved-configuration** command, the PVST path cost setting for the only VLAN in the last line cannot be displayed.
- Condition: This symptom might occur if the following operations are performed:
  - **a.** Configure the path cost for a PVST-enabled port in N×10+1 (n≥1) inconsecutive VLANs.
  - **b.** Save the configuration.
  - **c.** Execute the display saved-configuration command to view the path cost settings.

Resolved problems in R2222P07

201705040092

- Symptom: CVE-2014-9298
- Condition: An attacker could bypass source IP restrictions and send malicious control and configuration packets.

201705040049

- Symptom: CVE-2017-6458
- Condition: NTP are prone to a buffer-overflow vulnerability because it fails to properly bounds-check user-supplied data before copying it into an insufficiently sized buffer.

201706270522

- Symptom: After a port on the master node in an RRPP ring is set to the secondary port, the RRPP ring transits to Disconnect state and the status of the secondary port changes from down to up.

- Condition: This symptom might occur if the master node is an IRF subordinate device with member ID 1 and the port set to the secondary port is GigabitEthernet 1/0/1.

201707040634

- Symptom: Execution of the **qinq transparent-vlan** command fails if the switch runs software version R2221P20, R2221P22, R2221P25, R2221P30, R2222P02, or R2222P05.
- Condition: This symptom might occur in one of the following conditions:
  - The switch runs software version R2221P20 or R2221P22, and the **qinq transparent-vlan** command is executed in interface view.
  - The switch runs software version R2221P20, R2221P22, R2221P25, R2221P30, R2222P02, or R2222P05, and the **qinq transparent-vlan** command is executed in Layer 2 aggregate interface view.

Resolved problems in R2222P05

201612050252

- Symptom: CVE-2016-7427
- Condition: An attacker with access to the NTP broadcast domain can periodically inject specially crafted broadcast mode NTP packets into the broadcast domain which, while being logged by ntpd, can cause ntpd to reject broadcast mode packets from legitimate NTP broadcast servers.

201612050252

- Symptom: CVE-2016-7428
- Condition: An attacker with access to the NTP broadcast domain can send specially crafted broadcast mode NTP packets to the broadcast domain which, while being logged by ntpd, will cause ntpd to reject broadcast mode packets from legitimate NTP broadcast servers.

201612220015

- Symptom:CVE-2016-8610
- Condition: OpenSSL is prone to denial-of-service vulnerability.Successful exploitation of the issue will cause excessive memory or CPU resource consumption, resulting in a denial-of-service condition.

201611220384

- Symptom: A user logs in to a Comware 7 device or a third-party device from a Comware 5 switch. When the user presses Enter once, two new lines are created.
- Condition: This symptom might occur if a user Telnets to a Comware 5 switch and then logs in to a Comware 7 device or a third-party device through SSH from the switch.

201612080502

- Symptom: An interface does not learn MAC addresses.
- Condition: This symptom occurs if the following operations are performed:
  a. Set the maximum number of MAC addresses that can be learned and configure 802.1X authentication on the interface.
  b. Execute the default command on the interface after the maximum number of MAC addresses is reached.

201701060096

- Symptom: An interface cannot learn the MAC address of a PC connected to an IP phone on an interface when the IP phone and the PC cannot reach the authentication server.

- Condition: This symptom occurs if the following operations are performed:
  a. Enable port security, and set the port security mode to userLoginSecure or userLoginSecureExt for the interface.
  b. Configure a MAC authentication voice VLAN on the interface.
  The MAC address of the IP phone is learned in the voice VLAN after the IP phone passes authentication.
  c. Modify the MAC authentication voice VLAN ID, and configure the MAC authentication critical VLAN or 802.1X critical VLAN as the original MAC authentication voice VLAN ID.

Resolved problems in R2222P02

201609010374

- Symptom: CVE-2013-0169
- Condition: The TLS protocol and the DTLS protocol do not properly consider timing side-channel attacks on a MAC check requirement during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, aka the "Lucky Thirteen" issue.

201610260369

- Symptom: Extra characters are displayed in the **display saved-configuration** command output.
- Condition: This symptom occurs if the multiline text of a banner is pasted when the banner is configured, which results in line feeds but not carriage returns.

201609210333

- Symptom: CVE-2015-5219
- Condition: NTP is prone to a denial-of-service vulnerability. A remote attacker may exploit this issue to cause an infinite loop, resulting in a denial-of-service condition.

201609010392

- Symptom: CVE-2009-3238
- Condition: The get_random_int function in the Linux kernel before 2.6.30 produces insufficiently random numbers, which allows attackers to predict the return value, and possibly defeat protection mechanisms.

201609010432

- Symptom: CVE-2014-9751
- Condition: The read_network_packet function in ntp_io.c in ntpd in NTP 4.x before 4.2.8p1 on Linux and OS X does not properly determine whether a source IP address is an IPv6 loopback address, which makes it easier for remote attackers to spoof restricted packets, and read or write to the runtime state, by leveraging the ability to reach the ntpd machine's network interface with a packet from the ::1 address.

201609190248

- Symptom: The MAD IP addresses of members in an IRF fabric cannot be pinged, and ARP conflicts occur.
- Condition: This symptom might occur if BFD MAD is configured on an IRF fabric, and the MAD IP addresses of multiple IRF members are pinged.

201609070163

- Symptom: When certain conditions exist, the value of the **EAP Request/Challenge Packets** field is 0 in the output from the **display dot1x** command.
- Condition: This symptom might occur if the **dot1x authentication-method eap** command is executed, and 802.1X authentication is successful.

Resolved problems in R2221P30

201608180290

- Symptom: CVE-2015-7974
- Condition: Fixed vulnerability in NTP 4.x before 4.2.8p6 and 4.3.x before 4.3.90 which might allow remote attackers to conduct impersonation attacks via an arbitrary trusted key.

201608180290

- Symptom: CVE-2015-7973
- Condition: Fixed vulnerability when NTP is configured in broadcast mode, a man-in-the-middle attacker or a malicious client could replay packets received from the broadcast server to all (other) clients, which cause the time on affected clients to become out of sync over a longer period of time.

201605170555

- Symptom: CVE-2016-1550
- Condition: Fixed vulnerability in ntpd function allow an attacker to conduct a timing attack to compute the value of the valid authentication digest causing forged packets to be accepted by ntpd.

201605170555

- Symptom: CVE-2016-1551
- Condition: Fixed vulnerability in ntpd allows unauthenticated network attackers to spoof refclock packets to ntpd processes on systems that do not implement bogon filtering.

201607050187

- Symptom: CVE-2016-4954
- Condition: Fixed vulnerability in ntpd in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service by sending spoofed packets from source IP addresses in a certain scenario.

201606270469

- Symptom: After an IRF master device is rebooted or powered off, BGP neighborship cannot be established.
- Condition: This symptom occurs if the following operations are performed:
  - Configure BGP. BGP can establish neighborship properly.
  - Reboot or power off the IRF master device.

201606280333

- Symptom: In the display transceiver interface command output for a transceiver module SFP-GE-LH70-SM1550, the Transfer Distance(km) and Ordering Name field are incorrectly displayed. The correct information is as follows:

  ```
  Transfer Distance(km): 80(9um)
  Ordering Name: SFP-GE-LH80-SM1550
  ```

- Condition: This symptom occurs if the **display transceiver interface** command is used to display information about a transceiver module SFP-GE-LH70-SM1550.

201606130061

- Symptom: After the master of a four-member IRF fabric is rebooted, traffic forwarding between downstream devices is interrupted for about one minute.
- Condition: This symptom might occur if the master of a four-member IRF fabric is rebooted.

201604260165

- Symptom: When an aggregate interface is disconnected, traffic is interrupted for 9 seconds rather than 6 seconds.
- Condition: This symptom occurs if the LACP timeout interval is set to the short timeout interval on an interface and the aggregate link is disconnected.

201604140359

- Symptom: The IP source guard binding entries with IP address 255.255.255.255 cannot be deleted in the Web interface.
- Condition: This symptom occurs if you continue to configure static IPv4 binding entries with only MAC addresses specified when the number of static IPv4 binding entries created on the switch has reached 200. These entries are displayed as static IPv4 binding entries with IP address 255.255.255.255 in the Web interface.

201603100046

- Symptom: A walk on ifOutDiscards MIB returns a value of 0.
- Condition: This symptom can be seen during a walk on ifOutDiscards MIB.

201603290559

- Symptom: The switch reboots unexpectedly when private MIB nodes hh3cLswSlotPktBufFree and hh3cLswSlotPktBufInit are accessed.
- Condition: This symptom might occur if private MIB nodes hh3cLswSlotPktBufFree and hh3cLswSlotPktBufInit are accessed.

201109130022

- Symptom: The MIB does not have information of the dot3adAggPortSelectedAggID and dot3adAggPortAttachedAggID nodes.
- Condition: This symptom might occur if link aggregation is configured on the switch.

201512250171

- Symptom: The CLI for a Comware 7-based device is stuck.
- Condition: This symptom occurs if you log in to a Comware 5-based device through a console port and then the device telnets to a Comware 7-based device.

201401190006

- Symptom: The DHCP relay agent fails to assign an IP address to a client.
- Condition: This symptom occurs if the DHCP relay agent receives an offer packet where the yiaddr is 0.0.0.0, and the Bflag is 0.

Resolved problems in R2221P25

201601080614

- Symptom: BGP routes cannot be summarized when the labels of the routes change.

- Condition: This symptom might occur if BGP route summarization is enabled and the labels of BGP routes change.

201602180247

- Symptom: Execution of the qinq transparent-vlan command fails if the switch uses R2221P20 or R2221P22.
- Condition: This symptom might occur if the switch uses R2221P20 or R2221P22, and the qinq transparent-vlan command is executed in interface view.

201602010047

- Symptom: An IRF fabric cannot generate DHCP snooping entries for some interfaces.
- Condition: This symptom might occur if the following conditions exist:
  - The IRF fabric contains three or more member switches, and DHCP snooping is enabled on the IRF fabric.
  - Two master/subordinate switchovers occur, and some interfaces of the subordinate switches are down before the second switchover.

201512010460

- Symptom: An SSH client logs in to the switch that acts as an SSH server. When the SSH client tries to log out, the switch does not respond to the logout request. The SSH client must wait for the connection to time out.
- Condition: This symptom might occur if the switch acts an SSH server.

201511190090

- Symptom: On an IRF fabric, the static multicast MAC address entries on aggregate interfaces are lost after a master/subordinate switchover.
- Condition: This symptom might occur if static multicast MAC address entries are configured on aggregate interfaces and a master/subordinate switchover occurs.

201601040443

- Symptom: A PC connected to a Layer 3 interface cannot obtain an IPv6 address through stateless address autoconfiguration if the interface uses a static IPv6 address and constantly flaps.
- Condition: This symptom might occur if the following conditions exist:
  - Stateless address autoconfiguration is enabled on a Layer 3 interface that is connected to a PC.
  - The Layer 3 interface uses a static IPv6 address and constantly flaps.

201603140431

- Symptom: The switch keeps outputing the "`System is busy with warm backup, please wait......`" message.
- Condition: This symptom might occur if routing loops occur.

201603140376

- Symptom: MFF accesses invalid memory and the switch reboots unexpectedly if certain conditions exist.
- Condition: This symptom might occur if the following conditions exist:
  - DHCP snooping and MFF are used together.
  - IP source guard generates IPSG bindings with invalid VLAN information based on DHCP snooping entries, and MFF uses these bindings.

LSD64848

- Symptom: DHCP clients can obtain IP addresses only once because DHCP snooping entries are incorrect.
- Condition: This symptom might occur if basic QinQ and DHCP snooping are used together.

201507090353

- Symptom: When the **display interface** command is repeatedly executed, the CPU usage stays at 100% and the PVST topology changes after a period of time.
- Condition: This symptom might occur if the **display interface** command is repeatedly executed.

201603150457

- Symptom: The transfer distance and ordering name of an HP X125 1G SFP LC LH70 Transceiver module (JD063B) are incorrect in the output from the **display transceiver interface** command.
- Condition: This symptom might occur if the **display transceiver interface** command is used to display information for an HP X125 1G SFP LC LH70 Transceiver module (JD063B).

201601190549

- Symptom: The switch cannot establish an IPv6 BGP peer relationship with a neighbor if the primary IPv6 address of the output interface is a network address.
- Condition: This symptom might occur if the primary IPv6 address of the output interface is a network address.

201511110159

- Symptom: After the **snmp-agent trap enable stp tc** command is configured, the switch sometimes displays incorrect information for the configuration.
- Condition: This symptom might occur if the **snmp-agent trap enable stp tc** command is executed and the configuration is saved.

Resolved problems in R2221P22

201512290216

- Symptom: CVE-2015-3195
- Condition: When presented with a malformed X509_ATTRIBUTE structure OpenSSL will leak memory. This structure is used by the PKCS#7 and CMS routines so any application which reads PKCS#7 or CMS data from untrusted sources is affected.

201501060439

- Symptom: ICMP error packets fail to be sent.
- Condition: This symptom might be seen if an interface configured with NAT needs to forward packets that exceed the MTU of the interface and cannot be fragmented.

201601180342

- Symptom: MAC address entries for online MAC authentication users age out before the offline detect timer (set by using mac-authentication timer offline-detect) expires.
- Condition: This symptom might be seen if MAC authentication is enabled.

201512080086

- Symptom: Dynamic MAC address entries do not age out when a large number of 802.1X or MAC authentication users come online and go offline repeatedly.

- Condition: This symptom might be seen if a large number of 802.1X or MAC authentication users come online and go offline repeatedly.

201511100130

- Symptom: An error occurs when the switch reboots to join an IRF fabric as a subordinate member.
- Condition: This symptom might be seen if the switch reboots to join an IRF fabric as a subordinate member.

Resolved problems in R2221P20

201507280105

- Symptom: All member switches in an IRF fabric reboot when the **issu run switchover** command is executed on a subordinate switch after the subordinate switch is upgraded successfully.
- Condition: This symptom occurs if the following conditions exist:
    - The IRF fabric uses ISSU for upgrade.
    - The priority of the master switch is higher than that of the subordinate switch.

201510210123

- Symptom: The switch fails to transparently transmit OSPF multicast protocol packets.
- Condition: This symptom occurs if the OSPF multicast protocol packets are sent on an interface with QinQ enabled.

201510200101

- Symptom: The switch prints a message indicating an IP address conflict when a newly online wireless client obtains the IP address of a wireless client that just went offline.
- Condition: This symptom occurs if the following conditions exist:
    - Wireless clients obtain IP addresses through DHCP.
    - A wireless client comes online after another wireless client goes offline.

201509300381

- Symptom: An OpenFlow entry with a Group action fails to be added on the subordinate switch in an IRF fabric.
- Condition: This symptom occurs if the controller deploys an output interface for a group on the master switch when the subordinate switch has synchronized the OpenFlow data but not the interface data from the master switch.

201510150262

- Symptom: The controller fails to deploy a flow entry to the switch.
- Condition: This symptom occurs if the flow entry has an empty action list and has the last OXM as metadata.

201510220542

- Symptom: An IP phone cannot obtain an IP address after the IP phone passes 802.1X authentication.
- Condition: This symptom occurs if the switch cannot advertise the voice VLAN ID specified by using the **dot1x voice vlan** command to the IP phone through LLDP or CDP.

Resolved problems in R2221P19

201507170252

- Symptom: The switch reboots unexpectedly when the FreeRADIUS server issues a command to force an 802.1X user offline.
- Condition: Condition: This symptom might occur if the switch uses a FreeRADIUS server for 802.1X authentication.

201507160220

- Symptom: CVE-2015-1788
- Condition: When processing an ECParameters structure OpenSSL enters an infinite loop. This can be used to perform denial of service against any system which processes public keys, certificate requests or certificates.

201507160220

- Symptom: CVE-2015-1789
- Condition: X509_cmp_time does not properly check the length of the ASN1_TIME string and/or accepts an arbitrary number of fractional seconds in the time string. An attacker can use this to craft malformed certificates and CRLs of various sizes and potentially cause a segmentation fault, resulting in a DoS on applications that verify certificates or CRLs.

201507160220

- Symptom: CVE-2015-1790
- Condition: The PKCS#7 parsing code does not handle missing inner EncryptedContent correctly. An attacker can craft malformed PKCS#7 blobs with missing content and trigger a NULL pointer dereference on parsing.

201508180092

- Symptom: Symptom: The switch cannot negotiate the power with a powered device through LLDP.
- Condition: This symptom occurs if the powered device must negotiate the power twice with the switch.

Resolved problems in R2221P18

201506150192

- Symptom: The DHCP server on the switch does not preferentially use the static address pool when processing DHCP-INFORM packets.
- Condition: This symptom might occur if the following conditions exist:
  - The DHCP-INFORM packets are sent by a DHCP client bound to an IP address in the static address pool.
  - The address range of a dynamic address pool covers the static address pool.

201506250206

- Symptom: The switch does not forward traffic based on PBR policies that have been configured.
- Condition: This symptom might occur if PBR policies are configured on multiple VLAN interfaces, and a large number of PBR policies exist on the switch.

201505120391

- Symptom: The server cannot assign the voice VLAN attribute to an IP phone.
- Condition: This symptom might occur if the 802.1X authentication in EAP relay mode is used.

201506180403

- Symptom: The switch fails to cooperate with a specific authentication server.
- Condition: This symptom might occur if the following conditions exist:
  - The switch is connected to a specific authentication server.
  - The NAS_PORT_ID field in the sent RADIUS packets contains the VLAN field, which cannot be processed by the authentication server.

201507100159

- Symptom: An IP phone connected to a subordinate switch in an IRF fabric is removed from the voice VLAN after the subordinate switch reboots.
- Condition: This symptom might occur if the following conditions exist:
  - The IP phone receives power through PoE.
  - The subordinate switch experienced a cold reboot.

201306280329

- Symptom: The BIMS server fails to enable periodical notification for a switch that accesses the server for the first time. The BIMS server cannot manage the switch because the switch cannot actively access the BIMS server periodically.
- Condition: This symptom might occur if the following conditions exist:
  - The switch starts up without a configuration file.
  - The switch accesses the BIMS server for the first time after the switch obtains CWMP settings through DHCP.

201505120286

- Symptom: The switch cannot obtain the serial number of a transceiver module that is not certified.
- Condition: This symptom occurs if a MIB browser is used to obtain the serial number.

Resolved problems in R2221P15

201505140479

- Symptom: The CPU usage of an IRF fabric is excessively high.
- Condition: This symptom occurs if the following conditions exist:
  - A large number of GRE tunnels are configured on aggregate interfaces on the IRF fabric.
  - No member switch is specified by using the service slot *slot-number* command to forward traffic for the tunnel interfaces.

201505260034

- Symptom: Each member switch in a split IRF fabric set to the Recovery state takes a long time to shut down its interfaces.
- Condition: This symptom occurs if LACP MAD is used.

201506080236

- Symptom: An IP phone connected to a subordinate switch in an IRF fabric is removed from the voice VLAN after the subordinate switch reboots.

- Condition: This symptom might occur if the following conditions exist:
    - The IP phone receives power through PoE.
    - The subordinate switch is rebooted by using the reboot command.

201506270158

- Symptom: The switch reboots unexpectedly when a match criterion for QoS is added, deleted, or modified.
- Condition: This symptom occurs if a match criterion for QoS is added, deleted, or modified.

201506190301

- Symptom: The TTL value in ICMP messages does not decease by hop.
- Condition: This symptom occurs if the following conditions exist:
    - The switch is in a network that has routing loops.
    - The ICMP messages are triggered by using the ping –r command.

201505120295

- Symptom: The switch cannot obtain the serial number of a transceiver module that is not certified by H3C.
- Condition: This symptom occurs if a MIB browser is used to obtain the serial number.

201505180128

- Symptom: A 24-port PoE+ switch cannot supply power over PoE after a sharp decrease in input voltage.
- Condition: This symptom occurs if a sharp decrease in input voltage happens to the switch.

201504240056

- Symptom: New users can access Internet resources without passing portal authentication after a user passes portal authentication.
- Condition: This symptom occurs if portal roaming is enabled before any user passes portal authentication.

Resolved problems in R2221P12

201504170082

- Symptom: After being logged out, an authenticated user can access Internet resources without passing portal authentication in triple authentication.
- Condition: This symptom occurs if the cable is removed from and then installed into the interface connected to the user after the user passes the previous portal authentication.

201504170082

- Symptom: MAC authentication succeeds after a delay of 20 to 30 seconds.
- Condition: This symptom occurs if both portal authentication and MAC authentication are configured for triple authentication.

201504070107

- Symptom: CVE-2015-0209
- Condition: A malformed EC private key file consumed via the d2i_ECPrivateKey function could cause a use after free condition. This could lead to a DoS attack or memory corruption for applications that receive EC private keys from untrusted sources.

201504070107

- Symptom: CVE-2015-0287
- Condition: Reusing a structure in ASN.1 parsing may allow an attacker to cause memory corruption via an invalid write. Applications that parse structures containing CHOICE or ANY DEFINED BY components may be affected.

201504070107

- Symptom: CVE-2015-0288
- Condition: The function X509_to_X509_REQ will crash with a NULL pointer dereference if the certificate key is invalid.

201504070107

- Symptom: CVE-2015-0289
- Condition: The PKCS#7 parsing code does not handle missing outer ContentInfo correctly. An attacker can craft malformed ASN.1-encoded PKCS#7 blobs with missing content and trigger a NULL pointer dereference on parsing.

201504070107

- Symptom: CVE-2015-0292
- Condition: Vulnerability existed in previous versions of OpenSSL related to the processing of base64 encoded data.

201505110036

- Symptom: The irf link-delay command configuration does not take effect.
- Condition: This symptom occurs after the IRF fabric splits when the irf link-delay command is configured on an IRF fabric.

201504240250

- Symptom: The switch fails to cooperate with a specific authentication server.
- Condition: This symptom occurs when the following conditions exist:
  - The switch is connected to a specific authentication server.
  - The NAS_PORT_ID field in the sent RADIUS packets contains the VLAN field, which cannot be processed by the server.

201505180146

- Symptom: A PoE+ switch is identified as a PoE switch.
- Condition: This symptom occurs after the PoE+ switch is power cycled.

201504140243

- Symptom: The values of the sysUptime and ifLastChange nodes are different.
- Condition: This symptom occurs if the values are obtained by using a MIB tool.

201504210151

- Symptom: The portal roaming enable command configuration is no longer in effect after the switch is upgraded to Release 2221P10 from a version earlier than Release 2221P10.
- Condition: This symptom occurs if patches run on the switch before the upgrade.

Resolved problems in R2221P10

201501200392

- Symptom: CVE-2015-0205
- Condition: An OpenSSL server will accept a DH certificate for client authentication without the certificate verify message. This effectively allows a client to authenticate without the use of a private key. This only affects servers which trust a client certificate authority which issues certificates containing DH keys.

201501200392

- Symptom: CVE-2014-3570
- Condition: Bignum squaring (BN_sqr) may produce incorrect results on some platforms, including x86_64. This bug occurs at random with a very low probability, and is not known to be exploitable in any way.

201501200392

- Symptom: CVE-2015-0204
- Condition: An OpenSSL client will accept the use of an RSA temporary key in a non-export RSA key exchange ciphersuite. A server could present a weak temporary key and downgrade the security of the session.

201501200392

- Symptom: CVE-2014-3572
- Condition: An OpenSSL client will accept a handshake using an ephemeral ECDH ciphersuite using an ECDSA certificate if the server key exchange message is omitted. This effectively removes forward secrecy from the ciphersuite.

201501200392

- Symptom: CVE-2014-8275
- Condition: By modifying the contents of the signature algorithm or the encoding of the signature, it is possible to change the certificate's fingerprint. Only custom applications that rely on the uniqueness of the fingerprint may be affected.

201501200392

- Symptom: CVE-2014-3569
- Condition: The ssl23_get_client_hello function in s23_srvr.c in OpenSSL 0.9.8zc, 1.0.0o, and 1.0.1j does not properly handle attempts to use unsupported protocols, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an unexpected handshake, as demonstrated by an SSLv3 handshake to a no-ssl3 application with certain error handling.

201503230385

- Symptom: A route does not take effect if its lower eight bits are 01111111 (127 in decimal format).
- Condition: This symptom occurs if the lower eight bits of the route are 01111111 (127 in decimal format).

201502110105

- Symptom: When a host moves between the local switch and a peer, the MAC address entry for the host does not update on the local switch.

- Condition: This symptom might occur if the local switch is connected to its peer by an aggregate link, and the host moves between the lowest-numbered port of the local switch and a port of the peer.

201502270218

- Symptom: iMC is disconnected from a managed switch and generates an ICMP no response alarm for the switch.
- Condition: This symptom occurs if the switch suffers from attacks against the ipForwarding and ipDefaultTTL nodes.

201502160179

- Symptom: After a switch obtains an IPv6 address from a DHCPv6 server, the switch cannot successfully ping the DHCPv6 server.
- Condition: This symptom occurs when the following conditions exist:
  - A subordinate IRF member switch is connected to the DHCPv6 server through a VLAN interface.
  - The VLAN interface is configured to actively send RS messages and receive RA messages by using the ipv6 address dhcp-alloc command.

201502280198

- Symptom: When a user that has logged in through a port logs in again through another port in the same VLAN as the preceding port, the system always redirects the user to the page that the user has logged in to.
- Condition: This symptom occurs after portal roaming is enabled and the user successfully passes authentication on a port.

201501290196

- Symptom: The switch reboots unexpectedly.
- Condition: This symptom occurs after the following procedure is performed:
  - Configure a QoS policy. The QoS policy contains a traffic class and a traffic behavior with the same name as the QoS policy.
  - Apply the QoS policy to a control plane.
  - Remove the QoS policy from the control plane.

Resolved problems in R2221P08

201412310368

- Symptom: CVE-2014-9295
- Condition: Stack-based buffer overflows in ntpd in NTP before 4.2.8 allows remote attackers to execute arbitrary code via a crafted packet.

201410230229

- Symptom: SSL 3.0 Fallback protection
- Condition: OpenSSL has added support for TLS_FALLBACK_SCSV to allow applications to block the ability for a MITM attacker to force a protocol downgrade. Some client applications (such as browsers) will reconnect using a downgraded protocol to work around interoperability bugs in older servers. This could be exploited by an active man-in-the-middle to downgrade connections to SSL 3.0 even if both sides of the connection support higher protocols. SSL 3.0 contains a number of weaknesses including POODLE (CVE-2014-3566).

201501120301

- Symptom: A routing policy contains a high-priority deny node and a low-priority permit node with the action of redirecting traffic to a next hop. Traffic matching both nodes is not forwarded based on the high-priority deny node. Instead, the traffic is forwarded based on the low-priority permit node and redirected to the next hop.
- Condition: This symptom can be seen when a flow matches the following nodes of a routing policy at the same time:
  - A high-priority deny node.
  - A low-priority permit node with the action of redirecting traffic to a next hop.

201412190129

- Symptom: The switch reboots unexpectedly.
- Condition: This symptom can be seen when the switch receives NTP control packets with the Mode field being 6.

201412090423

- Symptom: The DR on the multicast source side reboots unexpectedly.
- Condition: This symptom can be seen when the following conditions exist:
  - The interface directly connected to the multicast source is designated as an RP.
  - The DR on the multicast source side is a different device from the RP.
  - The DR on the multicast source side uses the same unicast route to register with the RP and select an RPF interface to the multicast source. The route is used by PIM entries for two times.

201412220343

- Symptom: After a master/subordinate switchover in an IRF fabric, the **dhcp-snooping check mac-port** command configuration is lost.
- Condition: This symptom can be seen after the following procedure is performed in the IRF fabric:
  - Execute the **dhcp-snooping check mac-port** command.
  - Save the configuration.
  - Perform a master/subordinate switchover.

201409240424

- Symptom: The **dhcp-snooping check mac-port** command configuration does not take effect. After a client that has been assigned an IP address on port 1 is moved to port 2, the client can still be assigned an IP address.
- Condition: This symptom can be seen after the following procedure is performed:
  - Execute the **dhcp-snooping check mac-port** command.
  - Move a client that has been assigned an IP address on port 1 to port 2.

201501160266

- Symptom: The switch reboots unexpectedly.
- Condition: This symptom can be seen when the following conditions exist in a tunneling network:
  - The switch receives an IP packet with a specific option. The option is not IPOPT_EOL (0) or IPOPT_NOP (1). The second byte of the option is 0.
  - The IP packet is too long and needs to be fragmented.

201412230355

- Symptom: The entries in the obtained VRRP-MIB table are arranged by VLAN ID, rather than by index.
- Condition: This symptom can be seen when the following conditions exist:
    - VRRP groups are configured on multiple VLAN interfaces without a specific order.
    - A MIB tool is used to obtain the vrrpOperEntry entries.

Resolved problems in R2221P07

201411190163

- Symptom: The IS-IS routes might be lost.
- Condition: This symptom occurs when the IS-IS routes are flapping.

201410110181

- Symptom: IP broadcast packets cannot be relayed and forwarded.
- Condition: This symptom occurs when the udp-helper server command is executed on a Layer 3 virtual interface to configure the IP address of the destination server for UDP helper as a subnet broadcast address.

201410110326

- Symptom: The system displays an ARP conflict prompt for the MAD IP addresses.
- Condition: This symptom occurs when the following procedure is performed:
    - Configure BFD MAD in the IRF fabric.
    - Configure the **arp ip-conflict prompt** command.
    - The switch receives TCN BPDUs.

201411190489

- Symptom: The switch drops the packets sent by a user that comes online after passing MAC authentication.
- Condition: This symptom occurs when the MAC address entries for the user that comes online after passing MAC authentication is deleted after the switch receives TCN BPDUs.

201411030489

- Symptom: Subordinate IRF member switches reboot.
- Condition: This symptom occurs when the following procedure is performed:
    - Configure the IRF fabric as the DHCP Server to allocate IP addresses in the extended address pool.
    - A master/subordinate switchover occurs in the IRF fabric.
    - A client releases its IP address. The IP address will exist in both the free IP list and the conflicting IP list.
    - The IP address is obtained by a client again.

201411180434

- Symptom: The RADIUS protocol packets that the switch receives on the interface connected to the authentication server are dropped. As a result, a user fails to pass authentication.
- Condition: This symptom occurs when the following conditions exist:
    - The switch is configured with RADIUS to authenticate and authorize users.
    - The interface connected to the user receives a large number of packets with unknown source MAC addresses.

Resolved problems in R2221P06

201408280078

- Symptom: CVE-2008-5161
- Description: Error handling in the SSH protocol in several SSH servers/clients, including OpenSSH 4.7p1 and possibly other versions, when using Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data.

201408140565

- Symptom: CVE-2014-3508
- Condition: A flaw in OBJ_obj2txt may cause pretty printing functions such as X509_name_oneline, X509_name_print_ex et al. to leak some information from the stack. Applications may be affected if they echo pretty printing output to the attacker.

201410090414

- Symptom: A power interface (PI) does not supply power.
- Condition: This symptom occurs when lightning strikes cause crosstalk on the power supply of the switch.

201409040331

- Symptom: The summary routes in a VPN do not contain the RT attribute of the VPN.
- Condition: This symptom occurs when the extended community attributes of the withdrawn routes contain the RT attribute of the local VPN and the other routes do not contain the RT attribute.

201409150368

- Symptom: The switch keeps generating log messages showing that the MAC learning limit has been reached on a port.
- Condition: This symptom occurs if the **mac-address max-mac-count** *value* command is executed on two or more ports.

201409050021

- Symptom: A user cannot pass the RADIUS authentication.
- Condition: This symptom occurs when the attributes issued by the RADIUS server are as follows during the RADIUS authentication/authorization process:
  - The attribute 65 (Tunnel-Medium-Type) is set to 802.
  - The attribute 64 (Tunnel-Type) is set to VLAN.
  - No VLAN ID is configured in the attribute 81 (Tunnel-Private-Group-ID).

201409100112

- Symptom: The switch forwards a BDDP packet in which the destination MAC address is 0180-c200-000e and the Ethernet protocol number is 0x8999, which should be terminated by the switch.
- Condition: This symptom can be seen when default settings are used.

201408190596

- Symptom: IPv6 portal users cannot be forcibly logged out by configuring the security policy server.
- Condition: N/A.

Resolved problems in R2221P05

201407110331

- Symptom: In an OpenFlow application, BDDP packets cannot be sent to the controller.
- Condition: This symptom can be seen when the following conditions exist:
    - The switch has a flow table that can send BDDP packets to the controller.
    - BDDP packets with destination MAC address 0180-C200-000E and EtherType 0x8999 enter the switch through an OpenFlow port.

201408050475

- Symptom: The ABR of an NSSA area fails to advertise intra-NSSA routes in Type-3 LSAs to other areas.
- Condition: This symptom can be seen if the AS has more than 100 NSSA areas.

201408050489

- Symptom: A BGP session between two BGP peers is broken upon TCP packet timeout.
- Condition: This symptom can be seen if the following conditions exist:
    - The two BGP peers use loopback interfaces to establish a BGP session.
    - The physical link between the peers goes down and up.

201407030446

- Symptom: SPI conflicts occur during IKE SA establishment.
- Condition: This symptom can be seen when the switch uses IKE autonegotiation to establish SAs with the peer.

201408050575

- Symptom: Static routes might fail to take effect.
- Condition: This symptom might be seen after an IRF master/subordinate switchover.

201405230224

- Symptom: The output from the **display interface** command for a Layer 3 aggregate interface always shows 0s for all statistics items.
- Condition: This symptom can be seen when you use the **display interface** command to view statistics for a Layer 3 aggregate interface.

201407030392

- Symptom: A software upgrade through IMC BIMS fails.
- Condition: This symptom can be seen if you use IMC BIMS to upgrade software.

201407250142

- Symptom: ND snooping fails to create entries on a port.
- Condition: This symptom can be seen if the port is enabled with port security.

201408040236

- Symptom: IMC fails to obtain MAC entries from a switch.
- Condition: This symptom can be seen if the MAC entries are on an IRF subordinate switch and they are secure MAC entries.

201407280518

- Symptom: The **voice vlan qos** command does not take effect on a port.

- Condition: This symptom can be seen if the port is configured with **lldp voice-vlan**.

201407220494

- Symptom: After commands are pasted in interface range view, some commands fail to be executed.
- Condition: This symptom can be seen after commands are pasted in interface range view.

201407160145

- Symptom: A Key Expansion Module (KEM) connected to an IP phone fails to startup.
- Condition: This symptom can be seen if the IP phone is connected to a PoE+ switch.

201407080366

- Symptom: After an IRF split, the switches are forced to wait for three seconds to start up.
- Condition: This symptom can be seen if an IRF fabric that is not configured with MAD splits.

201406200507

- Symptom: A port does not learn MAC addresses.
- Condition: This symptom can be seen if the following procedure is performed on the port:
    - Enable port security.
    - Configure port-based 802.1X authentication (userlogin).
    - Configure guest VLAN for 802.1X authentication.
    - Disable port security.

201407240303

- Symptom: The switch fails to deliver packets that match OpenFlow flow entries to the controller.
- Condition: This symptom can be seen if the matching OpenFlow flow entries include meter and an action of delivering packets to the controller.

201407150532

- Symptom: The switch fails to match packets with OpenFlow entries.
- Condition: This symptom can be seen if the OpenFlow entries of the flow tables in the pipeline have a metadata value of 0.

201408140267

- Symptom: The switch generates log messages when MMU parity errors occur.
- Condition: This symptom can be seen when MMU parity errors occur.

Resolved problems in R2221P04

201405190421

- Symptom: A portal client fails to pass portal authentication.
- Condition: This symptom can be seen if the following conditions exist:
    - The portal client, portal server, and RADIUS server belong to the same VPN instance.
    - A route that matches the IP address of the portal client exists in the public network or another VPN instance.

201406040506

- Symptom: A client fails to ping the gateway address.
- Condition: This symptom can be seen if the gateway address is in an 802.1X Free IP network.

201404290204

- Symptom: After the display openflow instance x flow-table command (x is an instance) is executed, the system takes about two minutes to show the information.
- Condition: This symptom can be seen if the following conditions exist:
  - The instance x contains 4094 VLANs and is connected to the controller.
  - The switch has learned a large number of MAC entries.

201405270108

- Symptom: Packet loss occurs when OpentFLow is enabled.
- Condition: This symptom can be seen if the controller deploys flow entries to multiple slices.

201406130469

- Symptom: On an IRF fabric, a port might fail to quit the 802.1X Guest VLAN after a user passes 802.1X authentication on the port.
- Condition: This symptom can be seen after a user passes 802.1X authentication on a port in the 802.1X Guest VLAN.

201405190429

- Symptom: The switches in an OSPF broadcast network might fail to communicate with each other after the OSPF broadcast network splits into multiple OSPF broadcast networks.
- Condition: This symptom can be seen after an OSPF broadcast network splits into multiple OSPF broadcast networks, because the switches fail to recalculate OSPF routes.

201405130384

- Symptom: The MAC addresses of authenticated users are aged out before the offline-detect timer expires.
- Condition: This symptom can be seen when MAC authentication is enabled.

201405070212

- Symptom: After a UPE is disconnected and then connected to an SPE, the SPE does not advertise optimal VPNv4 routes learned from the UPE to other PEs.
- Condition: This symptom can be seen when the following conditions exist:
  - In a HoVPN network, an SPE has leaned the same VPNv4 prefixes from a UPE and other PEs, and it prefers the prefixes from the UPE based on local preference.
  - The UPE is disconnected and then connected to the SPE to re-establish a BGP session.

201404160027

- Symptom: A DHCP client that moves from a port to another port of a DHCP snooping switch fails to re-obtain an IP address.
- Condition: This symptom occurs if the **dhcp-snooping no-user-binding** command is configured on the downlink port of the switch that connects to the client.

201404240078

- Symptom: The device provides no prompt information when the number of MAC entries exceeds the upper limit on a port.
- Condition: This symptom occurs if the port is configured with voice VLAN.

201404160434

- Symptom: A transient loop occurs in a smart link network.
- Condition: This symptom occurs if the primary and secondary ports of the smart link group reside on different IRF member switches and the primary link recovers from a failure.

201406100280

- Symptom: CVE-2014-0224
- Condition: When Open SSL Server or Client is used.

201406230110

- Symptom: When the controller deploys flow entries and barrier request messages to the switch, the replies to the barrier request messages time out.
- Condition: This symptom can be seen when an OpenFlow instance is activated and the switch has established a connection to the controller.

Resolved problems in R2221P02

201404020445

- Symptom: A DHCP client takes a long time to request an IP address.
- Condition: This symptom occurs when the VLAN interface enabled with the DHCP server is not on the same subnet as the IP address requested by the DHCP client. The DHCP server does not respond with a NAK packet, so the client sends the request multiple times before sending a Discovery packet.

201404020414

- Symptom: The switch unexpectedly reboots when the DHCP server receives a DHCP request.
- Condition: This symptom occurs if the DHCP request contains Option 82 sub-option 5 that is longer than four bytes.

201404020474

- Symptom: The CPU usage is 100% after a static route is configured.
- Condition: This symptom occurs if the following conditions exist:
  - The static route has a nonexistent next hop that belongs to the static route's destination network.
  - There is a route destined to a super network that comprises the static route's destination network, or there is a default route.

201404040414

- Symptom: Using SSH user accounts A and B on SecureCRT fails to log in to the switch through Stelnet or Telnet.
- Condition: This symptom occurs if the following conditions exist:
  - Account A uses password authentication, and account B uses password-public key authentication.
  - Using account A fails to log into the switch and then use account B to log into the switch.

201404030004

- Symptom: Deleting a BGP VPN instance or a BGP address family on an IRF fabric fails.
- Condition: This symptom occurs if the IRF master switch does not receive any response from the IRF subordinate switch because an error occurs on the subordinate switch during the delete operation.

201403120056

- Symptom: After a port goes down, dynamic secure MAC entries on the port cannot move to other ports.

- Condition: This symptom occurs when a port configured with autolearn security mode and dynamic MAC learning goes down.

201402110424

- Symptom: The switch does not send LLDP packets to the connected controller.
- Condition: This symptom occurs when the switch enabled with LLDP is configured with a link aggregation group.

201404180344

- Symptom: The default ARP rate-limit setting fails to be restored after the **undo arp rate-limit** command is configured.
- Condition: This symptom can be seen if the following procedure is performed:
- Enable ARP detection.
- Execute the **arp rate-limit rate** command.
- Execute the **undo arp rate-limit** command.

201404120217

- Symptom: The switch fails to bind N:1 vlan mappings to DHCP snooping entries.
- Condition: This symptom can be seen when DHCP snooping is enabled.

201404100060

- Symptom: A portal-free rule configured with **source ip any** can be assigned for Layer 2 portal authentication.
- Condition: This symptom can be seen when a portal-free rule is configured with **source ip any**.

201404020238

- Symptom: A Web user can delete local users.
- Condition: This symptom can be seen when the Web user has a level 2 privilege.

201401100054

- Symptom: When a duplicate flow entry is deployed to an OpenFlow switch, the switch prompts "add flow entry", which should be "add duplicate flow entry".
- Condition: This symptom can be seen when a duplicate flow entry is deployed to an OpenFlow switch.

201402250517

- Symptom: A user fails 802.1X authentication.
- Condition: This symptom occurs if the server assigns the user an ACL name.

201403040400

- Symptom: An intra-area or inter-area OSPF route is added with a tag.
- Condition: This symptom occurs if the intra-area or inter-area OSPF route has the same destination address, mask, and egress interface as a tag-included OSPF route calculated from a Type 5 LSA.

201402270224

- Symptom: A user fails to log in to the switch.
- Condition: This symptom occurs if the following conditions exist:
    - The user uses RADIUS authentication.
    - The RADIUS server assigns multiple login-service attributes for the user.

201402250220

- Symptom: After an inactive combo interface is activated, the **bpdu-drop any** setting configured on the interface does not take effect.
- Condition: This symptom can be seen after an inactive combo interface configured with **bpdu-drop any** is activated.

201403010118

- Symptom: The server fails to assign an authorized VLAN to a user who has passed 802.1X, MAC, or portal authentication.
- Condition: This symptom occurs if the authorized VLAN ID is a character string ended with null characters, such as 0x0032313900.

Resolved problems in R2221P01

201401070024

- Symptom: BGP ECMP does not consider IGP costs, resulting in unbalanced load sharing.
- Condition: This symptom can be seen when multiple BGP ECMP routes exist.

201401150513

- Symptom: Memory leaks occur.
- Condition: This symptom can be seen when the switch sends large numbers of packets to the controller through packet-in and then packet-out fails due to configuration errors.

201401130043

- Symptom: The switch loses the connection to the controller.
- Condition: This symptom occurs if the switch takes a long time to learn the flow entries, resulting in keepalive timeout.

201401100124

- Symptom: A Table Miss rule in the MAC-IP flow table exists in software but does not exist in hardware.
- Condition: This symptom can be seen if the following conditions exist:
  - All hardware ACL resources are used up.
  - The action of the assigned Table Miss rule is gototable, and then the Table Miss rule is deleted.

201312230375

- Symptom: The switch is attacked by IPv6 packets with a TTL of 1.
- Condition: This symptom might be seen when the switch is disabled from sending ICMPv6 timeout packets.

201401090182

- Symptom: IGMPv3 fails to create multicast entries.
- Condition: This symptom occurs when the following conditions exist:
  - IGMPv3 and IGMP SSM-Mapping are configured on the switch.
  - The client uses IGMPv3 but has no multicast source specified.

201402190416

- Symptom: The active physical port of a Combo interface automatically enables the STP BPDU drop function.

- Condition: This symptom occurs if the inactive physical port of the Combo interface is configured with **bpdu-drop any**.

201401150506

- Symptom: The DHCP server on the switch fails to assign IP addresses to clients.
- Condition: This symptom occurs if PBR matching broadcast packets is configured on the switch.

201312160317

- Symptom: The ARP packets that match a miss rule are not sent to the OpenFlow controller.
- Condition: This symptom occurs if the VLAN in the OpenFlow instance is not configured with a VLAN interface.

201401070307

- Symptom: If a flow entry is added or deleted on the controller, the flow entries on the switch become incorrect for milliseconds, resulting in forwarding errors.
- Condition: This symptom can be seen if a flow entry is added or deleted on the controller.

201312220008

- Symptom: If an ACL rule in PBR is deleted and added, the IRF fabric fails to assign the ACL to the subordinate switch.
- Condition: This symptom occurs if an ACL rule in PBR is deleted and added on an IRF fabric.

Resolved problems in R2221

201311280368

- Symptom: An interface on an LSPM2GP2P/LSPM2SP2P card cannot come up.
- Condition: This symptom occurs after the following procedure is performed:
    - Install an LSPM2GP2P/LSPM2SP2P card on the switch.
    - Use the **shutdown** command to shut down an interface on the LSPM2GP2P/LSPM2SP2P card.
    - Save the configuration and reboot the switch.
    - After the switch is rebooted, execute the **undo shutdown** command on the interface.

201310160360

- Symptom: The switch unexpectedly reboots when it repeatedly loads and unloads a hot patch for link aggregation.
- Condition: This symptom might occur when the switch repeatedly loads and unloads a hot patch for link aggregation.

201308160251

- Symptom: ARP Scan does not work on Layer 3 interfaces of IRF subordinate switches.
- Condition: This symptom can be seen on Layer 3 interfaces of IRF subordinate switches.

201309220392

- Symptom: The CDP neighbor continually ages out.
- Condition: This symptom occurs if the CDP neighbor is a Cisco's LLDP-capable phone.

201311150133

- Symptom: A DHCP response is discarded during inter-VLAN forwarding. The DHCP client thus fails to obtain an IP address.

- Condition: This symptom can be seen when DHCP snooping is globally enabled and multiple VLANs are configured.

201310230091

- Symptom: Modifying DHCP option 60 fails on the switch that acts as the DHCP server.
- Condition: This symptom can be seen when you modify DHCP option 60 on the switch that acts as the DHCP server.

201312160300

- Symptom: The A5500-24G EI switch fails to load the configuration file after a reboot.
- Condition: This symptom can be seen if the A5500-24G EI switch has two AC power modules and uses only one of them.

Resolved problems in R2220P11

201311280103

- Symptom: Addressed SSRT101324. A security bulletin for SSRT101324 should be published in January 2014. Please see the security bulletin for additional details.
- Condition: Addressed SSRT101324. A security bulletin for SSRT101324 should be published in January 2014. Please see the security bulletin for additional details.

Resolved problems in R2220P10

None

Resolved problems in R2220P09

ZDD06392

- Symptom: The switch unexpectedly reboots because of an SNMP agent anomaly.
- Condition: This symptom occurs when the following conditions exist:
    - SNMPv2, SNMPv3, SSH, DHCP, and OSPF attacks exist.
    - The SMMP agent on the switch receives an SNMPv3 packet that is larger than the globPDUSize (the default is 1500) and the contextName field of the SNMPv3 packet is almost the globPDUSize.

LSD075609

- Symptom: After a static route becomes invalid due to power-down of the master, the track entry bound to the static route is still in positive state.
- Condition: This symptom occurs after a static route becomes invalid due to power-down of the master.

LSD075361

- Symptom: sFlow MIBs such as sFlowRcvrTimeout fail to be set.
- Condition: This symptom can be seen when sFlow is enabled.

LSD075443

- Symptom: The switch unexpectedly reboots after two voice NQA operations that have the same source IP address but different destination IP addresses have been performed for a certain time.

- Condition: This symptom occurs if two voice NQA operations that have the same source IP address but different destination IP addresses have been performed for a certain time.

201307310278

- Symptom: The **System Information** Web page displays garbled characters under the **Temperature** option of the **System Resource State** field.
- Condition: This symptom can be seen if you use IE10 to access the Web interface of the switch.

201308010339

- Symptom: The system repeatedly prompts “The default route has been changed or deleted, protocol is OSPF” when the optimal default route is not changed.
- Condition: This symptom occurs if a non-optimal default route is deleted.

201309060056

- Symptom: The switch prints information about duplicate memory releases.
- Condition: This symptom can be seen if the SNMP agent uses the getbulk operation to obtain the values of four or more ospfLsdbAdvertisement MIB variables when OSPF neighbor relationships have been established.

201308290108

- Symptom: When SNMP Agent V3 is used to obtain the values of two MIB variables, the first value is Null.
- Condition: This symptom can be seen if the second MIB variable is ifTableLastChange or ifStackLastChange.

201305210418

- Symptom: OSPF fails to calculate routes to specific networks.
- Condition: This symptom occurs if IP addresses in a subnet such as 192.168.1.1/24 and 192.168.1.2/24 reside in different networks.

201308300169

- Symptom: When an ACS server acts as the RADIUS server, the switch fails to assign priorities for authenticated SSH users.
- Condition: This symptom occurs when an ACS server is used as the RADIUS server to authenticate SSH users.

201308060203

- Symptom: The hh3cSysImageName MIB cannot be read.
- Condition: This symptom occurs if hh3cSysImageName MIB is read.

LSD074587

- Symptom: Device could not handle invalid SNMP packet and resulted in an exception.
- Condition: Device received an invalid SNMP packet with overlong OID.

LSD074729

- Symptom: Device could not handle SSH packet which had many special characters and resulted in an exception.
- Condition: Device received a SSH packet which had many 0x07 as control-character.

LSD075470

- Symptom: Device could not handle invalid SNMP packet and resulted in an exception.
- Condition: Device received an invalid SNMP packet which had an oversize ContextName field.

Resolved problems in R2220P07

ZDTB00315

- Symptom: Failed to upload files to an appointed path when authentication is required by iMC BIMs.
- Condition: When system try to upload a file to iMC BIMs and authentication is required.

LSD075250

- Symptom: A switch fails to communicate with a Cisco's 6509 device through STP.
- Condition: This symptom can be seen when a switch tries to communicate with a Cisco's 6509 device through STP.

LSD074592

- Symptom: The switch discards ARP packets with multiple VLAN tags received from a QinQ-enabled interface.
- Condition: This symptom occurs if the QinQ-enabled interface is a trunk or hybrid interface that permits VLANs on which ARP detection or ARP snooping is enabled.

LSD075296

- Symptom: A switch does not send traps to the NMS after it recovers from high-temperature alarm state.
- Condition: This symptom can be seen after a switch recovers from high-temperature alarm state.

ZDTB00320

- Symptom: The VPN instance specified in an ACL that is referenced by the **ip http acl** command does not work.
- Condition: This symptom can be seen if a VPN instance is specified in an ACL that is referenced by the **ip http acl** command.

ZDTB00321

- Symptom: The CPU usage on a PVST-enabled Switch is 100% when the switch receives a lot of TC packets.
- Condition: This symptom occurs when the device enables PVST and receives a lot of TC packets.

ZDTB00323

- Symptom: A switch unexpectedly reboots when it performs IKE negotiation with a TOPSEC device.
- Condition: This symptom occurs when a switch performs IKE negotiation with a TOPSEC device.

ZDTB00324

- Symptom: A 10-second traffic interruption occurs during an IRF split.
- Condition: This symptom can be seen if the following conditions exist:
  - LACP MAD is enabled on the IRF fabric
  - The number of member ports in the link aggregation group that connect the intermediate device to the IRF fabric almost reach or has reached the upper limit.
  - An IRF split occurs.

LSD074994

- Symptom: If a port that has learned an authenticated MAC address in multiple VLANs leaves a VLAN, the authenticated MAC address is removed from that VLAN and also from all other VLANs.
- Condition: This symptom occurs if the following conditions exist:
  - The port is a trunk/hybrid port.
  - The port is enabled with MAC authentication multi-VLAN mode.
  - The port has learned an authenticated MAC address in multiple VLANs.
  - The port leaves a VLAN.

Resolved problems in R2220L06

LSD074756

- Symptom: The master device of the IRF fabric abnormally reboots.
- Condition: The contact or location configured in SNMP contains more than 200 characters. A user logs into the Web NMS.

LSD074592

- Symptom: The software drops the multi-tagged ARP packets received from a QinQ-enabled port.
- Condition: Configure the link type of a port as trunk or hybrid, enable QinQ on the port, and assign the port to a VLAN with ARP detection or ARP snooping enabled.

ZDTB00317

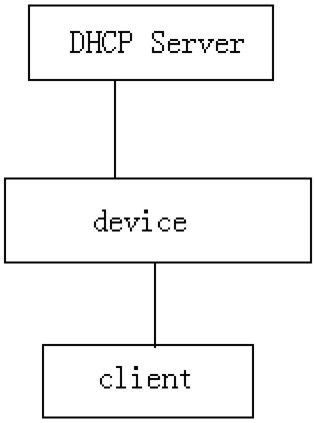
- Symptom: The standby MPU of the device frequently prints “The default route has been changed or deleted, protocol is OSPF.”
- Condition: Enable the NSR function on two MPUs (one active MPU and one standby MPU). The OSPF routes change.

LSD074248

- Symptom: Directly connected devices cannot ping each other.
- Condition: Configure a Layer 2 aggregation group in the Web interface. When you choose multiple member ports and add them to the aggregation group in batches, the member ports become Selected in the platform, but part of the ports are blocked in the driver.

LSD074348

- Symptom: No DHCP snooping entries exist on the device.
- Condition: As shown in the following figure, DHCP snooping and the DHCP relay agent are enabled on the device. The client obtains an IPv6 address from the DHCP server.



-

Resolved problems in R2220P02

LSD074256

- Symptom: When a DHCP relay device receives an Option 82-included packet in which the length value specified for the Agent Information Field is larger than the actual length of the Agent Information Field, the device reboots.
- Condition: This symptom occurs when the DHCP relay device receives an Option 82-included packet in which the length value specified for the Agent Information Field is larger than the actual length of the Agent Information Field.

LSD074279

- Symptom: After a user fails and then passes 802.1X authentication, the MAC address of the user in the 802.1X critical VLAN cannot be deleted.
- Condition: This symptom occurs if the configured 802.1X critical VLAN ID is the same as the PVID on the port.

LSD074423

- Symptom: After a PC passes MAC authentication on a port, the port still discards IGMP report packets from the PC.
- Condition: This symptom occurs if the port works in userlogin-secure-or-mac-ext mode and is enabled with both MAC authentication and 802.1X authentication.

LSD074302

- Symptom: After a switch reboots, the 10 GE fiber port on interface card 2 goes up but cannot forward packets and the STP state on the port is inactive.
- Condition: This symptom might occur when the following conditions exist:
    - Interface card 1 is not in position.
    - Interface card 2 is inserted with a 10 GE transceiver module and the STP state on the fiber port is forwarding.
    - The switch is rebooted.

LSD073833

- Symptom: After NTP traps are disabled with the “undo snmp-agent trap enable system” command, NTP traps are still generated.
- Condition: This symptom can be seen although NTP traps have been disabled with the “undo snmp-agent trap enable system” command.

ZDTB00312

- Symptom: When OSPF receives Type 4 LSAs from different areas, it does not select the optimal route, but selects the last received LSA and advertises it to other areas.
- Condition: This symptom occurs when OSPF receives Type 4 LSAs from different areas.

ZDTB00309

- Symptom: If an IS-IS cost is changed twice quickly, an error occurs to IS-IS route calculation.
- Condition: This symptom might occur if an IS-IS cost is changed twice quickly.

ZDTB00315

- Symptom: When CWMP uses an HTTP put operation to send a configuration file to a peer that requires authentication, the HTTP put operation fails.
- Condition: This symptom occurs when CWMP uses an HTTP put operation to send a configuration file to a peer that requires authentication.

Resolved problems in R2220

ZDTB00403

- Symptom: An MSDP peer cannot come up.
- Condition: This symptom might occur when the CPUs of the MSDP client and server are busy.

ZDTB00305

- Symptom: During a software upgrade, anomalies might occur to OSPF route calculation.
- Condition: This symptom might be seen if OSPF has multiple neighbors and large numbers of routing entries and summary routes.

LSD073378

- Symptom: In a RADIUS AAA scenario, RADIUS accounting packets carry incorrect traffic statistics.
- Condition: This symptom might occur if a dot1x user has been online for a long time in port security mode.

LSD072929

- Symptom: A switch in an IRF fabric might forward broadcast packets received from a member port of a link aggregation group to another member port in the same group.
- Condition: This symptom might occur if the member ports of the link aggregation group reside on different switches in the IRF fabric, and some member ports go up and down.

LSD073000

- Symptom: A port might fail to forward packets when its duplex state is continually changed.
- Condition: This symptom might occur if the port continually changes its duplex state and meanwhile multiple ports are congested.

LSD074033

- Symptom: The switch fails to learn new ARP entries when some ARP entries have errors.
- Condition: This symptom might be seen when the following conditions exist:
    - Inter-VPN traffic exists.
    - Multiple ARP entries contain the same MAC address, and the egress port to the MAC address of one ARP entry is changed.

LSD073845

- Symptom: ARP does not learn the addresses in an ARP reply in which the target MAC address in the message body is different from the destination MAC address in the message header.
- Condition: This symptom can be seen when the switch receives an ARP reply in which the target MAC address in the message body is different from the destination MAC address in the message header.

LSD073696

- Symptom: When the primary OSPF link recovers, the switch fails to switch traffic from the backup link to the primary link.
- Condition: This symptom might occur if the primary and backup OSPF links have different costs.
-

Resolved problems in F2218L02

ZDTB00301

- Symptom: BGP discards an incoming BGP route update that contains a summary route destined for 0.0.0.0, resulting in loss of some BGP routes.
- Condition: This symptom occurs when BGP receives a BGP route update that contains a summary route destined for 0.0.0.0.

ZDTB00302

- Symptom: During an IRF master/subordinate switchover, a user that is accessing a device connected to the IRF fabric has traffic interruption that lasts more than 1 minute.
- Condition: This symptom might occur if an IRF master/subordinate switchover is performed when a user is accessing a device connected to the IRF fabric.

LSD072889

- Symptom: When the switch acts as the SSH server, the first SSH login to the switch times out.
- Condition: This symptom occurs if DSA, RSA, or hotkey is not configured, because the system needs time to create the key.

Resolved problems in F2218P01

- None

Resolved problems in F2218

LSD072187

- Symptom: When access the hh3cUserPassword node of hh3cUserInfoTable by SNMP, the device return the user’s password.
- Condition: Access the hh3cUserPassword node of hh3cUserInfoTable by SNMP.

ZDTB00298

- Symptom: The switch might reboot if the portal authentication function on a VLAN interface is disabled when portal users are going online.
- Condition: This symptom might occur if you disable portal authentication function on a VLAN interface when portal users are going online.

LSD072331

- Symptom: After a reboot, the **super password level x hash** setting gets lost from the configuration file.
- Condition: This symptom might occur after a reboot.

LSD072325

- Symptom: A user that has passed MAC-based 802.1X authentication on a port cannot access the network.
- Condition: This symptom might occur if some ports are configured with MAC-based 802.1X authentication and some other ports are configured with port-based 802.1X authentication and guest VLAN.

LSD072523

- Symptom: When CWMP is disabled on an IRF fabric, a reboot of a member switch might cause the other member switch to reboot.
- Condition: This symptom might occur if an IRF member switch is rebooted when CWMP is disabled on the IRF fabric.

LSD072504

- Symptom: If the **mac-address station-move quick-notify enable** command is configured on the RRPP master node, a link-down event on a transit node cannot be quickly reported.
- Condition: This symptom occurs if the **mac-address station-move quick-notify enable** command is configured on the RRPP master node.

Resolved problems in F2217

ZDTB00288

- Symptom: The IP address of a Null interface assigned through SNMP cannot be deleted.
- Condition: This symptom might occur on a Null interface whose IP address is assigned through SNMP.

ZDTB00293

- Symptom: A walk of lldpRemSysName MIB returns “No Such Instance currently exists at this OID”.
- Condition: This symptom might occur when the port has an LLDP neighbor and the TimeFilter is set to 0.

LSTB005612

- Symptom: The etherStatsOversizePkts field has an exceptionally large value in the output of the display rmon statistics command.
- Condition: This symptom might occur if the reset count interface command is executed on a port configured with RMON accounting when the port has traffic.

ZDTB00287

- Symptom: When a device uses a routing policy to filter BGP routes with specific AS-path and community attributes, the device has low efficiency. When some routes matching the policy flap, the CPU usage is high for a long time.
- Condition: The first symptom might occur if the routing policy contains a large number of regular expressions. The second symptom might occur if some routes matching such a routing policy flap.

LSD071986

- Symptom: This symptom might occur on a switch where MFF is enabled on some VLANs to which a combo port belongs but is disabled on other VLANs of the combo port , save configuration and the switch cannot boot up.
- Condition: None.

LSD071810

- Symptom: The value obtained by an SNMP walk of probeCapabilities MIB is incorrect.
- Condition: This symptom might occur during an SNMP walk of probeCapabilities MIB.

LSD071866

- Symptom: A port connected to a client that fails and then passes 802.1X authentication cannot leave the guest VLAN. As a result, the client cannot access the network.
- Condition: This symptom might occur if the both following conditions exist:
- (1)802.1X is enabled on the port, and the guest VLAN and Auth-Fail VLAN are configured as the same VLAN.
- (2)The port is assigned to the guest VLAN after the client fails authentication, and then the client passes authentication.

LSD071501

- Symptom: A client that passes 802.1X authentication cannot access the network.
- Condition: This symptom might occur when the both following conditions exist on the port connected to the client:
- (1)MAC authentication and 802.1X authentication are both configured and the VLAN to which the port is assigned when the client passes MAC authentication is configured.
- (2)802.1X authentication is performed after MAC authentication succeeds.

LSD071635

- Symptom: A port cannot come up after the fiber or fiber transceiver connected to the port is inserted and removed multiple times.
- Condition: This symptom might occur after the fiber or fiber transceiver connected to a port is inserted and removed multiple times.

Resolved problems in R2215

LSD69938

- Symptom: After an IRF master/subordinate switchover, configuring PoE ports through a PoE profile fails.
- Condition: This symptom might occur if you use a PoE profile to configure PoE ports after an IRF master/subordinate switchover.

ZDD04981

- Symptom: The HTTPS server enabled on the switch fails to work and users cannot access the Web interface or log in to the switch through SSH.
- Condition: This symptom might occur when the switch receives TCP attacks such as SSH attacks.

ZDD04994

- Symptom: The CLI does not respond to an NMS that uses SNMPv3 with 3DES to access the switch.

- Condition: This symptom might occur when an NMS uses SNMPv3 with 3DES to access the switch.

LSD070340

- Symptom: The switch reboots when an SNMPv3 client accesses it.
- Condition: This symptom might occur if the SNMPv3 client matches an ACL rule that is configured with the **logging** keyword.

LSD070554

- Symptom: Saving a large configuration file through Web fails.
- Condition: This symptom might occur when you use Web to save a large configuration file.

LSD68432

- Symptom: Strict uRPF check does not work for specific traffic.
- Condition: This symptom might occur if the specific traffic matches Ipv4 routes learned from an ABR.

LSD67940

- Symptom: CDP packets have incorrect checksums.
- Condition: This symptom might occur when the **lldp compliance cdp** command is configured in system view.

LSD070943

- Symptom: IMC fails to walk the hh3cSysCurImageIndex MIB node and cannot get version information.
- Condition: This symptom might occur when IMC walks the hh3cSysCurImageIndex MIB node to get version information.

LSD64524

- Symptom: LLDP packets have incorrect auto-negotiation capability values in TLVs and relevant MIB values displayed are also incorrect.
- Condition: This symptom might occur when the switch is enabled with LLDP.

Resolved problems in F2212

LSD66630

- Symptom: The panels of HP TAA devices are wrongly displayed
- Condition: Entering the web interface.

LSD67507

- Symptom: Only 32 ARP entries are updated when more than 32 MAC addresses are moved to different ports.
- Condition: This symptom might occur when more than 32 MAC addresses are moved to different ports.

LSD68504

- Symptom: A QoS policy fails to be applied.
- Condition: This symptom might occur when the traffic behaviors of the QoS policy include both Car and Remark actions.

LSD65758

- Symptom: There is some checksum error information when insert old 3Com SFP transceivers.
- Condition: None.

Resolved problems in F2211

LSD64553

- Symptom: The switch cannot be rebooted from an NMS (for example, IMC) through SNMP.
- Condition: This symptom might occur if the NMS uses SNMP to reboot the switch.

LSD65459

- Symptom: Memory leaks occur on the HTTP module and the switch might reboot if the switch receives large amounts of HTTP packets with the same fields.
- Condition: This symptom might occur if the switch receives large amounts of HTTP packets with the same fields.

LSD65492

- Symptom: The switch drops IP fragments.
- Condition: This symptom might occur when DHCP snooping is enabled globally.

LSD65749

- Symptom: The returned value of dot3StatsDuplexStatus MIB on a down port is not “unknown” but is the same as the value (for example, full-duplex) when the port is up.
- Condition: This symptom might occur during a walk of dot3StatsDuplexStatus MIB on a port that is down.

Resolved problems in R2210

LSD59568

- Symptom: During IRF split, OSPF neighbors are reformed, resulting in packet loss.
- Condition: This symptom might occur if an IRF fabric that comprises multiple S5500EI switches and has LACP MAD configured splits.

LSD62084

- Symptom: A MAC address that has passed authentication in a VLAN cannot be authenticated in other VLANs.
- Condition: None.

LSD57794

- Symptom: The port information in trap messages is incorrect when MAC addresses are added or removed on a port configured with mac-address information.
- Condition: This symptom exists in trap messages generated when MAC addresses are added or removed on a port configured with mac-address information.

LSD62470

- Symptom: The switch performs unknown unicast storm suppression according to all unicast packets, including known unicast packets and unknown unicast packets.
- Condition: This symptom might occur if storm-constrain mode for unicast traffic is configured as PPS.

LSD62954

- Symptom: EAP failure messages sent by the switch do not conform to RFC3748.
- Condition: This symptom exists in EAP failure messages sent by the switch.

LSD58411

- Symptom: During IRF split and merge, LACP MAD on an aggregate interface fails to work because some member ports cannot be selected.
- Condition: This symptom might occur if the aggregate interface is configured as a reserved interface and IRF split and IRF merge occur.

TCD02667

- Symptom: Some online users are logged off when many users get online through a port enabled with MAC-based VLAN, Voice VLAN, and 802.1X.
- Condition: This symptom might occur if the port is enabled with MAC-based VLAN, Voice VLAN, and 802.1X and too many users get online through the port.

LSD60563

- Symptom: When an SSH user passes TACACS+ authentication but fails authorization, a memory access anomaly occurs, resulting in protocol interruption or system reboot.
- Condition: This symptom might occur when an SSH user passes TACACS+ authentication but fails authorization.

LSD60569

- Symptom: Authenticated portal users experience a very slow speed during access to the Web server.
- Condition: This symptom might occur when more than 100 portal users access the Web server concurrently and many portal-free rules are configured.

Resolved problems in R2208

LSD60570

- Symptom: Applying MQC or packet filter rules on ports fails.
- Condition: This symptom might occur if the same Ipv4 and IPv6 rules are applied in the outbound direction on two or more physical ports.

LSD56439

- Symptom: OSPF neighbors are disconnected and reformed.
- Condition: This symptom might occur if OSPF with MD5 authentication has run for a long time when many OSPF neighbors exist.

LSD57597

- Symptom: The Option field of DHCP packets received by the switch has incorrect information.
- Condition: This symptom might occur when the switch is configured with the DHCP snooping option and the receiving port is configured with QinQ.

ZDD03868

- Symptom: An NQA operation fails.
- Condition: This symptom might occur when a next hop is specified for the NQA operation.

LSD59556

- Symptom: OSPF routes cannot be removed during continuous route flapping.

- Condition: This symptom might occur because continuous OSPF route flapping results in fast increase of LSA advertisement time.

LSD55389

- Symptom: The configured NAS IP address cannot be assigned.
- Condition: This symptom might occur if the least significant octet of the NAS IP address is 255.

LSD58705

- Symptom: The NTP peer on a VLAN interface cannot be removed.
- Condition: This symptom might occur if you perform the following steps multiple times:

a. Configure the NTP broadcast-server or NTP broadcast-client on the VLAN interface.

b. Configure the NTP peer on the VLAN interface.

c. Remove the VLAN interface' IP address, the VLAN interface, and the NTP peer.

LSD60991

- Symptom: The switch cannot establish LLDP neighbor relationship with a Cisco IP phone.
- Condition: This symptom might occur when the switch connects to the Cisco IP phone through LLDP.

LSD59580

- Symptom: The mac-address max-mac-count configuration cannot take effect when you make this configuration on two ports whose port number difference is 24 (for example, g1/0/1 and g1/0/25 or g1/0/3 and g1/0/27).
- Condition: This symptom might occur if you configure mac-address max-mac-count on two ports whose port number difference is 24 on an S5500-52C-EI/S5500-52C-PWR-EI switch.

LSD60395

- Symptom: An SNMP walk of dot1qVlanStaticUntaggedPorts MIB returns an incorrect value.
- Condition: This symptom occurs during an SNMP walk of dot1qVlanStaticUntaggedPorts MIB.

ZDD03986

- Symptom: The 64-byte memory is corrupted when a packet received from the RADIUS server contains a 63-byte callback number, resulting in command resolution failure or a system reboot.
- Condition: This symptom might occur if a packet received from the RADIUS server contains a 63-byte callback number.

LSD59641

- Symptom: Authentication and accounting servers configured on the IMC fail to be assigned.
- Condition: This symptom might occur when you use IMC to configure and assign authentication and accounting servers.

LSD60392

- Symptom: The **bpdu-drop any** configuration gets lost on some ports of a subcard.
- Condition: This symptom might occur after you configure the **bpdu-drop any** command on the subcard and then remove and insert the subcard.

Resolved Problems in R2208

First release

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:
  www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:
  www.hpe.com/support/hpesc

Information to collect:

- Technical support registration number (if applicable).
- Product name, model or version, and serial number.
- Operating system name and version.
- Firmware version.
- Error messages.
- Product-specific reports and logs.
- Add-on products or components.
- Third-party products or components.

Documents

To find related documents, see the Hewlett Packard Enterprise Support Center website at http://www.hpe.com/support/hpesc.

- Enter your product name or number and click **Go**. If necessary, select your product from the resulting list.
- For a complete list of acronyms and their definitions, see HPE FlexNetwork technology acronyms.

Related documents

The following documents provide related information:

- HP 5500 EI & 5500 SI Switch Series Installation Guide
- HP 5500 EI & 5500 SI Switch Series Configuration Guides-Release 2220
- HP 5500 EI & 5500 SI Switch Series Command References-Release 2220
- HP PSR150-A & PSR150-D Series Power Supplies User Guide

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

Appendix A Feature list

Hardware features

Table 6 Technical specifications (I)

<table>
<tr><th>Item</th><th>HP A5500-24G EI (2 slots)
HP A5500-24G EI TAA (2 slots)</th><th>HP A5500-48G EI (2 slots)
HP A5500-48G EI TAA (2 slots)</th><th>HP A5500-24G-SFP EI (2 slots)
HP A5500-24G-SFP EI TAA (2 slots)</th></tr>
<tr><td>Dimensions (H × W × D)</td><td>43.6 × 440 × 300 mm
(1.72 × 17.32 × 11.81 in)</td><td>43.6 × 440 × 300 mm
(1.72 × 17.32 × 11.81 in)</td><td>43.6 × 440 × 360 mm
(1.72 × 17.32 × 14.17 in)</td></tr>
<tr><td>Weight</td><td>< 5 kg (11.02 lb)</td><td>< 5 kg (11.02 lb)</td><td>< 6 kg (13.23 lb)</td></tr>
<tr><td>Management port</td><td colspan="3">One console port, on the front panel</td></tr>
<tr><td rowspan="3">Fixed network ports (on the front panel)</td><td>24 × 10/100/1000Base-T auto-sensing Ethernet port
4 × 1000Base-X SFP port</td><td>48 × 10/100/1000Base-T auto-sensing Ethernet port
4 × 1000Base-X SFP port</td><td>8 × 10/100/1000Base-T auto-sensing Ethernet port
24 × 1000Base-X SFP port</td></tr>
<tr><td colspan="2">The last four 10/100/1000Base-T Ethernet ports and the four SFP ports comprise four combo interfaces.</td><td>The last eight SFP ports and the eight 10/100/1000Base-T Ethernet ports comprise eight combo interfaces.</td></tr>
<tr><td colspan="3">For each combo interface, either the SFP port or the corresponding Ethernet port can be used at a time. For the port pairs forming combo interfaces, see Table 8.</td></tr>
<tr><td>Interface card slots</td><td colspan="3">Two on the rear panel</td></tr>
<tr><td>Interface card models</td><td colspan="3">• LSPM2GP2P (JD367A) (not supporting IRF)
• LSPM1CX2P (JD360B) (supporting IRF)
• LSPM2SP2P (JD368B) (supporting IRF)
• LSPM1XP2P (JD359B) (supporting IRF)
• LSPM1XP1P (JD361B) (supporting IRF)</td></tr>
<tr><td>Hot swappable power supplies</td><td>N/A</td><td>N/A</td><td>PSR150-A (JD362A)
PSR150-D (JD366A)</td></tr>
<tr><td>Power supply system</td><td colspan="3">The A5500-24G-SFP EI (2 slots), A5500-24G-SFP EI TAA (2 slots) and S5500-28F-EI adopt hot-swappable power supplies, and provides two power supply slots.
The other models have two fixed power receptacles.</td></tr>
<tr><td>Power receptacle types and quantity</td><td>H3C S5500-28C-EI-DC: 1 AC power socket and 1 –48V DC power socket
The other models:1 AC power socket and 1 RPS power socket</td><td>1 AC power socket and 1 RPS power socket</td><td>PSR150-A (JD362A): 1 AC power socket
PSR150-D (JD366A): 1 –48V DC power socket</td></tr>
</table>

Item	HP A5500-24G EI (2 slots) HP A5500-24G EI TAA (2 slots)	HP A5500-48G EI (2 slots) HP A5500-48G EI TAA (2 slots)	HP A5500-24G-SFP EI (2 slots) HP A5500-24G-SFP EI TAA (2 slots)
Input voltage	AC	• Rated voltage range: 100 VAC to 240 VAC, 50 Hz or 60 Hz • Input voltage range: 90 VAC to 264 VAC, 47 Hz to 63 Hz	
	–48V DC	• Rated voltage range: –48 VDC to –60 VDC • Input voltage range: –36 VDC to –72 VDC	
	RPS	The rated voltage range is 10.8 VDC to 13.2 VDC. Use the external RPS power supply unit—HPE A-RPS800 (JD183A) and H3C RPS800-A—recommended by HPE/H3C only.	
Minimum power consumption	H3C S5500-28C-EI-DC: 27W The other models:36 W	63 W	PSR150-A (JD362A): 44 W PSR150-D (JD366A): 30 W
Maximum power consumption	H3C S5500-28C-EI-DC: 105W The other models:110 W	155 W	115 W
Cooling system	4 fans	6 fans (4 for the system, and 1 for each power supply)	
Operating temperature	0°C to 45°C (32°F to 113°F)		
Relative humidity (noncondensing)	10% to 90%		

Table 7 Technical specifications (II)

Item	HP A5500-24G-PoE+ EI (2 slots) HP A5500-24G-PoE+ EI TAA (2 slots)	HP A5500-48G-PoE+ EI (2 slots) HP A5500-48G-PoE+ EI TAA (2 slots)
Dimensions (H × W × D)	43.6 × 440 × 420 mm (1.72 × 17.32 × 16.54 in)	43.6 × 440 × 420 mm (1.72 × 17.32 × 16.54 in)
Weight	< 7.5 kg (16.53 lb)	< 8.0 kg (17.64 lb)
Management port	1 console port, on the front panel	
Fixed network ports (on the front panel)	24 × 10/100/1000Base-T auto-sensing Ethernet port (support PoE) 4 × 1000Base-X SFP port	48 × 10/100/1000Base-T auto-sensing Ethernet port (support PoE) 4 × 1000Base-X SFP port
	The last four 10/100/1000Base-T Ethernet ports and the four SFP ports comprise four combo interfaces. For each combo interface, either the SFP port or the corresponding Ethernet port can be used at a time. For the port pairs forming combo interfaces, see Table 8.	
Interface card slots	Two on the rear panel	

Item	HP A5500-24G-PoE+ EI (2 slots) HP A5500-24G-PoE+ EI TAA (2 slots)	HP A5500-48G-PoE+ EI (2 slots) HP A5500-48G-PoE+ EI TAA (2 slots)
Interface card models	• LSPM2GP2P (JD361B) (not supporting IRF) • LSPM1CX2P (JD360B) (supporting IRF) • LSPM2SP2P (JD368B) (supporting IRF) • LSPM1XP2P (JD359B) (supporting IRF) • LSPM1XP1P (JD361B) (supporting IRF)	
Power supply system	Two fixed power receptacles, one AC receptacle, and one RPS receptacle.	
Input voltage	AC Rated voltage range: 100 VAC to 240 VAC, 50 Hz or 60 Hz Input voltage range: 90 VAC to 264 VAC, 47 Hz to 63 Hz	
	RPS The rated voltage range is –55 VDC to –52 VDC. Use the external RPS power supply unit—HPE A-RPS1600 (JG136A) and H3C RPS1600-A—recommended by HPE/H3C only.	
Maximum PoE power per port	30 W	30 W
Total PoE power	370 W	AC power supply: 370 W RPS power supply: 740 W (The total PoE power of ports numbered 1 through 24 is 370 W, and that of ports numbered 25 through 48 is 370 W.)
Minimum power consumption	60 W	85 W
Maximum power consumption (including PoE power)	AC	221 W + 370W
	RPS	122 W + 370W
Cooling system	6 fans	
Operating temperature	0°C to 45°C (32°F to 113°F)	
Relative humidity (noncondensing)	10% to 90%	

Table 8 SFP-Ethernet port pairs forming Combo interfaces

Model	SFP port	10/100/1000Base-T Ethernet port
HP A5500-24G EI (2 slots) HP A5500-24G EI TAA (2 slots) HP A5500-24G-PoE+ EI (2	GigabitEthernet 1/0/25	GigabitEthernet 1/0/22
	GigabitEthernet 1/0/26	GigabitEthernet 1/0/24
	GigabitEthernet 1/0/27	GigabitEthernet 1/0/21

Model	SFP port	10/100/1000Base-T Ethernet port
slots) HP A5500-24G-PoE+ EI TAA (2 slots)	GigabitEthernet 1/0/28	GigabitEthernet 1/0/23
HP A5500-48G EI (2 slots) HP A5500-48G EI TAA (2 slots) HP A5500-48G-PoE+ EI (2 slots) HP A5500-48G-PoE+ EI TAA (2 slots)	GigabitEthernet 1/0/49	GigabitEthernet 1/0/46
	GigabitEthernet 1/0/50	GigabitEthernet 1/0/48
	GigabitEthernet 1/0/51	GigabitEthernet 1/0/45
	GigabitEthernet 1/0/52	GigabitEthernet 1/0/47
HP A5500-24G-SFP EI (2 slots) HP A5500-24G-SFP EI TAA (2 slots)	GigabitEthernet 1/0/17	GigabitEthernet 1/0/25
	GigabitEthernet 1/0/18	GigabitEthernet 1/0/26
	GigabitEthernet 1/0/19	GigabitEthernet 1/0/27
	GigabitEthernet 1/0/20	GigabitEthernet 1/0/28
	GigabitEthernet 1/0/21	GigabitEthernet 1/0/29
	GigabitEthernet 1/0/22	GigabitEthernet 1/0/30
	GigabitEthernet 1/0/23	GigabitEthernet 1/0/31
	GigabitEthernet 1/0/24	GigabitEthernet 1/0/32

Software features

Table 9 Software features

Feature	HP A5500-24G EI (2 slots) HP A5500-24G EI TAA (2 slots) HP A5500-24G-SFP EI (2 slots) HP A5500-24G-SFP EI TAA (2 slots)	HP A5500-48G EI (2 slots) HP A5500-48G EI TAA (2 slots)	HP A5500-24G-PoE+ EI (2 slots) HP A5500-24G-PoE+ EI TAA (2 slots)	HP A5500-48G-PoE+ EI (2 slots) HP A5500-48G-PoE+ EI TAA (2 slots)
Switching capacity (Full duplex)	128 Gbps	176 Gbps	128 Gbps	176 Gbps
Packet forwarding rate	95.2 Mpps	130.9 Mpps	95.2 Mpps	130.9 Mpps
Power over Ethernet	Not supported		Supported	

Feature	HP A5500-24G EI (2 slots) HP A5500-24G EI TAA (2 slots) HP A5500-24G-SFP EI (2 slots) HP A5500-24G-SFP EI TAA (2 slots)	HP A5500-48G EI (2 slots) HP A5500-48G EI TAA (2 slots)	HP A5500-24G-PoE+ EI (2 slots) HP A5500-24G-PoE+ EI TAA (2 slots)	HP A5500-48G-PoE+ EI (2 slots) HP A5500-48G-PoE+ EI TAA (2 slots)
Link aggregation	• Aggregation of GE ports • Aggregation of 10-GE ports • Static link aggregation • Dynamic link aggregation • Supports up to 128 aggregation groups, each supporting up to eight GE ports or eight 10-GE ports • Supports local-first load sharing for link aggregation • Supports configuring load sharing criteria for IRF links			
IRF	Supported			
IRF MAD Detection	• LACP MAD • ARP MAD • BFD MAD			
Flow control	IEEE 802.3x flow control and back pressure			
Jumbo Frame	Supports maximum frame size of 9 KB			
OpenFlow	Supported			
MAC address table	• 32K MAC addresses • 1K static MAC addresses • Blackhole MAC addresses • MAC address learning limit on a port			
VLAN	• Port-based VLANs (4094 VLANs) • QinQ and selective QinQ • Voice VLAN • Protocol-based VLANs • MAC-based VLANs • IP subnet-based VLANs • GVRP • Isolate User VLAN			
VLAN mapping	• One-to-one VLAN mapping • Many-to-one VLAN mapping • Two-to-two VLAN mapping			
ARP	• 8K entries • 1K static entries • Gratuitous ARP • Standard proxy ARP and local proxy ARP • ARP source suppression • ARP detection (based on static IP source guard binding Entries/DHCP snooping entries/802.1X security entries/OUI MAC addresses) • ARP filtering			

Feature	HP A5500-24G EI (2 slots) HP A5500-24G EI TAA (2 slots) HP A5500-24G-SFP EI (2 slots) HP A5500-24G-SFP EI TAA (2 slots)	HP A5500-48G EI (2 slots) HP A5500-48G EI TAA (2 slots)	HP A5500-24G-PoE+ EI (2 slots) HP A5500-24G-PoE+ EI TAA (2 slots)	HP A5500-48G-PoE+ EI (2 slots) HP A5500-48G-PoE+ EI TAA (2 slots)
ND	• 4K entries • 1K static entries • ND proxy • ND detection • ND snooping			
VLAN virtual interface	1K			
IPv4 DHCP	• DHCP client • DHCP snooping • DHCP relay agent • DHCP server			
IPv6 DHCP	• IPv6 DHCP snooping • IPv6 DHCP client • IPv6 DHCP relay agent • IPv6 DHCP server			
UDP Helper	UDP helper			
DNS	• Dynamic domain name resolution • Dynamic domain name resolution client • IPv4/IPv6 addresses			
IPv4 route	• 4K static routes • RIP v1/2; up to 2K IPv4 routes • OSPF v1/v2; up to 12K IPv4 routes • BGP; up to 12K IPv4 routes • ISIS; up to 12K IPv4 routes • Eight equal-cost routes • Routing policy • VRRP (supports standard mode and load balancing mode) • Policy based routing			
IPv6 route	• 1K static routes • RIPng; up to 2K IPv6 routes • OSPF v3; up to 6K IPv6 routes • BGP4+ for IPv6; up to 6K IPv6 routes • ISIS for IPv6;up to 6K IPv6 routes • Eight equal-cost routes • Routing policy • VRRP (supports standard mode and load balancing mode) • Policy based routing • Authenticating RIPng packets by using an IPsec policy • Authenticating OSPFv3 packets by using an IPsec policy • Authenticating IPv6 BGP packets by using an IPsec policy			

Feature	HP A5500-24G EI (2 slots) HP A5500-24G EI TAA (2 slots) HP A5500-24G-SFP EI (2 slots) HP A5500-24G-SFP EI TAA (2 slots)	HP A5500-48G EI (2 slots) HP A5500-48G EI TAA (2 slots)	HP A5500-24G-PoE+ EI (2 slots) HP A5500-24G-PoE+ EI TAA (2 slots)	HP A5500-48G-PoE+ EI (2 slots) HP A5500-48G-PoE+ EI TAA (2 slots)
URPF	Supported			
MCE	• Unicast • Multicast			
BFD	• OSPF • BGP • IS-IS • Static route			
IPv6 over IPv4 Tunnel	• IPv6 manual tunnel • 6to4 tunnel • ISATAP tunnel			
IPv4 multicast	• IGMP snooping v1/v2/v3 • Multicast VLAN • Multicast VLAN+ • IGMP v1/v2/v3 • PIM-DM • PIM-SM • PIM-SSM • MSDP • Multicast BGP • BIDIR-PIM • Configuring static multicast MAC address entries • Configuring a multicast user control policy			
IPv6 multicast	• MLD snooping v1/v2 • MLD v1/v2 • PIM-DM/SM/SSM/BIDIR-PIM for IPv6 • IPv6 multicast VLAN • IPv6 multicast VLAN+ • MBGP for IPv6 • Configuring an IPv6 multicast user control policy			
Broadcast/multicast/unicast storm control	• Storm control based on port rate percentage • PPS-based storm control • Kbps-based storm control			
MSTP	• STP/RSTP/MSTP protocol • STP root guard • BPDU guard			
RRPP	• RRPP protocol • Multi-instance RRPP			
Smart link	• Up to 26 groups • Multi-instance smart link			

Feature	HP A5500-24G EI (2 slots) HP A5500-24G EI TAA (2 slots) HP A5500-24G-SFP EI (2 slots) HP A5500-24G-SFP EI TAA (2 slots)	HP A5500-48G EI (2 slots) HP A5500-48G EI TAA (2 slots)	HP A5500-24G-PoE+ EI (2 slots) HP A5500-24G-PoE+ EI TAA (2 slots)	HP A5500-48G-PoE+ EI (2 slots) HP A5500-48G-PoE+ EI TAA (2 slots)
Monitor link	Supported			
BPDU tunnel	CDP\DLDP\EOAM\GVRP\HGMP\LACP\LLDP\PAGP\PVST\STP\UDLD\VTP			
QoS/ACL	• Restriction of the rates at which a port sends and receives packets, with a granularity of 64 kbps. • Packet redirection • Committed access rate (CAR), with a granularity of 64 kbps. • Eight output queues for each port • Flexible queue scheduling algorithms based on port and queue, including strict priority (SP), weighted round robin (WRR), WFQ(Weighted Fair Queuing), SP + WRR, WDRR, and WDRR+SP. • Remarking of 802.1p and DSCP priorities • Packet filtering at L2 (Layer 2) through L4 (Layer 4); flow classification based on source MAC address, destination MAC address, source IP (IPv4/IPv6) address, destination IP (IPv4/IPv6) address, port, protocol, and VLAN. • Time range • Weighted Random Early Detection (WRED) • Traffic shaping • Packet filtering • Dynamically modifying QoS			
Mirroring	• Traffic mirroring • Port mirroring			
Remote mirroring	Remote port mirroring			

Feature	HP A5500-24G EI (2 slots) HP A5500-24G EI TAA (2 slots) HP A5500-24G-SFP EI (2 slots) HP A5500-24G-SFP EI TAA (2 slots)	HP A5500-48G EI (2 slots) HP A5500-48G EI TAA (2 slots)	HP A5500-24G-PoE+ EI (2 slots) HP A5500-24G-PoE+ EI TAA (2 slots)	HP A5500-48G-PoE+ EI (2 slots) HP A5500-48G-PoE+ EI TAA (2 slots)
Security	• Hierarchical management and password protection of users • AAA authentication • RADIUS authentication • HWTACACS • SSH 2.0 • Port isolation • Port security • MAC address authentication • IP-MAC-port binding • IP Source Guard (Including IPv4 and IPv6) • HTTPS • SSL • PKI • Portal • EAD • Boot ROM access control (password recovery) • Local security authentication based on layer-2 Portal and RADIUS • Triple authentication • Portal stateful failover • User profile			
802.1X	• Up to 1,024 users • Port-based and MAC address-based authentication • Guest VLAN • 802.1X-based dynamic QoS/ACL/VLAN delivery • 802.1X re-authentication			
Download and upgrade	• XModem • FTP • TFTP			
Management	• Configuration at the command line interface • Remote configuration through Telnet • Configuration through Console port • Simple network management protocol (SNMP) • Remote monitoring (RMON) alarm, event and history recording • IMC • Web-based network management • System log • Hierarchical alarms • HGMP v2 • NTP • Power supply alarms • Fan and temperature alarms			

Feature	HP A5500-24G EI (2 slots) HP A5500-24G EI TAA (2 slots) HP A5500-24G-SFP EI (2 slots) HP A5500-24G-SFP EI TAA (2 slots)	HP A5500-48G EI (2 slots) HP A5500-48G EI TAA (2 slots)	HP A5500-24G-PoE+ EI (2 slots) HP A5500-24G-PoE+ EI TAA (2 slots)	HP A5500-48G-PoE+ EI (2 slots) HP A5500-48G-PoE+ EI TAA (2 slots)
Maintenance	• Debugging information output • Ping and Tracert • NQA • Track • Virtual cable test • CFD (IEEE 802.1ag and ITU-T Y.1731) • Ethernet OAM (IEEE 802.3ah) • DLDP • ISSU • sFlow			
Energy saving	• Port auto-power-down • Configuring scheduled tasks • Regulating fan speed according to temperature			

Appendix B Upgrading software

This section describes how to upgrade software while the router is operating normally or when the router cannot correctly start up.

You can access the Boot menu or the CLI to upgrade software images (.bin system software images and .btm Boot ROM images).

Table 10 Software upgrade methods

Method	Section
Upgrading software from the Boot menu	XMODEM download through the console port
	TFTP download through an Ethernet port
	FTP download through an Ethernet port
Upgrading software from the CLI	FTP download from a server
	TFTP download from a server

Method	Section
	XMODEM download through the console port
	TFTP download through an Ethernet port
	FTP download through an Ethernet port
Upgrading software from the CLI	FTP download from a server
	TFTP download from a server

When upgrading software, make sure the versions of the Boot ROM and system software images are compatible.

The procedures for upgrading Boot ROM and system software from the Boot menu are the same except that you must choose different options from the Boot menu (**1** for upgrading system software, and **6** for upgrading Boot ROM) to start the upgrade procedure. This appendix describes only the Boot ROM upgrade procedure.

Accessing the Boot menu

1. Power on the switch, for example, an HP A5500-24G EI Switch with 2 Interface Slots.

   The following information appears:

```
Starting......
*****************************************************************************
*                                                                           *
*      HP A5500-24G EI Switch with 2 Interface Slots BOOTROM, Version 713   *
*                                                                           *
*****************************************************************************
            Copyright (c) 2010-2012 Hewlett-Packard Development Company, L.P.
            Creation date   : Dec 11 2012, 00:50:08
            CPU Clock Speed : 533MHz
```

```
                BUS Clock Speed : 133MHz
                Memory Size     : 256MB
                Mac Address     : 00238980549a
Press Ctrl-B to enter Boot Menu... 1
```

2. Press **Ctrl** + **B** within 1 second (in fast startup mode) or 5 seconds (in full startup mode) after the "Press Ctrl-B to enter Boot Menu..." prompt message appears. If you fail to do this, the system starts decompressing the system software.

   By default, the system starts up in fast mode.

   ```
   BootRom password: Not required. Please press Enter to continue.
   ```

3. Press **Enter** at the prompt for password.

   The password recovery capability is enabled." or "Password recovery capability is disabled." message appears, followed by the Boot menu. Availability of some menu options depends on the state of password recovery capability (see Table 11). For more information about password recovery capability, see *HP 5500 EI & 5500 SI Switch Series Fundamentals Configuration Guide* .

```
Password recovery capability is enabled.

            BOOT   MENU

1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter bootrom upgrade menu
7. Skip current configuration file
8. Reserved
9. Set switch startup mode
0. Reboot
Ctrl+F: Format File System
Ctrl+D: Enter Debugging Mode
Ctrl+T: Enter Board Test Environment

Enter your choice(0-9):
```

Table 11 Boot menu options

Option	Tasks
1. Download application file to flash	Download a .bin system software image to the flash.
2. Select application file to boot	• Specify the main and backup system software images for the next startup. • Specify the main and backup configuration files for the next startup. This task can be performed only if password recovery capability is enabled.
3. Display all files in flash	Display files on the flash.
4. Delete file from flash	Delete files to free storage space.
5. Restore to factory default configuration	Delete the current next-startup configuration files and restore the factory-default configuration. This option is available only if password recovery capability is disabled.

Option	Tasks
6. Enter BootRom upgrade menu	Access the Boot ROM upgrade menu. If password recovery capability is enabled, you can upgrade the Boot ROM to any version. If password recovery capability is disabled, you can upgrade the Boot ROM to only Version 715 or higher.
7. Skip current system configuration	Start the switch without loading any configuration file. This is a one-time operation and takes effect only for the first system boot or reboot after you choose this option. This option is available only if password recovery capability is enabled.
8. Reserved	Reserved option field.
9. Set switch startup mode	Set the startup mode to fast startup mode or full startup mode.
0. Reboot	Reboot the switch.
Ctrl+F: Format File System	Format the current storage medium.
Ctrl+D: Enter Debugging Mode	Access the debugging menu. For options in the debugging menu, see Table 12. This option is available only if password recovery capability is enabled.
Ctrl+T: Enter Board Test Environment	This option is not supported.

Table 12 Debugging menu options

Option	Task
1. Load elf file	Download an ELF file and start the switch with the file.
2. display cpld version	Display CPLD information.
3. Load app file to sdram	Load and run a system software image in the SDRAM.
0. Return to boot menu	Return to the Boot menu.

XMODEM download through the console port

You can connect a PC or terminal to the console port to download files to the switch by using XMODEM. XMODEM supports 128-byte data packets and provides the reliability mechanisms including checksum, CRC, and retransmissions (up to 10).

Setting terminal parameters

Run a terminal emulator program on the console terminal, for example, a PC.

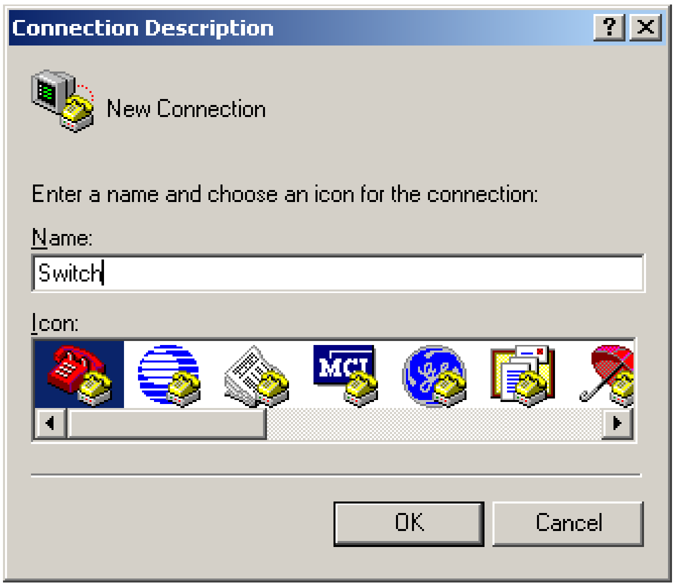
The following are the required terminal settings:

- Bits per second—9,600
- Data bits—8
- Parity—None
- Stop bits—1
- Flow control—None
- Emulation—VT100

Follow these steps to set terminal parameters, for example, on a Windows XP HyperTerminal:

1. Select **Start** > **All Programs** > **Accessories** > **Communications** > **HyperTerminal**, and in the **Connection Description** dialog box that appears, type the name of the new connection in the **Name** text box and click **OK**.

Figure 1 Connection description of the HyperTerminal

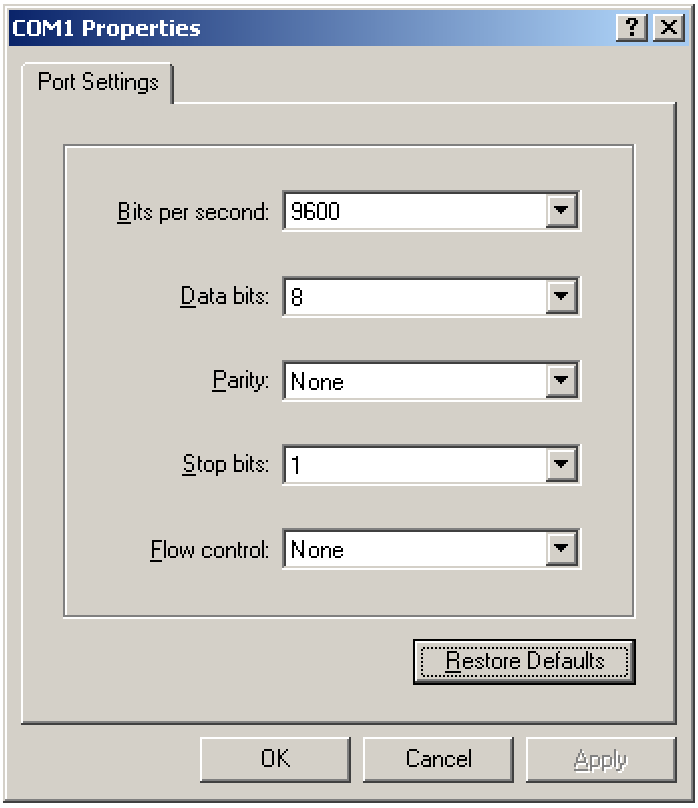


2. Select the serial port to be used from the **Connect using** drop-down list, and click **OK**.

Figure 2 Set the serial port used by the HyperTerminal connection

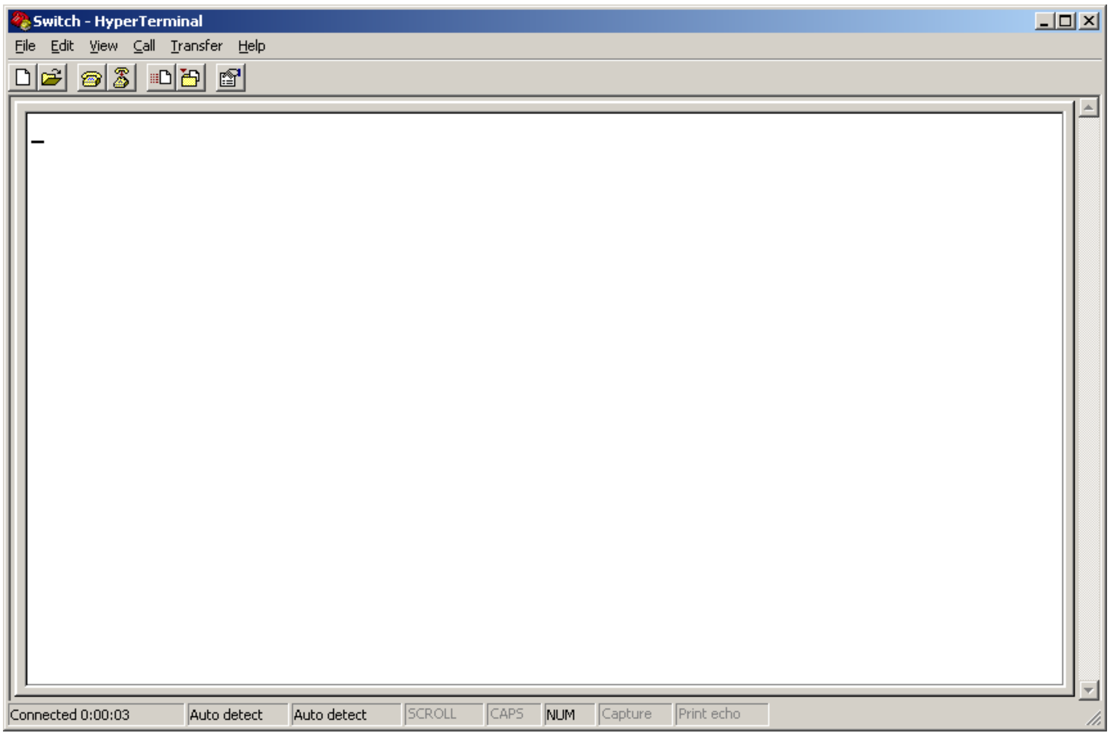
3. Set **Bits per second** to **9600**, **Data bits** to **8**, **Parity** to **None**, **Stop bits** to **1**, and **Flow control** to **None**, and click **OK**.

Figure 3 Set the serial port parameters



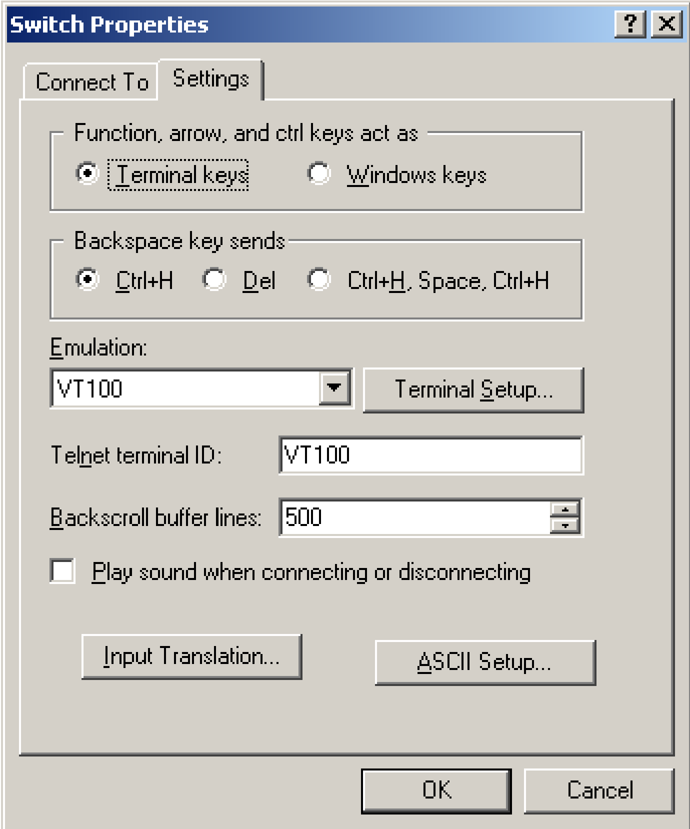
4. Select **File** > **Properties** in the HyperTerminal window.

Figure 4 HyperTerminal window



5. Click the **Settings** tab, set the emulation to **VT100**, and click **OK** in the **Switch Properties** dialog box.

Figure 5 Set terminal emulation in Switch Properties dialog box



Upgrading Boot ROM

Perform the following tasks to upgrade Boot ROM by using XMODEM through the console port:

1. Enter **6** or press **Ctrl** + **U** at the Boot menu to access the Boot ROM update menu:

```
Bootrom update menu:
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu

Enter your choice(0-3):
```

2. Enter **3** to set the XMODEM download baud rate.

```
Please select your download baudrate:
1.* 9600
2. 19200
3. 38400
4. 57600
5. 115200
0. Return
Enter your choice (0-5):
```

3. Select an appropriate download rate, for example, enter **5** to select 115200 bps.

```
Download baudrate is 115200 bps
Please change the terminal's baudrate to 115200 bps and select XMODEM protocol
Press enter key when ready
```

NOTE:

Typically the size of a .bin file is over 10 MB. Even at a baud rate of 115200 bps, the download takes tens of minutes.

4. Set the serial port on the terminal to use the same baud rate and protocol as the console port. If you select 9600 bps as the download rate for the console port, skip this task.
5. Select **Call** > **Disconnect** in the HyperTerminal window to disconnect the terminal from the switch.

Figure 6 Disconnect the terminal from the switch

6. Select **File** > **Properties**. In the **Properties** dialog box, click **Configure** (see Figure 7), and then select **115200** from the **Bits per second** drop-down list box (see Figure 8).

Figure 7 Properties dialog box

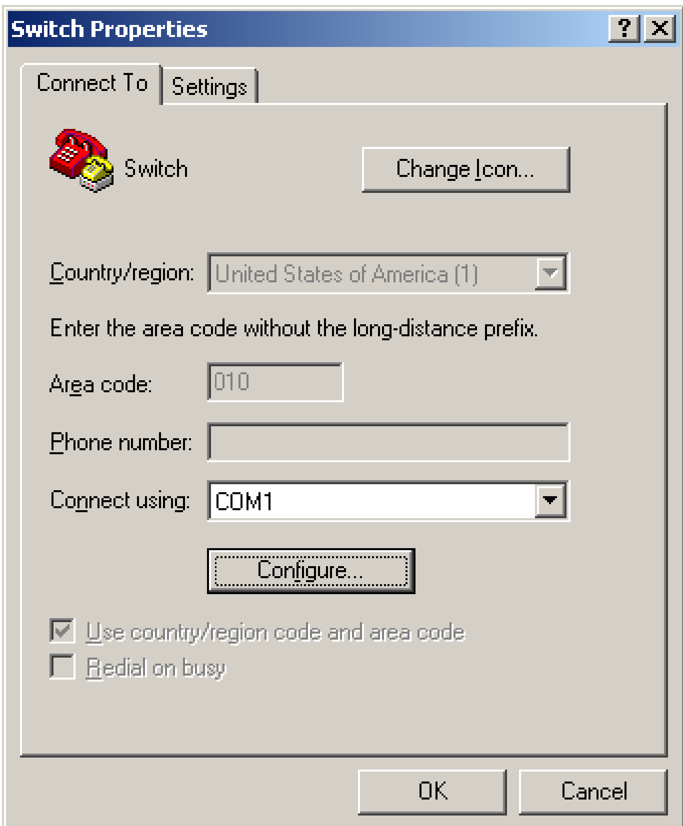
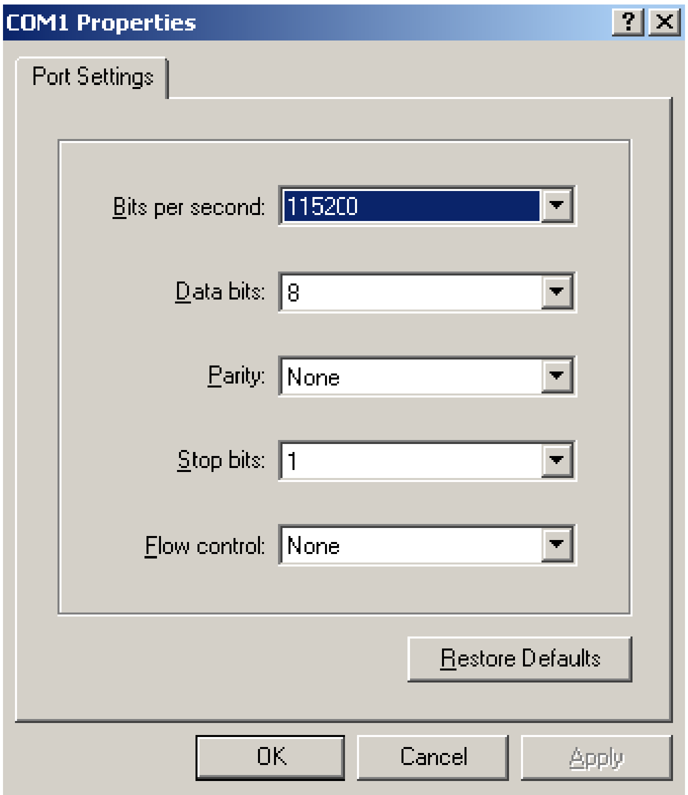
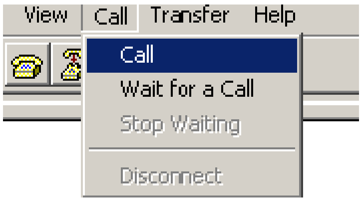


Figure 8 Modify the baud rate



7. Select **Call** > **Call** to reestablish the connection.

Figure 9 Reestablish the connection



NOTE:

The new settings take effect after you reestablish the connection.

---

8. Upload the software package file from the terminal to the switch.
9. After establishing a connection between the terminal and the switch, press **Enter** in the HyperTerminal window.

```
CCCCCCCCCCCCCCCCCC
```

NOTE:

To abort the downloading, press **Ctrl + X**.

---

10. Select **Transfer** > **Send File** in the HyperTerminal window (see Figure 10), and click **Browse** in the pop-up dialog box (see Figure 11) to select the source file (for example, **bootrom.btm**), and select **Xmodem** from the **Protocol** drop-down list.

Figure 10 Transfer menu

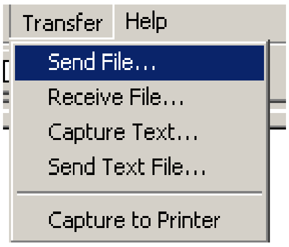
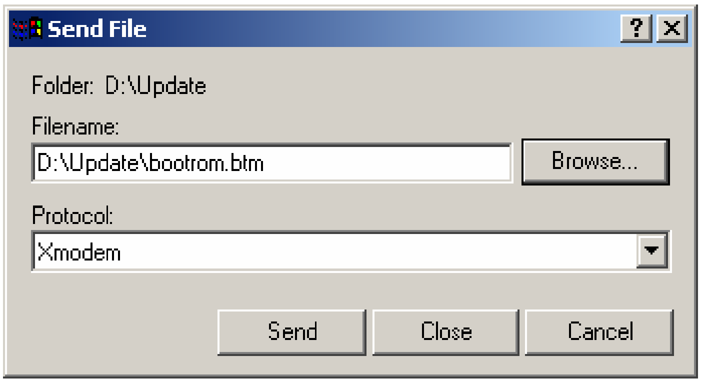
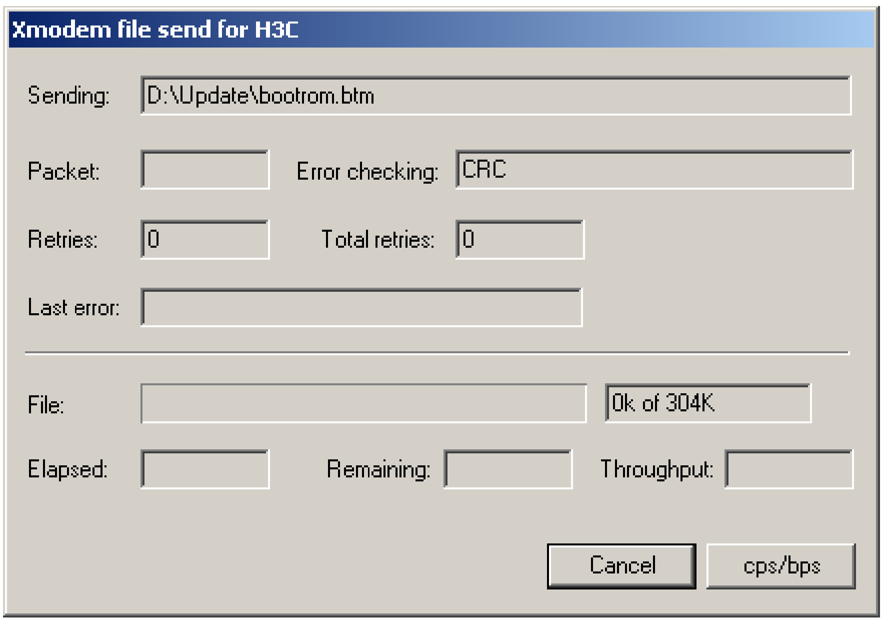


Figure 11 File transmission dialog box



11. Click **Send**. The following dialog box appears:

Figure 12 Send the application file using XMODEM



When the download is completed, the terminal displays the following information:

```
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCdone!
Bootrom updating..........done!

Your baudrate should be set to 9600 bps again!
Press enter key when ready
```

12. If you are using a download rate other than 9600 bps, restore the baud rate of the serial port on the terminal to 9600 bps. If the baud rate is 9600 bps, skip this step.
13. Press **Enter** to return to the Boot menu and enter **0** to restart the switch so the updated image can take effect.

```
         BOOT  MENU

1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter bootrom upgrade menu
7. Skip current configuration file
8. Reserved
9. Set switch startup mode
0. Reboot
Ctrl+F: Format File System
Ctrl+D: Enter Debugging Mode
Ctrl+T: Enter Board Test Environment

Enter your choice(0-9):
```

Upgrading system software

1. To upgrade system software, enter **1** at the Boot menu.

   The following menu appears:

```
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu

Enter your choice(0-3):3
```

2. Enter **3** to set the XMODEM parameters for downloading the system software image.

   The subsequent procedure is the same as loading Boot ROM images, except that you must set the attribute of the file as **main**, **backup**, or **none** to complete the file loading.

```
Please input a new file name           :update.bin
Free flash Space: 15598592 bytes
Writing flash.....................................................................
..................................................................................
..................................................................................
..................................................................................
..................................................................................
..................................................................................
.............................done!
Please input the file attribute (main/backup/none):main
done!
```

NOTE:

- The switch always attempts to boot first with the main file. If the attempt fails, for example, because the main file is not available, the switch tries to boot with the backup file. A file with the **none** attribute is for backup only and cannot be used for startup.
- If a file with the same attribute as the file you are loading is already in the flash, the attribute of the old file changes to **none** after the new file becomes valid.

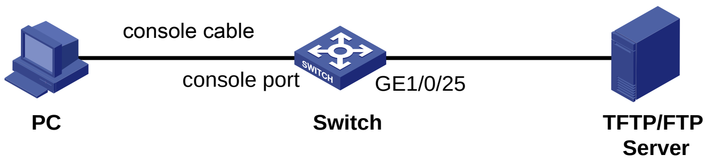
TFTP download through an Ethernet port

The switch can work as a TFTP client to download files from a TFTP server.

Upgrading Boot ROM

1. Connect an Ethernet port (for example, GigabitEthernet 1/0/25) of the switch to the server and connect the console port of the switch to a PC (see Figure 13).

Figure 13 Load software using TFTP/FTP through Ethernet port



NOTE:

- The PC and the TFTP/FTP server can be co-located.
- The HP A5500 EI switches do not come with any TFTP server program, and you must install one yourself.

2. Run the TFTP server program on the server and specify the source file path.
3. Run a terminal emulator program on the PC, power on the switch, access the Boot menu, and enter **6** to access the Boot ROM update menu:

```
Bootrom update menu:
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu

Enter your choice(0-3):
```

4. Enter **1** to set the TFTP parameters.

```
Load File Name      :update.btm
Switch IP address         :10.10.10.3
Server IP address         :10.10.10.2
```

Table 13 Description of the TFTP parameters

Item	Description
Load File Name	Name of the file to be downloaded (for example, **update.btm**)
Switch IP address	IP address of the switch (for example, 10.10.10.3)
Server IP address	IP address of the TFTP server (for example, 10.10.10.2)

NOTE:

The switch must be on the same subnet as the server.

5. Enter all required parameters.

```
Are you sure you want to download file to flash? Yes or No(Y/N)
```

6. Enter **Y** at the prompt to upgrade Boot ROM.

```
Loading.......................................done
Bootrom updating..........done!


         BOOT  MENU

1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter bootrom upgrade menu
7. Skip current configuration file
8. Reserved
9. Set switch startup mode
0. Reboot
Ctrl+F: Format File System
Ctrl+D: Enter Debugging Mode
Ctrl+T: Enter Board Test Environment

Enter your choice(0-9):
```

7. Enter **0** to restart the switch from the Boot menu so the upgraded Boot ROM can take effect.

Upgrading system software

1. To upgrade system software, enter **1** at the Boot menu to access the following menu:

```
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu

Enter your choice(0-3):3
```

2. Enter **1** to set the TFTP parameters.

   The subsequent procedure of is the same as upgrading Boot ROM, except that you must set the attribute of the file as **main**, **backup**, or **none** to complete the file loading.

```
Writing flash...............................................................
................Done!
Please input the file attribute (Main/Backup/None) Main
Done!
```

NOTE:

- The switch always attempts to boot first with the main file. If the attempt fails, for example, because the main file is not available, the switch tries to boot with the backup file. A file with the **none** attribute is for backup only and cannot be used for startup.
- If a file with the same attribute as the file you are loading is already in the flash, the attribute of the old file changes to **none** after the new file becomes valid.

FTP download through an Ethernet port

The switch can work as an FTP server or FTP client to download files through an Ethernet port. This section uses the switch as an FTP client to describe the procedure.

Upgrading Boot ROM

NOTE:

When upgrading Boot ROM, the switch can work only as an FTP client.

1. Connect an Ethernet port (GigabitEthernet 1/0/25, for example) of the switch to the server and connect the console port of the switch to a PC (see Table 12Figure 13).
2. Run an FTP server program on the server, configure an FTP username and password, and specify the source file path.
3. Run a terminal emulator program on the PC, power on the switch, access the Boot menu, and enter **6** to access the Boot ROM update menu:

```
Bootrom update menu:

1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu

Enter your choice(0-3):
```

4. Enter **2** to set the FTP parameters.

```
Load File name      :update.btm
Switch IP address    :10.10.10.3
Server IP address   :10.10.10.2
FTP User Name       :user
FTP User Password   :123
```

Table 14 Description of the FTP parameters

Item	Description
Load File name	Name of the file to be downloaded (for example, **update.btm**)
Switch IP address	IP address of the switch (for example, 10.10.10.3)
Server IP address	IP address of the FTP server (for example, 10.10.10.2)
FTP User Name	Username for accessing the FTP server, which must be the same as configured on the FTP server.
FTP User Password	Password for accessing the FTP server, which must be the same as configured on the FTP server.

NOTE:

The switch must be on the same subnet as the server.

5. Enter all required parameters.

```
Are you sure you want to download file to flash? Yes or No(Y/N)
```

6. Enter **Y** at the prompt to upgrade Boot ROM.

```
Loading........................................done
Bootrom updating.........done!
```

```
         BOOT  MENU

1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter bootrom upgrade menu
7. Skip current configuration file
8. Reserved
9. Set switch startup mode
0. Reboot
Ctrl+F: Format File System
Ctrl+D: Enter Debugging Mode
Ctrl+T: Enter Board Test Environment

Enter your choice(0-9):
```

7. Enter **0** to restart the switch from the Boot menu so the upgraded Boot ROM can take effect.

Upgrading system software

1. To upgrade system software, enter **1** at the Boot menu to access the following menu:

```
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu
Enter your choice(0-3):3
```

2. Enter **2** to set the FTP parameters.

   The subsequent procedure is the same as upgrading Boot ROM, except that you must set the attribute of the file as **main**, **backup**, or **none** to complete the file loading.

```
Writing flash...............................................................
................Done!
Please input the file attribute (Main/Backup/None) M
Done!
```

NOTE:

- The switch always attempts to boot first with the main file. If the attempt fails, for example, because the main file is not available, the switch tries to boot with the backup file. A file with the **none** attribute is for backup only and cannot be used for startup.
- If a file with the same attribute as the file you are loading is already in the flash, the attribute of the old file changes to **none** after the new file becomes valid.

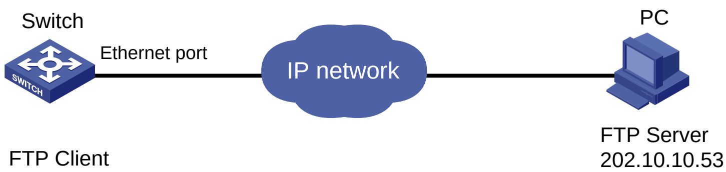
Upgrading software from the CLI

You can remotely download Boot ROM and system software images from the CLI.

FTP download from a server

This section uses the topology in Figure 14 as an example. Run FTP server on the management PC at 202.10.10.53, create an FTP username **admin** and password, specify the source file path, telnet to the switch, and get the system software image file **update.bin** and the Boot ROM image file **update.btm** from the server.

Figure 14 FTP download from a server



1. Get the files to the switch by using FTP.

```
<HP> ftp 202.10.10.53
Trying ...
Press CTRL+K to abort
Connected.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(none):user
331 Give me your password, please
Password:
230 Logged in successfully
[ftp] get update.bin
[ftp] get update.btm
[ftp] bye
```

2. Upgrade Boot ROM.

```
<HP> bootrom update file update.btm slot 1
This command will update bootrom file on the specified board(s), Continue? [Y/N]y
 Now updating bootrom, please wait...
Succeeded to update bootrom of Board 1
```

3. Load the system software image and specify the file as the main file at the next reboot.

```
<HP> boot-loader file update.bin slot 1 main
Slot 1
  This command will set the boot file. Continue? [Y/N]: y
  The specified file will be used as the main boot file at the next reboot on slot
1!
<HP> display boot-loader
 The current boot app is:  flash:/update.bin
 The main boot app is:     flash:/update.bin
 The backup boot app is:   flash:/update.bin
```

4. Reboot the switch with the **reboot** command to complete the upgrade.

CAUTION:

- If you have made any configuration, save the configuration before the reboot to avoid data loss.
- Avoid power failure during the loading process.

TIP:

If flash memory is insufficient, load the Boot ROM image first and delete unused files to free up flash memory before you load the system software image.

TFTP download from a server

The switch can work as a TFTP client to download files from a TFTP server, and the downloading procedure is similar to downloading files through FTP. With these two protocols, the subsequent Boot ROM and system software image loading procedures are the same.

HPE A5500EI-CMW520-R2222P12 Release Notes

Software Feature Changes

Contents

A5500EI-CMW520-R2222P12

This release has no feature changes.

A5500EI-CMW520-R2222P09

This release has the following changes:

- Modified feature: RADIUS Calling-Station-ID attribute value for the login service
- Modified feature: Port security need to know feature

Modified feature: RADIUS Calling-Station-ID attribute value for the login service

Feature change description

Before modification, the device fills 0 in the RADIUS Calling-Station-ID attribute for the login service.

After modification, the device fills the IP address of each login user in the RADIUS Calling-Station-ID attribute for the login service.

Command changes

None

Modified feature: Port security need to know feature

Feature change description

In this version, the ntkauto mode was added to the need to know (NTK) feature.

Command changes

Modified command: port-security ntk-mode

Old syntax

port-security ntk-mode { **ntk-withbroadcasts** | **ntk-withmulticasts** | **ntkonly** }

undo port-security ntk-mode

New syntax

port-security ntk-mode { **ntk-withbroadcasts** | **ntk-withmulticasts** | **ntkauto** | **ntkonly** }

undo port-security ntk-mode

Views

Ethernet interface view

Change description

The **ntkauto** keyword was added. If you specify this keyword, the device can send the following packets out of a port security-enabled port only when the port has online users:

- Broadcast packets.
- Multicast packets.

- Unicast packets whose destination MAC addresses have passed authentication.

A5500EI-CMW520-R2222P08

This release has no feature changes.

A5500EI-CMW520-R2222P07

This release has the following changes:

- New feature: Configuring the action a port takes after it receives an Ethernet OAM event from the remote end

New feature: Configuring the action a port takes after it receives an Ethernet OAM event from the remote end

Configuring the action a port takes after it receives an Ethernet OAM event from the remote end

This feature enables a port to log events and automatically terminate the OAM connection and set the link state to down.

To configure the action the port takes after it receives an Ethernet OAM event from the remote end:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet port view.	**interface** *interface-type interface-number*	N/A
3. Configure the action the port takes after it receives an Ethernet OAM event from the remote end.	**oam remote-failure** { **connection-expired** | **critical-event** | **dying-gasp** | **link-fault** } **action error-link-down**	By default, the port only logs the Ethernet OAM event it receives from the remote end.

Command reference

oam remote-failure action

Use **oam remote-failure action** to configure the action the port takes after it receives an Ethernet OAM event from the remote end.

Use **undo oam remote-failure action** to remove the configuration.

Syntax

oam remote-failure { **connection-expired** | **critical-event** | **dying-gasp** | **link-fault** } **action error-link-down**

undo oam remote-failure { **connection-expired** | **critical-event** | **dying-gasp** | **link-fault** } **action error-link-down**

Default

The port only logs the Ethernet OAM event it receives from the remote end.

Views

Layer 2 Ethernet port view

Default command level

2: System level

Parameters

connection-expired: Specifies a connection timeout fault.

critical-event: Specifies a critical fault.

dying-gasp: Specifies a fatal fault.

link-fault: Specifies a link fault.

error-link-down: Terminates the OAM connection and sets the link state of the port to down.

Examples

Configure Gigabitethernet 1/0/1 to terminate the OAM connection after it receives a critical event from the remote end, and set the link state of the interface to down.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname- Gigabitethernet1/0/1] oam remote-failure critical-event action error-link-down
```

A5500EI-CMW520-R2222P05

This release has no feature changes.

A5500EI-CMW520-R2222P02

This release has the following changes:

- Modified feature: Uploading IPv6 addresses for 802.1X and MAC authentication users

Modified feature: Uploading IPv6 addresses for 802.1X and MAC authentication users

Feature change description

Before modification: The device does not support uploading the IPv6 addresses of 802.1X and MAC authentication users to the RADIUS server.

After modification: After a user passes 802.1X or MAC authentication, the device obtains the IPv6 address of the user through DHCPv6 snooping or ND snooping entries. Then, the device uploads the IPv6 address to the RADIUS server through the Framed-IPv6-Address RADIUS attribute in realtime accounting packets.

A5500EI-CMW520-R2221P30

This release has the following changes:

- New feature: Including user IP addresses in realtime accounting packets for MAC authentication users with dynamic IP addresses
- New feature: Ignoring the ingress ports of ARP packets during user validity check
- New feature: Authorization VLAN auto-tagging for MAC authentication
- Modified feature: Specifying file name for storing DHCP snooping entries on a remote server
- Modified feature: Confining RADIUS Vendor-Specific extended attributes to a specific vendor

New feature: Including user IP addresses in realtime accounting packets for MAC authentication users with dynamic IP addresses

This feature enables the device to add user IP addresses to realtime accounting packets for the MAC authentication users who obtain IP addresses dynamically from a DHCP server. For this feature to work, you must configure MAC authentication and DHCP snooping.

The device sends a DHCP-REQUEST packet to the DHCP server after an MAC authentication users passes authentication. Upon receiving a DHCP-ACK packet from the DHCP server, the device generates a DHCP snooping entry and an IPSG binding entry for the user. The MAC authentication module obtains the user IP address from the IPSG binding entry. The device includes the obtained IP address in the realtime accounting packets for the user.

New feature: Ignoring the ingress ports of ARP packets during user validity check

Configuring ARP detection to ignore the ingress ports of ARP packets during user validity check

ARP detection performs user validity check on ARP packets from ARP untrusted interfaces. User validity check compares the sender IP and sender MAC in the received ARP packet with static IP source guard bindings, DHCP snooping entries, and 802.1X security entries. In addition, user validity check also compares the ingress port of the ARP packet with the port in the entries. If no matching port is found, the ARP packet is discarded.

You can enable this feature to ignore the ingress ports of ARP packets during user validity check.

To ignore the ingress ports of ARP packets during user validity check:

Step	Command	Remarks
4. Enter system view.	**system-view**	N/A
5. Ignore the ingress ports of ARP packets during user validity check.	**arp detection port-match-ignore**	Required. By default, the ingress ports of ARP packets are not ignored during user validity check.

Command reference

arp detection port-match-ignore

Use **arp detection port-match-ignore** to ignore the ingress ports of ARP packets during user validity check.

Use **undo arp detection port-match-ignore** to remove the configuration.

Syntax

arp detection port-match-ignore

undo arp detection port-match-ignore

Default

The ingress ports of ARP packets are not ignored during user validity check.

Views

System view

Default command level

2: System view

Examples

Ignore the ingress ports of ARP packets during user validity check.

```
<Sysname> system-view
[Sysname] arp detection port-match-ignore
```

New feature: Authorization VLAN auto-tagging for MAC authentication

Enabling authorization VLAN auto-tagging for MAC authentication

This feature adds a port to the authorization VLAN as a tagged or untagged member based on the tagged status of packets that triggered MAC authentication on the port.

This feature takes effect only on hybrid ports with MAC-based VLAN enabled.

The VLAN tag configuration set by this feature has higher priority than the server setting of whether to assign a tagged VLAN or not. However, if the server assigns a PVID, this feature does not take effect. Whether the port will add to the PVID as a tagged or untagged member depends on the server setting.

To enable authorization VLAN auto-tagging for MAC authentication:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A

Step	Command	Remarks
3. Enable authorization VLAN auto-tagging for MAC authentication.	**mac-authentication auto-tag** [**ignore-config**]	By default, authorization VLAN auto-tagging for MAC authentication is disabled. If you do not specify the **ignore-config** keyword, this command does not take effect if the authorization VLAN is specified by the **port hybrid vlan** command.

Command reference

mac-authentication auto-tag

Syntax

mac-authentication auto-tag [**ignore-config**]

undo mac-authentication auto-tag

Views

Ethernet interface view

Default command level

2: System level

Parameters

ignore-config: Ignores VLAN tag configuration on a port. If you do not specify this keyword, this command does not take effect if the authorization VLAN is specified by the **port hybrid vlan** command. Whether the port adds to the authorization VLAN as a tagged or untagged member depends on the port configuration.

Usage guidelines

Use **mac-authentication auto-tag** to enable authorization VLAN auto-tagging for MAC authentication.

Use **undo mac-authentication auto-tag** to disable authorization VLAN auto-tagging for MAC authentication.

By default, authorization VLAN auto-tagging for MAC authentication is disabled.

This command enables the device to add a port to the authorization VLAN as a tagged or untagged member based on the tagged status of packets that triggered MAC authentication.

This command takes effect only on hybrid ports with MAC-based VLAN enabled.

The VLAN tag configuration set by this command has higher priority than the server setting of whether to assign a tagged VLAN. However, if the server assigns a PVID, this command does not take effect. Whether the port will add to the PVID as a tagged or untagged member depends on the server setting.

Examples

Enable authorization VLAN auto-tagging for MAC authentication.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication auto-tag ignore-config
```

Modified feature: Specifying file name for storing DHCP snooping entries on a remote server

Feature change description

In this release, the device supports storing the DHCP snooping entries on a remote server. You can configure the login username and password when you specify the remote file name.

Command changes

Modified command: dhcp-snooping binding database filename

Old syntax

dhcp-snooping binding database filename *filename*

NewW syntax

dhcp snooping binding database filename { *filename* **| url** *url* [**username** *username* [**password** { **cipher | simple** } *string*]] }

Views

System view

Change description

After modification, the device supports configuring the URL of a remote file and configuring the username and password for login to the remote server.

Modified feature: Confining RADIUS Vendor-Specific extended attributes to a specific vendor

Feature change description

Support for confining RADIUS Vendor-Specific extended attributes to a specific vendor was added. With this feature, the device supports only a specific vendor for the Vendor-Specific attribute field to be sent to a RADIUS server.

Command changes

Modified command: service-type

Old syntax

server-type { **extended | standard** }

undo server-type

New syntax

server-type { **extended** [**vendor** *vendor-id*] **| standard** }

undo server-type

Views

RADIUS scheme view

Change description

The **vendor** *vendor-id* option was added to this command. This option confines Vendor-Specific extended attributes to a specific vendor. The value range for the *vendor-id* argument is 1 to 65535. The device supports the vendor IDs of 9, 43, 311, 2011, and 25506 in the current software version. If you do not specify a vendor ID with the **extended** keyword, the device can send Vendor-Specific extended attributes of all supported vendors to a RADIUS server.

A5500EI-CMW520-R2221P25

This release has the following changes:

- New feature: Configuring periodic MAC re-authentication

New feature: Configuring periodic MAC re-authentication

Configuring periodic MAC re-authentication

The device re-authenticates online MAC authentication users on a port at the periodic re-authentication interval if the port is enabled with periodic MAC re-authentication. Periodic MAC re-authentication tracks the connection status of online users and updates the authorization attributes assigned by the server, such as the ACL and VLAN.

You can set the periodic re-authentication interval either in system view or in interface view by using the **mac-authentication timer reauth-period** command. A change to the periodic re-authentication timer applies to online users only after the old timer expires.

The device selects a periodic re-authentication timer for MAC re-authentication in the following order:

1. Server-assigned re-authentication timer.
2. Port-specific re-authentication timer.
3. Global re-authentication timer.
4. Default re-authentication timer.

To configure periodic MAC re-authentication:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the global periodic re-authentication timer.	**mac-authentication timer reauth-period** *reauth-period-value*	Optional. The default is 3600 seconds.
3. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
4. Enable periodic MAC re-authentication.	**mac-authentication re-authenticate**	Required. By default, periodic MAC re-authentication is disabled on a port.
5. Set the periodic re-authentication timer on the port.	**mac-authentication timer reauth-period** *reauth-period-value*	Optional. By default, no periodic re-authentication timer is set on a port.

Command reference

New command: mac-authentication timer reauth-period (system view)

Use **mac-authentication timer reauth-period** to set the global periodic MAC re-authentication timer.

Use **undo mac-authentication timer reauth-period** to restore the default.

Syntax

mac-authentication timer reauth-period *reauth-period-value*

undo mac-authentication timer reauth-period

Default

The global periodic MAC re-authentication timer is 3600 seconds.

Views

System view

Default command level

2: System view

Parameters

reauth-period-value: Specifies the global periodic MAC re-authentication timer in seconds. The value range is 60 to 7200.

Usage guidelines

The device re-authenticates online MAC authentication users on a port at the specified periodic re-authentication interval if the port is enabled with periodic MAC re-authentication. To enable periodic MAC re-authentication on a port, use the **mac-authentication re-authenticate** command.

A change to the global periodic re-authentication timer applies to online users only after the old timer expires.

The device selects a periodic re-authentication timer for MAC re-authentication in the following order:

1. Server-assigned re-authentication timer.
2. Port-specific re-authentication timer.
3. Global re-authentication timer.
4. Default re-authentication timer.

Examples

Set the global periodic MAC re-authentication timer to 150 seconds.

```
<Sysname> system-view
[Sysname] mac-authentication timer reauth-period 150
```

Related commands

- **display mac-authentication**
- **mac-authentication re-authenticate**

New command: mac-authentication re-authenticate

Use **mac-authentication re-authenticate** to enable the periodic MAC re-authentication feature on a port.

Use **undo mac-authentication re-authenticate** to disable the periodic MAC re-authentication feature on a port.

Syntax

mac-authentication re-authenticate

undo mac-authentication re-authenticate

Default

The periodic MAC re-authentication feature is disabled on a port.

Views

Layer 2 Ethernet interface view

Default command level

2: System view

Usage guidelines

Periodic MAC re-authentication enables the access device to periodically authenticate online MAC authentication users on a port. This feature tracks the connection status of online users and updates the authorization attributes assigned by the server, such as the ACL and VLAN.

To set the periodic re-authentication interval, use the **mac-authentication timer reauth-period** command in system view or Layer 2 Ethernet interface view.

Examples

Enable the periodic MAC re-authentication feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication re-authenticate
```

Related commands

- **display mac-authentication**
- **mac-authentication timer**

New command: mac-authentication timer reauth-period (interface view)

Use **mac-authentication timer reauth-period** to set the port-specific periodic MAC re-authentication timer.

Use **undo mac-authentication timer reauth-period** to restore the default.

Syntax

mac-authentication timer reauth-period *reauth-period-value*

undo mac-authentication timer reauth-period

Default

No port-specific periodic MAC re-authentication timer is set for MAC re-authentication.

Views

Layer 2 Ethernet interface view

Default command level

2: System view

Parameters

reauth-period-value: Specifies the port-specific periodic MAC re-authentication timer in seconds. The value range is 60 to 7200.

Usage guidelines

The device re-authenticates online MAC authentication users on a port at the specified periodic re-authentication interval if the port is enabled with periodic MAC re-authentication. To enable periodic MAC re-authentication on a port, use the **mac-authentication re-authenticate** command.

A change to the port-specific periodic re-authentication timer applies to online users only after the old timer expires.

The device selects a periodic re-authentication timer for MAC re-authentication in the following order:

1. Server-assigned re-authentication timer.
2. Port-specific re-authentication timer.
3. Global re-authentication timer.
4. Default re-authentication timer.

Examples

Set the periodic MAC re-authentication timer to 90 seconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication timer reauth-period 90
```

Related commands

- **display mac-authentication**
- **mac-authentication re-authenticate**

Modified command: display mac-authentication

Syntax

display mac-authentication [**interface** *interface-list*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Change description

New fields were added to the command output for the periodic MAC re-authentication feature.

Examples

Display MAC authentication information.

```
<Sysname> display mac-authentication
MAC address authentication is enabled.
 User name format is fixed account
 Fixed username: aaa
 Fixed password: ******
          Offline detect period is 300s
          Quiet period is 60s
          Server response timeout value is 100s
          Reauthentication period is 3600s
          Guest vlan reauthentication timeout value is 30s
```

```
          The max allowed user number is 1024 per slot
          Current user number amounts to 0
          Current domain is bbb

Silent MAC User info:
          MAC Addr         From Port                     Port Index

GigabitEthernet1/0/1 is link-up
  MAC address authentication is disabled
  Periodic reauthentication is enabled
          Reauthentication period is not configured
  Authenticate success: 0, failed: 0
  Max number of on-line users is 0
  Current online user number is 0
          MAC Addr         Authenticate State            Auth Index
GigabitEthernet1/0/2 is link-down
  MAC address authentication is disabled
  Periodic reauthentication is disabled
  Authenticate success: 0, failed: 0
  Max number of on-line users is 0
  Current online user number is 0
          MAC Addr         Authenticate State            Auth Index
```

Table 1 Command output

Field	Description
Periodic reauthentication is enabled/disabled	Status of the MAC re-authentication feature on a port.
Reauthentication period	MAC re-authentication interval.

A5500EI-CMW520-R2221P22

This release has the following changes:

- New feature: Enabling sending of ICMPv6 redirect messages
- Modified feature: Disabling advertising prefix information in RA messages

New feature: Enabling sending of ICMPv6 redirect messages

Enabling sending of ICMPv6 redirect messages

When a device receives a large number of attack packets that require the device to send ICMPv6 redirect packets, the device's performance is degraded for processing these packets. To protect the device from such attacks, you can use the undo form of the following command to disable sending of ICMPV6 redirect packets.

To enable sending of ICMPv6 redirect messages:

Step	Command	Remarks
1. Enter system view	**system-view**	N/A
2. Enable sending of ICMPv6 redirect messages	**ipv6 redirects enable**	Optional. By default, this function is disabled.

Command reference

New command: ipv6 redirects enable

Use **ipv6 redirects enable** to enable sending of ICMPv6 redirect packets.

Use **undo ipv6 redirects** to disable sending of ICMPv6 redirect packets.

Syntax

ipv6 redirects enable

undo ipv6 redirects

Default

Sending of ICMPv6 redirect packets is disabled.

Views

System view

Default command level

System level

Examples

Enable sending of ICMPv6 redirect packets.

```
<Sysname> system-view
[Sysname] ipv6 redirects enable
```

Modified feature: Disabling advertising prefix information in RA messages

Feature change description

The **no-advertise** keyword was added to disable the device from advertising the prefix specified in the **ipv6 nd ra prefix** command.

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**] *

undo ipv6 nd ra prefix { *ipv6-prefix* **|** *ipv6-prefix***/***prefix-length* }

New syntax

ipv6 nd ra prefix { *ipv6-prefix prefix-length* **|** *ipv6-prefix***/***prefix-length* } { *valid-lifetime preferred-lifetime* [**no-autoconfig** | **off-link**] * **|** **no-advertise** }

undo ipv6 nd ra prefix { *ipv6-prefix* **|** *ipv6-prefix***/***prefix-length* }

Views

Interface view

Change description

Before modification: The device advertises the prefix specified in the **ipv6 nd ra prefix** command.

After modification: If the **no-advertise** keyword is specified, the device does not advertise the prefix specified in this command.

A5500EI-CMW520-R2221P20

This release has the following changes:

- New feature: MAC authentication voice VLAN
- Modified feature: Random number generator standards
- Modified feature: Enhanced CC authentication feature

New feature: MAC authentication voice VLAN

Configuring a MAC authentication voice VLAN

You can configure a MAC authentication voice VLAN on a MAC authentication-enabled port that connects to voice terminals. The MAC authentication voice VLAN feature applies only to voice terminals that support VLAN-tagged packets.

The MAC authentication voice VLAN feature works with a remote authentication server. The device uses the following process to implement this feature:

1. Identifies a terminal as a voice device from the packet sent by the authentication server when the terminal passes MAC authentication. The authentication server identifies the terminal as a voice device by its OUI information, and then sends the terminal type information to the device.
2. Assigns the port to the configured voice VLAN as a tagged member and sends the voice VLAN information through an LLDP or CDP packet to the terminal.

Configuration prerequisites

Before you configure this feature, complete the following tasks:

- Enable MAC authentication on the port.
- Set the port type to hybrid or trunk, because the port is assigned to the MAC authentication voice VLAN as a tagged member. For information about port types, see VLAN in *Layer 2—LAN Switching Configuration Guide*.
- Configure LLDP or CDP compatibility on the device. For information about the LLDP and CDP compatibility features, see LLDP in *Layer 2—LAN Switching Configuration Guide*.

Configuration guidelines

When you configure a MAC authentication voice VLAN, follow these restrictions and guidelines:

- You can configure only one MAC authentication voice VLAN on a port. The MAC authentication voice VLANs on different ports can be different.
- A server-assigned authorization VLAN for a voice terminal takes precedence over the MAC authentication voice VLAN. The port will be assigned to the authorization VLAN if both VLANs coexist. For information about MAC authentication VLAN assignment, see MAC authentication in *Security Configuration Guide*.
- The MAC authentication voice VLAN feature cannot work with the RADIUS server provided by IMC.

Configuration procedure

To configure a MAC authentication voice VLAN on a port:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure a MAC authentication voice VLAN on the port.	**mac-authentication voice vlan** *vlan-id*	By default, no MAC authentication voice VLAN exists on a port.

Example of Configuring 802.1X or MAC authentication for IP phones

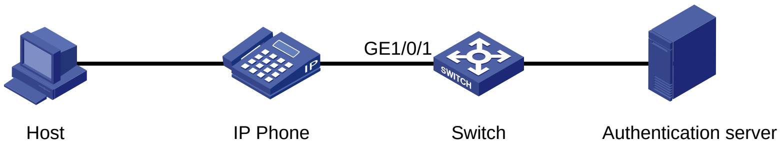
Network requirements

As shown in Figure 1:

- Configure the switch to perform 802.1X and MAC authentication for the host and the IP phone.
- Configure the authentication server to assign authorization VLAN 100 to the host without tags and authorization VLAN 2 to the IP phone with tags, respectively.

After the host passes authentication, data packets from the host will be forwarded within VLAN 100 without tags. After the IP phone passes authentication, voice packets from the IP phone will be forwarded within VLAN 2 with tags.

Figure 1 Network diagram



Requirements analysis

To meet the network requirements, complete the following tasks:

- For users to use 802.1X and MAC authentication flexibly, enable port security on the switch, and set the port security mode to **macAddressOrUserLoginSecureExt**.
- For voice packets to pass through GigabitEthernet 1/0/1 with tags and data packets to pass through GigabitEthernet 1/0/1 without tags, configure the port as a hybrid port.
- To ensure a correct exchange of 802.1X EAPOL packets, configure the switch to send 802.1X EAPOL packets without tags on the port that connects to the IP phone.
- For the switch to notify the IP phone of the specified voice VLAN information through LLDP or CDP packets, configure LLDP or CDP compatibility on the device.

Configuration restrictions and guidelines

When you configure 802.1X and MAC authentication for the IP phone, follow these restrictions and guidelines:

- An authentication server such as ACS is required for this configuration example. The authentication server cannot be the RADIUS server provided by IMC.
- If the IP phone can automatically record voice VLANs, you must use the **port hybrid vlan** *vlan-id* **tagged** command on GigabitEthernet 1/0/1. As a result, the port will be assigned to the specified voice VLANs that are automatically recorded by the IP phone and can send the tagged packets of these voice VLANs.

- By default, the switch encapsulates LLDP packets in Ethernet II format. To ensure correct communication with the IP phone, make sure the switch encapsulates LLDP packets on the IP phone-connected port in the same encapsulation format with the IP phone. For example, if a Cisco IP phone uses SNAP format, you must set the encapsulation format for LLDP packets to SNAP by using the **lldp encapsulation snap** command.

Configuration procedure

1. Assign IP addresses to the host, the IP phone, the switch, and the authentication server. Make sure they can reach one another. (Details not shown.)
2. Perform the following tasks on the authentication server:
   - Configure the authentication server and add user accounts for 802.1X users and MAC authentication users. (Details not shown.)
   - Configure the server to support the **device-traffic-class=voice** attribute. (Details not shown.)
   - Configure the server to assign authorization VLAN 100 to the host without tags and authorization VLAN 2 to the IP phone with tags, respectively. (Details not shown.)

   Authentication server configuration varies by server type. For more information, see related server configuration guideline.
3. Configure VLAN settings on the switch:

   # Create VLAN 2 and VLAN 100.
   ```
   <Switch> system-view
   [Switch] vlan 2
   [Switch-vlan2] quit
   [Switch] vlan 100
   [Switch-vlan100] quit
   ```
   # Disable the voice VLAN security mode.
   ```
   [Switch] undo voice vlan security enable
   ```
   # Configure GigabitEthernet 1/0/1 as a hybrid port.
   ```
   [Switch] interface gigabitethernet 1/0/1
   [Switch-GigabitEthernet1/0/1] port link-type hybrid
   ```
   # Assign GigabitEthernet 1/0/1 to VLAN 2 as a tagged member and to VLAN 100 and VLAN 1 as an untagged member.
   ```
   [Switch-GigabitEthernet1/0/1] port hybrid vlan 2 tagged
   [Switch-GigabitEthernet1/0/1] port hybrid vlan 100 untagged
   [Switch-GigabitEthernet1/0/1] port hybrid vlan 1 untagged
   [Switch-GigabitEthernet1/0/1] quit
   ```
4. Configure an authentication scheme and domain on the switch:

   # Create a RADIUS scheme named **radius1** and enter its view.
   ```
   [Switch] radius scheme radius1
   ```
   # Specify the IP addresses of the primary authentication and accounting servers.
   ```
   [Switch-radius-radius1] primary authentication 10.1.1.1
   [Switch-radius-radius1] primary accounting 10.1.1.1
   ```
   # Specify the shared key between the switch and the authentication server.
   ```
   [Switch-radius-radius1] key authentication key
   ```
   # Specify the shared key between the switch and the accounting server.
   ```
   [Switch-radius-radius1] key accounting key
   ```
   # Exclude the ISP domain names from the usernames sent to the RADIUS servers.
   ```
   [Switch-radius-radius1] user-name-format without-domain
   ```

```
[Switch-radius-radius1] quit
```

Create an ISP domain named **acs**, and apply the RADIUS scheme **radius1** to the ISP domain for authentication, authorization, and accounting.

```
[Switch] domain acs
[Switch-isp-acs] authentication lan-access radius-scheme radius1
[Switch-isp-acs] authorization lan-access radius-scheme radius1
[Switch-isp-acs] accounting lan-access radius-scheme radius1
```

Enable the accounting optional feature for users in the domain **acs**.

```
[Switch-isp-acs] accounting optional
[Switch-isp-acs] quit
```

5. Configure authentication globally on the switch:

   # Enable port security.

```
[Switch] port-security enable
```

   # Specify the domain **acs** as the authentication domain for MAC authentication.

```
[Switch] mac-authentication domain acs
```

   # Configure MAC authentication to use MAC-based accounts. Each MAC address is in the hexadecimal notation with hyphens, and letters are in lower case.

```
[Switch] mac-authentication user-name-format mac-address with-hyphen lowercase
```

6. Configure authentication on GigabitEthernet 1/0/1 of the switch:

   # Set the port security mode to macAddressOrUserLoginSecureExt.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port-security port-mode userlogin-secure-or-mac-ext
```

   # Specify the domain **acs** as the mandatory 802.1X authentication domain.

```
[Switch-GigabitEthernet1/0/1] dot1x mandatory-domain acs
```

   # Disable 802.1X online user handshake.

```
[Switch-GigabitEthernet1/0/1] undo dot1x handshake
```

   # Disable the 802.1X multicast trigger feature, and enable the 802.1X unicast trigger feature.

```
[Switch-GigabitEthernet1/0/1] undo dot1x multicast-trigger
[Switch-GigabitEthernet1/0/1] dot1x unicast-trigger
```

   # Send 802.1X EAPOL packets without tags.

```
[Switch-GigabitEthernet1/0/1] dot1x eapol untag
```

   # Configure VLAN 2 as the 802.1X voice VLAN.

```
[Switch-GigabitEthernet1/0/1] dot1x voice vlan 2
```

   # Configure VLAN 2 as the MAC authentication voice VLAN.

```
[Switch-GigabitEthernet1/0/1] mac-authentication voice vlan 2
[Switch-GigabitEthernet1/0/1] quit
```

7. Configure LLDP:

   # Enable LLDP globally.

```
[Switch] lldp enable
```

   # Enable global CDP compatibility.

```
[Switch] lldp compliance cdp
```

   # Configure CDP-compatible LLDP to operate in TxRx mode on GigabitEthernet 1/0/1.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] lldp compliance admin-status cdp txrx
[Switch-GigabitEthernet1/0/1] quit
```

Command reference

mac-authentication voice vlan

Use **mac-authentication voice vlan** to configure a MAC authentication voice VLAN on a port.

Use **undo mac-authentication voice vlan** to restore the default.

Syntax

mac-authentication voice vlan *vlan-id*

undo mac-authentication voice vlan

Default

No MAC authentication voice VLAN exists on a port.

Views

Ethernet interface view

Default command level

2: System level

Parameters

vlan-id: Specifies a voice VLAN by its ID in the range of 1 to 4094. The VLAN must have been created.

Examples

Configure VLAN 20 as the MAC authentication voice VLAN on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication voice vlan 20
```

Modified feature: Random number generator standards

Feature change description

The standards for random number generator were changed to CTR_DRBG.

Command changes

None.

Modified feature: Enhanced CC authentication feature

Feature change description

The enhanced CC authentication feature enhances the cryptographic algorithms for IPsec, public key cryptography, SSH and SSL. It changes the method for configuring the IKE pre-shared key in FIPS mode, and causes command changes for IPsec, public key cryptography, SSH and SSL.

Command changes

New command: display public-key local ecdsa public

Use **display public-key local ecdsa public** to display the local ECDSA host public key.

Syntax

display public-key local ecdsa public [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

ecdsa: Displays the local ECDSA host public key.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Examples

Display the local ECDSA host public key.

```
<Sysname> display public-key local ecdsa public

=====================================================
Time of Key pair created: 15:01:54  2000/04/26
Key name: HOST_KEY
Key type: ECDSA Encryption Key
=====================================================
Key code:
3059301306072A8648CE3D020106082A8648CE3D03010703420004E963345D5122FC1BE4A7D22B9F
9906FBD19FBD274654CA84727710773176A88AD3960C7E7B17BA2C4F539EA146B20BFB2BA7951A90
55332819D34510A45D550E
```

Table 1 Command output

Field	Description
Time of Key pair created	Date and time when the local ECDSA key pair was created.
Key name	Name of the key.
Key type	Type of the key. **ECDSA Encryption Key** indicates the ECDSA key pair.
Key code	Public key data.

New command: public-key local export ecdsa

Use **public-key local export ecdsa** to display the local ECDSA host public key in a specific format, or export the key in a specific format to a file.

Syntax

public-key local export ecdsa { **openssh** | **ssh2** } [*filename*]

Views

System view

Default command level

2: System level

Parameters

openssh: Uses the format of OpenSSH.

ssh2: Uses the format of SSH2.0.

filename: Specifies the name of the file for saving the ECDSA host public key. For more information about file names, see *Fundamentals Configuration Guide.*

Usage guidelines

If you do not specify the *filename* argument, this command displays the ECDSA host public key in the specified format but does not save the key to a file.

SSH2.0 and OpenSSH are different public key formats. Choose the correct format that is supported by the device where you import the host public key.

You can export the ECDSA host public key to a file only when the key was created by using the secp256r1 curve.

Examples

Export the ECDSA host public key in OpenSSH format to the file named **key.pub**.

```
<Sysname> system-view
[Sysname] public-key local export ecdsa openssh key.pub
```

Modified command: authentication-algorithm

Old syntax

authentication-algorithm sha

New syntax

authentication-algorithm { **sha** | **sha256** }

Views

IKE proposal view

Change description

In FIPS mode, the **sha256** keyword was added to specify the HMAC-SHA256 authentication algorithm, and the default authentication algorithm was changed to HMAC-SHA256.

Modified command: ciphersuite

Old syntax

In FIPS mode:

ciphersuite { **dhe_rsa_aes_128_cbc_sha | dhe_rsa_aes_256_cbc_sha | rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha** } *

New syntax

In FIPS mode:

ciphersuite { **rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha** } *

Views

SSL server policy view

Change description

In FIPS mode, the **dhe_rsa_aes_128_cbc_sha** and **dhe_rsa_aes_256_cbc_sha** keywords were deleted.

Modified command: dh

Old syntax

dh { **group2 | group5 | group14** }

New syntax

dh group14

Views

IKE proposal view

Change description

In FIPS mode, the DH group for phase 1 IKE negotiation can only be the 2048-bit Diffie-Hellman group, and the default DH group was changed to the 2048-bit Diffie-Hellman group.

Modified command: pfs

Old syntax

pfs { **dh-group1 | dh-group2 | dh-group5 | dh-group14** }

New syntax

pfs dh-group14

Views

IPsec policy view

Change description

In FIPS mode, PFS can only use the 2048-bit Diffie-Hellman group.

Modified command: prefer-cipher

Old syntax

In FIPS mode:

prefer-cipher { **dhe_rsa_aes_128_cbc_sha | dhe_rsa_aes_256_cbc_sha | rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha** }

New syntax

In FIPS mode:

prefer-cipher { **rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha** }

Views

SSL client policy view

Change description

In FIPS mode, the **dhe_rsa_aes_128_cbc_sha** and **dhe_rsa_aes_256_cbc_sha** keywords were deleted.

Modified command: pre-shared-key

Old syntax

pre-shared-key [**cipher | simple**] *key*

New syntax

pre-shared-key [**cipher** *key*]

Views

IKE peer view

Change description

In FIPS mode, if you do not specify any parameter, you specify a plaintext pre-shared key in interactive mode. The pre-shared key must be a case-sensitive string of 8 to 201 characters composed of digits, uppercase and lowercase letters, and special characters.

Modified command: public-key local create

Old syntax

public-key local create { **dsa | rsa** }

New syntax

In non-FIPS mode:

public-key local create { **dsa| ecdsa** { **secp192r1 | secp256r1** } **| rsa** }

In FIPS mode:

public-key local create { **dsa| ecdsa secp256r1** } **| rsa** }

Views

System view

Change description

Before modification:

- When creating a DSA key pair in FIPS mode, you can set the key modulus length to a value between 1024 and 2048 bits.
- The command does not support creating ECDSA key pairs.

After modification:

- When you create a DSA key pair in FIPS mode, the key modules length defaults to 2048 bits and cannot be changed.
- The following options were added to the command:
    - **ecdsa secp192r1**: Creates a 192-bit ECDSA key pair by using the secp192r1 curve. This option is supported only in non-FIPS mode.
    - **ecdsa secp256r1**: Creates a 256-bit ECDSA key pair by using the secp256r1 curve.

Modified command: scp

Old syntax

In non-FIPS mode:

scp [**ipv6**] *server* [*port-number*] { **get | put** } *source-file-path* [*destination-file-path*] [**identity-key** { **dsa | rsa** } **| prefer-ctos-cipher** { **3des | aes128 | des** } **| prefer-ctos-hmac** { **md5 | md5-96 | sha1 | sha1-96** } **| prefer-kex** { **dh-group-exchange | dh-group1 | dh-group14** } **| prefer-stoc-cipher** { **3des | aes128 | des** } **| prefer-stoc-hmac** { **md5 | md5-96 | sha1 | sha1-96** } **| username** *username* **password** *password*] *

In FIPS mode:

scp [**ipv6**] *server* [*port-number*] { **get | put** } *source-file-path* [*destination-file-path*] [**identity-key rsa | prefer-ctos-cipher** { **aes128 | aes256** } **| prefer-ctos-hmac** { **sha1 | sha1-96** } **| prefer-kex dh-group14 | prefer-stoc-cipher** { **aes128 | aes256** } **| prefer-stoc-hmac** { **sha1 | sha1-96** } **| username** *username* **password** *password*] *

New syntax

In non-FIPS mode:

scp [**ipv6**] *server* [*port-number*] { **get | put** } *source-file-path* [*destination-file-path*] [**identity-key** { **dsa | ecdsa | rsa** } **| prefer-ctos-cipher** { **3des | aes128 | des** } **| prefer-ctos-hmac** { **md5 | md5-96 | sha1 | sha1-96** } **| prefer-kex** { **dh-group-exchange | dh-group1 | dh-group14** } **| prefer-stoc-cipher** { **3des | aes128 | des** } **| prefer-stoc-hmac** { **md5 | md5-96 | sha1 | sha1-96** } **| username** *username* **password** *password*] *

In FIPS mode:

scp [**ipv6**] *server* [*port-number*] { **get | put** } *source-file-path* [*destination-file-path*] [**identity-key** { **ecdsa | rsa** } **| prefer-ctos-cipher** { **aes128 | aes256** } **| prefer-ctos-hmac** { **sha1 | sha1-96** } **| prefer-kex dh-group14 | prefer-stoc-cipher** { **aes128 | aes256** } **| prefer-stoc-hmac** { **sha1 | sha1-96** } **| username** *username* **password** *password*] *

Views

User view

Change description

The keywords **identity-key ecdsa** were added.

Modified command: sftp

Old syntax

In non-FIPS mode:

sftp [**ipv6**] *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa | rsa** } **| prefer-ctos-cipher** { **3des | aes128 | des** } **| prefer-ctos-hmac** { **md5 | md5-96 | sha1 | sha1-96** } **| prefer-kex** { **dh-group-exchange | dh-group1 | dh-group14** } **| prefer-stoc-cipher** { **3des | aes128 | des** } **| prefer-stoc-hmac** { **md5 | md5-96 | sha1 | sha1-96** }] *

In FIPS mode:

sftp [**ipv6**] *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key rsa | prefer-ctos-cipher** { **aes128 | aes256** } **| prefer-ctos-hmac** { **sha1 | sha1-96** } **| prefer-kex dh-group14 | prefer-stoc-cipher** { **aes128 | aes256** } **| prefer-stoc-hmac** { **sha1 | sha1-96** }] *

New syntax

In non-FIPS mode:

sftp [**ipv6**] *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa | ecdsa | rsa** } **| prefer-ctos-cipher** { **3des | aes128 | des** } **| prefer-ctos-hmac** { **md5 | md5-96 | sha1 |**

sha1-96 } **| prefer-kex** { **dh-group-exchange | dh-group1 | dh-group14** } **| prefer-stoc-cipher** { **3des | aes128 | des** } **| prefer-stoc-hmac** { **md5 | md5-96 | sha1 | sha1-96** }] *

In FIPS mode:

sftp [**ipv6**] *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **ecdsa | rsa** } **| prefer-ctos-cipher** { **aes128 | aes256** } **| prefer-ctos-hmac** { **sha1 | sha1-96** } **| prefer-kex dh-group14 | prefer-stoc-cipher** { **aes128 | aes256** } **| prefer-stoc-hmac** { **sha1 | sha1-96** }] *

Views

User view

Change description

The keywords **identity-key ecdsa** were added.

Modified command: ssh2

Old syntax

In non-FIPS mode:

ssh2 [**ipv6** *server*] [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa | rsa** } **| prefer-ctos-cipher** { **3des | aes128 | des** } **| prefer-ctos-hmac** { **md5 | md5-96 | sha1 | sha1-96** } **| prefer-kex** { **dh-group-exchange | dh-group1 | dh-group14** } **| prefer-stoc-cipher** { **3des | aes128 | des** } **| prefer-stoc-hmac** { **md5 | md5-96 | sha1 | sha1-96** }] *

In FIPS mode:

ssh2 [**ipv6**] *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key rsa | prefer-ctos-cipher** { **aes128 | aes256** } **| prefer-ctos-hmac** { **sha1 | sha1-96** } **| prefer-kex dh-group14 | prefer-stoc-cipher** { **aes128 | aes256** } **| prefer-stoc-hmac** { **sha1 | sha1-96** }] *

New syntax

In non-FIPS mode:

ssh2 [**ipv6** *server*] [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa | ecdsa | rsa** } **| prefer-ctos-cipher** { **3des | aes128 | des** } **| prefer-ctos-hmac** { **md5 | md5-96 | sha1 | sha1-96** } **| prefer-kex** { **dh-group-exchange | dh-group1 | dh-group14** } **| prefer-stoc-cipher** { **3des | aes128 | des** } **| prefer-stoc-hmac** { **md5 | md5-96 | sha1 | sha1-96** }] *

In FIPS mode:

ssh2 [**ipv6** *server*] [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **ecdsa | rsa** } **| prefer-ctos-cipher** { **aes128 | aes256** } **| prefer-ctos-hmac** { **sha1 | sha1-96** } **| prefer-kex dh-group14 | prefer-stoc-cipher** { **aes128 | aes256** } **| prefer-stoc-hmac** { **sha1 | sha1-96** }] *

Views

User view

Change description

The keywords **identity-key ecdsa** were added.

A5500EI-CMW520-R2221P19

This release has no feature changes.

A5500EI-CMW520-R2221P18

This release has the following changes:

- New feature: Sending EAP-Success packets to 802.1X users in critical VLAN
- Modified feature: VPN instance support for NQA server configuration

New feature: Sending EAP-Success packets to 802.1X users in critical VLAN

Configuring the device to send EAP-Success packets to 802.1X users in critical VLAN

This feature allows specific 802.1X users in the critical VLAN to pass re-authentication directly when the device detects a reachable server. The device sends EAP-Success packets to the 802.1X clients that cannot respond to the EAP-Request packets of the device (for example, the Windows built-in 802.1X client).

The feature takes effect only after the **dot1x critical recovery-action reinitialize** command is configured on the port.

To configure the device to send EAP-Success packets to users in the 802.1X critical VLAN:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the 802.1X critical VLAN on the port.	**dot1x critical vlan** *vlan-id*	Required. By default, no 802.1X critical VLAN is configured. Different ports can be configured with different critical VLANs, and one port can only be configured with a maximum of one critical VLAN.
4. Configure the port to trigger 802.1X re-authentication on detection of an active authentication server for users in the critical VLAN.	**dot1x critical recovery-action reinitialize**	Required. By default, when a reachable server is detected, the system removes the port or 802.1X users from the critical VLAN without triggering authentication.
5. Configure the device to send EAP-Success packets to 802.1X users in the critical VLAN on the port.	**dot1X critical eapol**	Required. By default, the device does not send EAP-Success packets to 802.1X users in the critical VLAN.

Command reference

dot1x critical eapol

Use **dot1x critical eapol** to configure the device to send EAP-Success packets to 802.1X users in the critical VLAN.

Use **undo dot1x critical eapol** to restore the default.

Syntax

dot1x critical eapol

undo dot1x critical eapol

Default

The device does not send EAP-Success packets to 802.1X users in the critical VLAN.

Views

Layer 2 Ethernet interface view

Default command level

2: System level

Examples

Configure GigabitEthernet 1/0/1 to send EAP-Success packets to 802.1X users in the critical VLAN.

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x critical eapol
```

Modified feature: VPN instance support for NQA server configuration

Feature change description

The **vpn-instance** keyword was added to the **nqa server** command. You can use the keyword to enable the NQA server to listen on an IP address in a VPN instance.

Command changes

Modified command: nqa server

Old syntax

nqa server { **tcp-connect** | **udp-echo** } *ip-address port-number*

New syntax

nqa server { **tcp-connect** | **udp-echo** } *ip-address port-number* [**vpn-instance** *vpn-instance-name*]

Views

System view

Change description

The **vpn-instance** keyword was added. You can use the keyword to enable the NQA server to listen on an IP address in a VPN instance.

A5500EI-CMW520-R2221P15

This release has no feature changes.

A5500EI-CMW520-R2221P12

This release has the following changes:

- New feature: Login delay
- Modified feature: IPv6 address with a 127-bit prefix length

New feature: Login delay

Enabling the login delay

The login delay feature delays the device to accept a login request from a user after the user fails a login attempt. This feature can slow down login dictionary attacks.

To enable the login delay:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable the login delay feature.	**attack-defense login reauthentication-delay** *seconds*	By default, the login delay feature is disabled.

Command reference

attack-defense login reauthentication-delay

Syntax

attack-defense login reauthentication-delay *seconds*

undo attack-defense login reauthentication-delay

Views

System view

Default command level

2: System level

Parameters

seconds: Sets the delay period in seconds, in the range of 4 to 60.

Description

Use **attack-defense login reauthentication-delay** to enable the login delay feature.

Use **undo attack-defense login reauthentication-delay** to restore the default.

By default, the login delay feature is disabled. The device does not delay accepting a login request from a user who has failed a login attempt.

Examples

Enable the login delay feature and set the delay period to 5 seconds.

```
<Sysname> system-view
[Sysname] attack-defense login reauthentication-delay 5
```

Modified feature: IPv6 address with a 127-bit prefix length

Feature change description

Before modification, you cannot execute the **ipv6 address** command to configure an IPv6 global unicast address in the form of *XXX*::**2/127**. The system identifies IPv6 address in this form as an anycast address.

After modification:

- You can use the **ipv6 address** command to configure an IPv6 global unicast address in the form of *XXX*::**2/127**.
- The system does not support any IPv6 anycast address with the 127-bit prefix length.

Command changes

None.

A5500EI-CMW520-R2221P10

This release has the following changes:

- New feature: Support for NTP configuration in IPv6 networks

New feature: Support for NTP configuration in IPv6 networks

Configuring NTP in IPv6 networks

You can configure NTP in IPv6 networks.

Command reference

New command: display ntp-service ipv6 sessions

Syntax

display ntp-service ipv6 sessions [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

verbose: Displays detailed information about all IPv6 NTP sessions. If you do not specify this keyword, the command only displays brief information about the IPv6 NTP sessions.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ntp-service ipv6 sessions** to display information about all IPv6 NTP sessions.

Examples

Display brief information about all IPv6 NTP sessions.

```
<Sysname> display ntp-service ipv6 sessions
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.

 Source:   [125]3000::32
 Reference: 127.127.1.0           Clock stratum: 2
 Reachabilities: 1                Poll interval: 64
 Last receive time: 6             Offset: -0.0
```

```
Roundtrip delay: 0.0           Dispersion: 0.0

Total sessions: 1
```

Table 2 Command output

Field	Description
[12345]	• **1**—Clock source selected by the system (the current reference source). It has a system clock stratum level less than or equal to 15. • **2**—The stratum level of the clock source is less than or equal to 15. • **3**—The clock source has survived the clock selection algorithm. • **4**—The clock source is a candidate clock source. • **5**—The clock source was created by a command.
Source	IPv6 address of the NTP server. If this field displays **::**, the IPv6 address of the NTP server has not been resolved successfully.

Reference	Reference clock ID of the NTP server:
	• If the reference clock is the local clock, the value of this field is related to the value of the Clock stratum field:
	  ○ When the value of the Clock stratum field is 0 or 1, this field displays **Local**.
	  ○ When the Clock stratum field has another value, this field displays the MD5 digest value of the first 32 bits of the IPv6 address. The MD5 digest value is in dotted decimal format.
	• If the reference clock is the clock of another device on the network, this field displays the MD5 digest value of the first 32 bits of the IPv6 address. The MD5 digest value is in dotted decimal format. If this field displays **INIT**, the local device has not established a connection with the NTP server.

Clock stratum	Stratum level of the NTP server, which determines the clock accuracy. The value is in the range of 1 to 16. A lower stratum level represents higher clock accuracy. A stratum 16 clock is not synchronized and cannot be used as a reference clock.
Reachabilities	Reachability count of the NTP server. 0 indicates that the NTP server is unreachable.
Poll interval	Polling interval in seconds. It is the maximum interval between successive NTP messages.
Last receive time	Length of time from when the last NTP message was received or when the local clock was last updated to the current time. Time is in seconds by default. • If the time length is greater than 2048 seconds, it is displayed in minutes. • If the time length is greater than 300 minutes, it is displayed in hours. • If the time length is greater than 96 hours, it is displayed in days. • If the time length is greater than 999 days, it is displayed in years. If the time when the most recent NTP message was received or when the local clock was updated most recently is behind the current time, a hyphen (-) is displayed.
Offset	Offset of the system clock relative to the reference clock, in milliseconds.
Roundtrip delay	Roundtrip delay from the local device to the clock source, in milliseconds.
Dispersion	Maximum error of the system clock relative to the reference source.
Total sessions	Total number of associations.

New command: ntp-service ipv6 access

Syntax

ntp-service ipv6 access { **peer** | **query** | **server** | **synchronization** } *acl-number*

undo ntp-service ipv6 access { **peer** | **query** | **server** | **synchronization** }

View

System view

Default level

3: Manage level

Parameters

peer: Permits full access. This level of right permits the peer devices to perform synchronization and control query to the local device and also permits the local device to synchronize its clock to that of a peer device. Control query refers to query of NTP status information, such as alarm information, authentication status, and clock source information.

query: Permits control query. This level of right permits the peer devices to perform control query to the NTP service on the local device but does not permit a peer device to synchronize its clock to that of the local device.

server: Permits server access and query. This level of right permits the peer devices to perform synchronization and control query to the local device but does not permit the local device to synchronize its clock to that of a peer device.

synchronization: Permits server access only. This level of right permits a peer device to synchronize its clock to that of the local device but does not permit the peer devices to perform control query.

acl-number: Specifies a basic ACL number in the range of 2000 to 2999.

Description

Use **ntp-service ipv6 access** to configure the access-control right for the peer devices to access the IPv6 NTP services of the local device.

Use **undo ntp-service ipv6 access** to remove the configured IPv6 NTP service access-control right to the local device.

By default, the access-control right for the peer devices to access the IPv6 NTP services of the local device is set to **peer**.

From the highest NTP service access-control right to the lowest one are **peer**, **server**, **synchronization**, and **query**. When a device receives an NTP request, it matches against the access-control right in this order and uses the first matched right. If no matched right is found, the device drops the NTP request.

The **ntp-service ipv6 access** command provides only a minimum degree of security protection. A more secure method is identity authentication. The related command is **ntp-service authentication enable**.

Before specifying an ACL number in the **ntp-service ipv6 access** command, make sure you have already created and configured this ACL.

Examples

Configure the peer devices on subnet 2001::1 to have full access to the local device.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2001
[Sysname-acl6-basic-2001] rule permit source 2001::1 64
[Sysname-acl6-basic-2001] quit
[Sysname] ntp-service ipv6 peer acl 2001
```

New command: ntp-service ipv6 dscp

Syntax

ntp-service ipv6 dscp *dscp-value*

undo ntp-service ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies the Differentiated Services Code Point (DSCP) value for IPv6 NTP messages, in the range of 0 to 63.

Description

Use the **ntp-service ipv6 dscp** command to set the DSCP value for IPv6 NTP messages.

Use the **undo ntp-service ipv6 dscp** command to restore the default.

By default, the DSCP value for IPv6 NTP messages is 56.

Examples

Set the DSCP value to 30 for IPv6 NTP messages.

```
<Sysname> system-view
[Sysname] ntp-service ipv6 dscp 30
```

New command: ntp-service ipv6 in-interface disable

Syntax

ntp-service ipv6 in-interface disable

undo ntp-service ipv6 in-interface disable

View

VLAN interface view

Default level

3: Manage level

Parameters

None

Description

Use **ntp-service ipv6 in-interface disable** to disable an interface from receiving IPv6 NTP messages.

Use **undo ntp-service ipv6 in-interface disable** to restore the default.

By default, all interfaces are enabled to receive IPv6 NTP messages.

Examples

Disable VLAN-interface 1 from receiving IPv6 NTP messages.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service ipv6 in-interface disable
```

New command: ntp-service ipv6 multicast-client

Syntax

ntp-service ipv6 multicast-client *ipv6-address*

undo ntp-service ipv6 multicast-client *ipv6-address*

View

VLAN interface view

Default level

3: Manage level

Parameters

ipv6-address: Specifies an IPv6 multicast IP address. An IPv6 broadcast client and an IPv6 broadcast server must be configured with the same multicast address.

Description

Use **ntp-service ipv6 multicast-client** to configure the device to operate in IPv6 NTP multicast client mode and use the current interface to receive IPv6 NTP multicast packets.

Use **undo ntp-service ipv6 multicast-client** to remove the configuration.

By default, the device does not operate in any NTP operation mode.

Examples

Configure the device to operate in IPv6 multicast client mode and receive IPv6 NTP multicast messages with the destination FF21::1 on VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service ipv6 multicast-client ff21::1
```

New command: ntp-service ipv6 multicast-server

Syntax

ntp-service ipv6 multicast-server [*ipv6-address*] [**authentication-keyid** *keyid* **|** **ttl** *ttl-number*] *

undo ntp-service ipv6 multicast-server [*ipv6-address*]

View

VLAN interface view

Default level

3: Manage level

Parameters

ipv6-address: Specifies an IPv6 multicast IP address. An IPv6 multicast client and server must be configured with the same multicast address.

authentication-keyid *keyid*: Specifies the key ID to be used for sending multicast messages to multicast clients, where *keyid* is in the range of 1 to 4294967295. This parameter is not meaningful if authentication is not required.

ttl *ttl-number*: Specifies the TTL of NTP multicast messages. The value range for the *ttl-number* argument is 1 to 255, and the default is 16.

Description

Use **ntp-service ipv6 multicast-server** to configure the device to operate in IPv6 NTP multicast server mode and use the current interface to send IPv6 NTP multicast packets.

Use **undo ntp-service ipv6 multicast-server** to remove the configuration.

By default, the device does not operate in any NTP operation mode.

Examples

Configure the device to operate in IPv6 multicast server mode and send IPv6 NTP multicast messages on VLAN-interface 1 to the multicast address FF21::1, using key 4 for encryption.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service ipv6 multicast-server ff21::1 authentication-keyid
4
```

New command: ntp-service ipv6 source-interface

Syntax

ntp-service ipv6 source-interface *interface-type interface-number*

undo ntp-service ipv6 source-interface

View

System view

Default level

3: Manage level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Description

Use **ntp-service ipv6 source-interface** to specify the source interface for IPv6 NTP messages.

Use **undo ntp-service ipv6 source-interface** to restore the default.

By default, no source interface is specified for IPv6 NTP messages, and the system uses the IP address of the interface determined by the matched route as the source IP address of IPv6 NTP messages.

If you do not want the IP address of a certain interface on the local device to become the destination address of response messages, use this command to specify the source interface for IPv6 NTP messages so that the source IP address in IPv6 NTP messages is the primary IP address of this interface.

If the specified source interface goes down, NTP searches the routing table for the outgoing interface, and uses the primary IP address of the outgoing interface as the source IP address.

Examples

Specify the source interface of IPv6 NTP messages as VLAN-interface 1.

```
<Sysname> system-view
[Sysname] ntp-service ipv6 source-interface vlan-interface 1
```

New command: ntp-service ipv6 unicast-peer

Syntax

ntp-service ipv6 unicast-peer [**vpn-instance** *vpn-instance-name*] { *ipv6-address* **|** *peer-name* } [**authentication-keyid** *keyid* **| priority | source-interface** *interface-type interface-number*] *

undo ntp-service ipv6 unicast-peer [**vpn-instance** *vpn-instance-name*] { *ipv6-address* **|** *peer-name* }

View

System view

Default level

3: Manage level

Parameters

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN to which the symmetric-passive peer belongs, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If the symmetric-passive peer is on the public network, do not specify this option.

peer-name: Specifies a host name of the symmetric-passive peer, a string of 1 to 20 characters.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the peer, where *keyid* is in the range of 1 to 4294967295.

priority: Specifies the peer designated by *ip-address* or *peer-name* as the first choice under the same condition.

source-interface *interface-type interface-number*: Specifies the source interface for NTP messages. In an NTP message that the local device sends to its peer, the source IP address is the primary IP address of this interface.

Description

Use **ntp-service ipv6 unicast-peer** to designate an IPv6 symmetric-passive peer for the device.

Use **undo ntp-service ipv6 unicast-peer** to remove the IPv6 symmetric-passive peer designated for the device.

By default, no IPv6 symmetric-passive peer is designated for the device.

Examples

Designate the device with the IPv6 address of 2001::1 as the symmetric-passive peer of the device, configure the device to run IPv6 NTP version 4, and specify the source interface of IPv6 NTP messages as VLAN-interface 1.

```
<Sysname> system-view
[Sysname] ntp-service ipv6 unicast-peer 2001::1 source-interface vlan-interface 1
```

New command: ntp-service ipv6 unicast-server

Syntax

ntp-service ipv6 unicast-server [**vpn-instance** *vpn-instance-name*] { *ipv6-address* **|** *server-name* } [**authentication-keyid** *keyid* **|** **priority** **|** **source-interface** *interface-type interface-number*] *

undo ntp-service ipv6 unicast-server [**vpn-instance** *vpn-instance-name*] { *ipv6-address* **|** *server-name* }

View

System view

Default level

3: Manage level

Parameters

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN to which the NTP server belongs, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If the NTP server is on the public network, do not specify this option.

server-name: Specifies a host name of the NTP server, a string of 1 to 20 characters.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the NTP server, where *keyid* is in the range of 1 to 4294967295.

priority: Specifies this NTP server as the first choice under the same condition.

source-interface *interface-type interface-number*: Specifies the source interface for IPv6 NTP messages. In an IPv6 NTP message that the local device sends to the NTP server, the source IPv6 address is the primary IP address of this interface.

Description

Use **ntp-service ipv6 unicast-server** to designate an IPv6 NTP server for the device.

Use **undo ntp-service ipv6 unicast-server** to remove an IPv6 NTP server designated for the device.

By default, no IPv6 NTP server is designated for the device.

Examples

Designate NTP server 2001::1 for the device, and configure the device to run NTP version 4.

```
<Sysname> system-view
[Sysname] ntp-service ipv6 unicast-server 2001::1 version 4
```

A5500EI-CMW520-R2221P08

This release has the following changes:

- New feature: Applicable scope of packet filtering on a VLAN interface
- New feature: SNMP notifications for PVST topology changes
- New feature: Disabling SSL 3.0

New feature: Applicable scope of packet filtering on a VLAN interface

Configuring the applicable scope of packet filtering on a VLAN interface

You can configure the packet filtering on a VLAN interface to filter the following packets:

- Packets forwarded at Layer 3 by the VLAN interface.
- All packets, including packets forwarded at Layer 3 by the VLAN interface and packets forwarded at Layer 2 by the physical ports associated with the VLAN interface.

To configure the applicable scope of packet filtering on a VLAN interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a VLAN interface and enter its view.	**interface vlan-interface** *vlan-interface-id*	If the VLAN interface already exists, you directly enter its view. By default, no VLAN interface exists.
3. Specify the applicable scope of packet filtering on the VLAN interface.	**packet-filter filter** { **route** | **all** }	By default, the packet filtering filters all packets.

Command reference

packet-filter filter

Use **packet-filter filter** to specify the applicable scope of packet filtering on a VLAN interface.

Use **undo packet-filter filter** to restore the default.

Syntax

packet-filter filter { **route** | **all** }

undo packet-filter filter

Default

The packet filtering filters all packets.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

route: Filters packets forwarded at Layer 3 by the VLAN interface.

all: Filters all packets, including packets forwarded at Layer 3 by the VLAN interface and packets forwarded at Layer 2 by the physical ports associated with the VLAN interface.

Examples

Configure the packet filtering on VLAN-interface 2 to filter packets forwarded at Layer 3.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] packet-filter filter route
```

New feature: SNMP notifications for PVST topology changes

Enabling SNMP notifications for PVST topology changes

This feature enables the device to generate logs and report PVST topology change events to an NMS when the device detects or receives a TC BPDU. For the SNMP notifications to be sent correctly, you must also configure SNMP as described in *Network Management and Monitoring Configuration Guide*.

To enable SNMP notifications for PVST topology changes:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable SNMP notifications for PVST topology changes.	**snmp-agent trap enable stp** [**tc**]	By default, SNMP notifications are disabled for PVST topology changes on all VLANs.

Command reference

snmp trap enable stp

Use **snmp-agent trap enable stp** to enable SNMP notifications for PVST topology changes.

Use **undo snmp-agent trap enable stp** to disable SNMP notifications for PVST topology changes.

Syntax

snmp-agent trap enable stp [**tc**]

undo snmp-agent trap enable stp [**tc**]

Default

SNMP notifications are disabled for PVST topology changes on all VLANs.

Views

System view

Predefined user roles

3: Manage level

Parameters

tc: Specifies SNMP notifications for PVST topology changes.

Usage guidelines

This command configures SNMP notifications only for PVST topology changes whether you specify the tc keyword or not.

Examples

Enable SNMP notifications for PVST topology changes.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable stp tc
```

New feature: Disabling SSL 3.0

Disabling SSL 3.0

This feature allows you to disable SSL 3.0 on a device to enhance system security.

- An SSL server supports only TLS 1.0 after SSL 3.0 is disabled.
- An SSL client always uses SSL 3.0 if SSL 3.0 is specified for the client policy, whether you disable SSL 3.0 or not.

To ensure successful establishment of an SSL connection, do not disable SSL 3.0 on a device when the peer device only supports SSL 3.0. HP recommends upgrading the peer device to support TLS 1.0 to improve security.

To disable SSL 3.0 on a device:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Disable SSL 3.0 on the device.	**ssl version ssl3.0 disable**	By default, the device supports SSL 3.0.

Command reference

ssl version ssl3.0 disable

Syntax

ssl version ssl3.0 disable

undo ssl version ssl3.0 disable

Views

System view

Parameters

None

Description

Use **ssl version ssl3.0 disable** to disable SSL 3.0 on the device. Use **undo ssl version ssl3.0 disable** restore the default.

By default, the device supports SSL 3.0.

Examples

Disable SSL 3.0 on the device.

```
<Sysname> system-view
[Sysname] ssl version ssl3.0 disable
```

A5500EI-CMW520-R2221P07

This release has the following changes:

- New feature: 802.1X MAC address binding
- New feature: Automatic PI reset

New feature: 802.1X MAC address binding

Configuring 802.1X MAC address binding

This feature can automatically bind MAC addresses of authenticated 802.1X users to the users' access port and generate 802.1X MAC address binding entries. You can also use the **dot1x binding-mac** *mac-address* command to manually configure 802.1X MAC address binding entries.

802.1X MAC address binding entries never age out. They can survive a user logoff or a device reboot. To delete an entry, you must use the **undo dot1x binding-mac** *mac-address* command.

After the number of 802.1X MAC address binding entries reaches the upper limit of concurrent 802.1X users, the following restrictions exist:

- Users not in the binding entries will fail authentication even after users in the binding entries go offline.
- New 802.1X MAC address binding entries are not allowed.

When you configure the 802.1X MAC address binding feature on a port, follow these restrictions and guidelines:

- The 802.1X MAC address binding feature takes effect only when the port performs MAC-based access control.
- Manually configured MAC address binding entries take effect only when the 802.1X MAC address binding feature takes effect.
- An 802.1X MAC address binding entry cannot be deleted when the user in the entry is online.

To configure the 802.1X MAC address binding feature on a port:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Enable the 802.1X MAC address binding feature.	**dot1x binding-mac enable**	By default, the feature is disabled.
4. (Optional.) Manually configure 802.1X MAC address binding entries.	**dot1x binding-mac** *mac-address*	By default, no 802.1X MAC address binding entries are configured on the port.

Command reference

dot1x binding-mac enable

Use **dot1x binding-mac enable** to enable the 802.1X MAC address binding feature.

Use **undo dot1x binding-mac enable** to restore the default.

Syntax

dot1x binding-mac enable

undo dot1x binding-mac enable

Default

The 802.1X MAC address binding feature is disabled.

Views

Layer 2 Ethernet interface view

Default command level

2: System level

Usage guidelines

This command takes effect on a port only when the port performs MAC-based access control.

The 802.1X MAC address binding feature automatically binds MAC addresses of authenticated 802.1X users to the users' access port and generates 802.1X MAC address binding entries.

802.1X MAC address binding entries, both automatically generated and manually configured, never age out. They can survive a user logoff or a device reboot. To delete an entry, you must use the **undo dot1x binding-mac** *mac-address* command. An 802.1X MAC address binding entry cannot be deleted when the user in the entry is online.

After the number of 802.1X MAC address binding entries reaches the upper limit of concurrent 802.1X users (set by using the **dot1x max-user** command), the following restrictions exist:

- Users not in the binding entries will fail authentication even after users in the binding entries go offline.
- New 802.1X MAC address binding entries are not allowed.

Examples

Enable 802.1X MAC address binding on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x binding-mac enable
```

dot1x binding-mac

Use **dot1x binding-mac** to configure an 802.1X MAC address binding entry.

Use **undo dot1x binding-mac** to delete an 802.1X MAC address binding entry.

Syntax

dot1x binding-mac *mac-address*

undo dot1x binding-mac *mac-address*

Default

No 802.1X MAC address binding entries are configured on a port.

Views

Layer 2 Ethernet interface view

Default command level

2: System level

Parameters

mac-address: Specifies a MAC address, in the format of H-H-H, excluding broadcast, multicast, and all-zero MAC addresses.

Usage guidelines

This command takes effect only the 802.1X MAC address binding feature takes effect.

802.1X MAC address binding entries, both manually configured and automatically generated, never age out. They can survive a user logoff or a device reboot. To delete an entry, you must use the **undo dot1x binding-mac** *mac-address* command. An 802.1X MAC address binding entry cannot be deleted when the user in the entry is online.

After the number of 802.1X MAC address binding entries reaches the upper limit of concurrent 802.1X users (set by using the **dot1x max-user** command), the following restrictions exist:

- Users not in the binding entries will fail authentication even after users in the binding entries go offline.
- New 802.1X MAC address binding entries are not allowed.

Examples

Configure an 802.1X MAC address binding entry on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x binding-mac 000a-eb29-75f1
```

New feature: Automatic PI reset

Enabling automatic PI reset

This feature enables PIs to reset automatically after you reboot the device by using the **reboot** command. After the reset, the PIs resume data and power supply services.

To enable automatic PI reset:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable automatic PI reset.	**poe reset enable**	By default, automatic PI reset is disabled.

Command reference

poe reset enable

Use **poe reset enable** to enable automatic PI reset.

Use **undo poe reset enable** to disable automatic PI reset.

Syntax

poe reset enable

undo poe reset enable

Default

Automatic PI reset is disabled.

Views

System view

Default command level

2: System level

Examples

Enable automatic PI reset.

```
<Sysname> system-view
[Sysname] poe reset enable
```

A5500EI-CMW520-R2221P06

This release has no feature changes.

A5500EI-CMW520-R2221P05

This release has the following changes:

- New feature: Telnet/SSH user connection control
- New feature: Packet rate-limiting for the table-miss flow entry
- Modified feature: Including time zone information in the timestamp of system information sent to a log host
- Modified feature: Configuring physical state change suppression on an Ethernet interface
- Modified feature: Configuring a tag and description for an IPv6 static route

New feature: Telnet/SSH user connection control

Configuring Telnet/SSH user connection control

This feature allows you to control Telnet/SSH user connections to the device based on the referenced ACL. Only the Telnet/SSH users that the referenced ACL permits can initiate Telnet/SSH connections to the device.

All Telnet/SSH users can initiate Telnet/SSH connections to the device when any one of the following conditions exits:

- You do not specify any ACLs.
- The specified ACL does not exist.
- The specified ACL does not have any rules.

Configuration prerequisites

Before you configure Telnet/SSH user connection control, configure the ACL as required.

Configuration procedure

To configure Telnet user connection control:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure Telnet user connection control.	• Configure IPv4 Telnet user connection control: **telnet server acl** *acl-number* • Configure IPv6 Telnet user connection control: **telnet server ipv6 acl ipv6** *acl-number*	By default, all Telnet users can initiate Telnet connections to the device.

To configure SSH user connection control:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Configure SSH user connection control.	• Configure IPv4 SSH user connection control: **ssh server acl** *acl-number* • Configure IPv6 SSH user connection control: **ssh server ipv6 acl ipv6** *acl-number*	By default, all SSH users can initiate SSH connections to the device.

Command reference

ssh server acl

Use **ssh server acl** to specify an ACL to control IPv4 SSH user connections.

Use **undo ssh server acl** to restore the default.

Syntax

ssh server acl *acl-number*

undo ssh server acl

Default

No ACLs are specified and all IPv4 SSH users can initiate SSH connections to the device.

Views

System view

Default command level

3: Manage level

Parameters

acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999.

Usage guidelines

The specified ACL filters IPv4 SSH users' connection requests. Only the IPv4 SSH users that the ACL permits can initiate SSH connections to the device.

All IPv4 SSH users can initiate SSH connections to the device when any one of the following conditions exists:

- You do not specify any ACLs.
- The specified ACL does not exist.
- The specified ACL does not have any rules.

The ACL takes effect only on SSH connections that are initiated after the ACL configuration.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure ACL 2001 and permit only the users at 1.1.1.1 to initiate SSH connections to the device.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 1.1.1.1 0
[Sysname-acl-basic-2001] quit
[Sysname] ssh server acl 2001
```

ssh server ipv6 acl ipv6

Use **ssh server ipv6 acl ipv6** to specify an ACL to control IPv6 SSH user connections.

Use **undo ssh server ipv6 acl** to restore the default.

Syntax

ssh server ipv6 acl ipv6 *acl-number*

undo ssh server ipv6 acl

Default

No ACLs are specified and all IPv6 SSH users can initiate SSH connections to the device.

Views

System view

Default command level

3: Manage level

Parameters

acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999.

Usage guidelines

The specified ACL filters IPv6 SSH users' connection requests. Only the IPv6 SSH users that the ACL permits can initiate SSH connections to the device.

All IPv6 SSH users can initiate SSH connections to the device when any one of the following conditions exists:

- You do not specify any ACLs.
- The specified ACL does not exist.
- The specified ACL does not have any rules.

The ACL takes effect only on SSH connections that are initiated after the ACL configuration.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure ACL 2001 and permit only the users on the subnet 1::1/64 to initiate SSH connections to the device.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2001
[Sysname-acl6-basic-2001] rule permit source 1::1 64
[Sysname-acl6-basic-2001] quit
[Sysname] ssh server ipv6 acl ipv6 2001
```

telnet server acl

Use **telnet server acl** to specify an ACL to control IPv4 Telnet user connections.

Use **undo telnet server acl** to restore the default.

Syntax

telnet server acl *acl-number*

undo telnet server acl

Default

No ACLs are specified and all IPv4 Telnet users can initiate Telnet connections to the device.

Views

System view

Default command level

3: Manage level

Parameters

acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999.

Usage guidelines

This command is not supported in FIPS mode.

The specified ACL filters IPv4 Telnet users' connection requests. Only the IPv4 Telnet users that the ACL permits can initiate Telnet connections to the device.

All IPv4 Telnet users can initiate Telnet connections to the device when any one of the following conditions exists:

- You do not specify any ACLs.
- The specified ACL does not exist.
- The specified ACL does not have any rules.

The ACL takes effect only on Telnet connections that are initiated after the ACL configuration.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure ACL 2001 and permit only the users at 1.1.1.1 to initiate Telnet connections to the device.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 1.1.1.1 0
[Sysname-acl-basic-2001] quit
[Sysname] telnet server acl 2001
```

telnet server ipv6 acl ipv6

Use **telnet server ipv6 acl ipv6** to specify an ACL to control IPv6 Telnet user connections.

Use **undo telnet server ipv6 acl** to restore the default.

Syntax

telnet server ipv6 acl ipv6 *acl-number*

undo telnet server ipv6 acl

Default

No ACLs are specified and all IPv6 Telnet users can initiate Telnet connections to the device.

Views

System view

Default command level

3: Manage level

Parameters

acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999.

Usage guidelines

This command is not supported in FIPS mode.

The specified ACL filters IPv6 Telnet users' connection requests. Only the IPv6 Telnet users that the ACL permits can initiate Telnet connections to the device.

All IPv6 Telnet users can initiate Telnet connections to the device when any one of the following conditions exists:

- You do not specify any ACLs.
- The specified ACL does not exist.
- The specified ACL does not have any rules.

The ACL takes effect only on Telnet connections that are initiated after the ACL configuration.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure ACL 2001 and permit only the users at 2000::1 to initiate Telnet connections to the device.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2001
[Sysname-acl6-basic-2001] rule permit source 2000::1 128
[Sysname-acl6-basic-2001] quit
[Sysname] telnet server ipv6 acl ipv6 2001
```

New feature: Packet rate-limiting for the table-miss flow entry

Packet rate-limiting for the table-miss flow entry

You can specify a meter entry for the table-miss flow entry for rate-limiting on the controller and deploy the table-miss flow entry to devices. Packets that match the table-miss flow entry are directed to the meter entry for rate-limiting before they are sent to the controller.

Command reference

display openflow flow-table

Use **display openflow flow-table** to display flow table information for an OpenFlow instance.

Syntax

display openflow instance *instance-id* **flow-table** [*table-id*]

Views

Any view

Change description

Before modification: The output from the **display openflow flow-table** command does not include information about the meter entry used by the table-miss flow entry.

After modification: The output from the **display openflow flow-table** command includes information about the meter entry used by the table-miss flow entry.

Modified feature: Including time zone information in the timestamp of system information sent to a log host

Feature change description

Added support for including time zone information in the timestamp of system information sent to a log host.

Command changes

Modified command: info-center timestamp loghost

Old syntax

info-center timestamp loghost { **date** | **iso** | **no-year-date** | **none** }

New syntax

info-center timestamp loghost { **date** | **iso** [**with-timezone**] | **no-year-date** | **none** }

Views

System view

Change description

The following parameter was added:

with-timezone: Includes time zone information in the timestamp of system information sent to a log host.

Modified feature: Configuring physical state change suppression on an Ethernet interface

Feature change description

Before modification:

- The system can suppress only link-down or only link-up events. For example, if you configure the **link-delay** *delay-time* [**mode up**] command and then configure the **link-delay** *delay-time* command, the system suppresses only link-down events.
- When you disable physical state change suppression on an interface, suppression for both link-up and link-down events are disabled.

After modification, you can perform the following operations:

- Enable the physical state change suppression time to be accurate to milliseconds by specifying the **msec** keyword.
- Enable the system to suppress both link-down and link-up events by specifying the **updown** keyword.
- Configure different suppression intervals for link-up and link-down events. For example, if you configure the **link-delay** [**msec**] *delay-time* [**mode up**] command and then configure the **link-delay** [**msec**] *delay-time* command, both commands take effect.

- Disable suppression for only link-up events, only link-down events, or both. For example, when both link-up and link-down events are suppressed on an interface and you configure the **undo link-delay** *delay-time* **mode up** command, only suppression for link-up events is disabled.

Command changes

Modified command: link-delay

Old syntax

link-delay *delay-time* [**mode up**]

undo link-delay

New syntax

link-delay [**msec**] *delay-time* [**mode** { **up | updown** }]

undo link-delay [[**msec** *delay-time*] [**mode** { **up | updown** }]]

Views

Ethernet interface view

Change description

Before modification:

- The value range for the *delay-time* argument is 2 to 10 seconds.
- When you configure the **undo link-delay** command on an interface, suppression for both link-up and link-down events are disabled.

After modification:

- The **msec** and **updown** keywords were added to the **link-delay** *delay-time* [**mode up**] command.
    - If you specify the **msec** keyword, the value range for the *delay-time* argument is 500 to 10000 milliseconds, and the value must be an integer multiple of 100. If you do not specify the **msec** keyword, the value range for the *delay-time* argument is 2 to 10 seconds.
    - If you specify the **updown** keyword, the link-down or link-up event is not reported to the CPU unless the interface is still down or up when the suppression interval (*delay-time*) expires.
- The **undo link-delay** command was changed to **undo link-delay** [[**msec** *delay-time*] [**mode** { **up | updown** }]].

  You can disable suppression for only link-up events, only link-down events, or both. For example, when both link-up and link-down events are suppressed on an interface and you configure the **undo link-delay** *delay-time* **mode up** command, only suppression for link-up events is disabled.

Modified feature: Configuring a tag and description for an IPv6 static route

Feature change description

The **tag** *tag-value* and **description** *description-text* options were added to the **ipv6 route-static** command. The **tag** *tag-value* option configures a tag for an IPv6 static route, and the **description** *description-text* option configures a description for an IPv6 static route.

Command changes

Modified command: ipv6 route-static

Old syntax

ipv6 route-static *ipv6-address prefix-length* { *interface-type interface-number* [*next-hop-address*] **|** *next-hop-address* **|** **vpn-instance** *d-vpn-instance-name next-hop-address* } [**preference** *preference-value*]

ipv6 route-static vpn-instance *s-vpn-instance-name*&<1-6> *ipv6-address prefix-length* { *interface-type interface-number* [*next-hop-address*] **|** *next-hop-address* [**public**] **|** **vpn-instance** *d-vpn-instance-name next-hop-address* } [**preference** *preference-value*]

New syntax

ipv6 route-static *ipv6-address prefix-length* { *interface-type interface-number* [*next-hop-address*] **|** *next-hop-address* **|** **vpn-instance** *d-vpn-instance-name next-hop-address* } [**preference** *preference-value*] [**tag** *tag-value*] [**description** *description-text*]

ipv6 route-static vpn-instance *s-vpn-instance-name*&<1-6> *ipv6-address prefix-length* { *interface-type interface-number* [*next-hop-address*] **|** *next-hop-address* [**public**] **|** **vpn-instance** *d-vpn-instance-name next-hop-address* } [**preference** *preference-value*] [**tag** *tag-value*] [**description** *description-text*]

Views

System view

Change description

The **tag** *tag-value* and **description** *description-text* options were added.

- **tag** *tag-value*: Configures a tag for an IPv6 static route, in the range of 1 to 4294967295. The default is 0. Tags of routes are used for route control in routing policies.
- **description** *description-text*: Configures a description for an IPv6 static route. The description is a string of 1 to 60 characters, including special characters such as the space, but excluding the question mark (?).

A5500EI-CMW520-R2221P04

This release has the following changes:

- New feature: 802.1X voice VLAN
- New feature: Configuring the uplink port to permit multiple isolate-user-VLANs
- New feature: TCP fragment attack protection
- New feature: Portal roaming
- Modified feature: Username request timeout timer for 802.1X authentication
- Modified feature: Default configuration

New feature: 802.1X voice VLAN

Configuring an 802.1X voice VLAN

You can configure an 802.1X voice VLAN on an 802.1X-enabled port that connects to a voice terminal. The 802.1X voice VLAN feature is effective only on voice terminals that support VLAN-tagged packets.

The 802.1X voice VLAN feature works with a remote authentication server. The device uses the following process to implement this feature:

1. Identifies a voice terminal from the packet sent by the authentication server when the terminal passes 802.1X authentication. The authentication server identifies the terminal type by information such as its OUI and user account, and then sends the terminal type information to the device.
2. Assigns the port to the configured voice VLAN as a tagged member and sends the voice VLAN information through an LLDP or CDP packet to the terminal.

A voice terminal is not associated with a specific voice VLAN. The voice VLAN assigned to the voice terminal depends on the voice VLAN configuration on the access port.

Configuration guidelines

When you configure an 802.1X voice VLAN, follow these guidelines:

- You can configure only one 802.1X voice VLAN on a port. The 802.1X voice VLANs on different ports can be different.
- To ensure a correct exchange of 802.1X EAPOL packets, you must configure the **dot1x eapol untag** command. For information about how to configure this command, see *HP 5500 EI & 5500 SI Switch Series Security Configuration Guide-Release 2220*.
- A server-assigned authorization VLAN for a voice terminal takes precedence over the 802.1X voice VLAN. The port will be assigned to the authorization VLAN if both VLANs coexist. For information about 802.1 X VLAN manipulations, see *HP 5500 EI & 5500 SI Switch Series Security Configuration Guide-Release 2220*.
- This feature cannot work with the RADIUS server provided by IMC.

Configuration prerequisites

Before you configure this feature, complete the following tasks:

- Enable 802.1X on the port.

- Set the port type to hybrid or trunk, because the port is assigned to the 802.1X voice VLAN as a tagged member. For information about port types, see *HP 5500 EI & 5500 SI Switch Series Layer 2—LAN Switching Configuration Guide-Release 2220*.
- Configure LLDP or CDP compatibility on the device. For information about the LLDP and CDP compatibility features, see *HP 5500 EI & 5500 SI Switch Series Layer 2—LAN Switching Configuration Guide-Release 2220*.

Configuration procedure

To configure an 802.1X voice VLAN on a port:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure an 802.1X voice VLAN on the port.	**dot1x voice vlan** *vlan-id*	By default, no 802.1X voice VLAN is configured on a port.

Command reference

New command: dot1x voice vlan

Use **dot1x voice vlan** to configure an 802.1X voice VLAN on a port.

Use **undo dot1x voice vlan** to remove the 802.1X voice VLAN on a port.

Syntax

dot1x voice vlan *vlan-id*

undo dot1x voice vlan

Default

No 802.1X voice VLAN is configured on a port.

Views

Ethernet interface view

Default command level

2: System level

Parameters

vlan-id: Specifies a voice VLAN by its ID in the range of 1 to 4094. The VLAN must have been created.

Usage guidelines

This command must function with a remote authentication server (for example, FreeRADIUS). It cannot work with the RADIUS server provided by IMC.

To ensure a correct exchange of 802.1X EAPOL packets, you must configure the **dot1x eapol untag** command. For information about how to configure this command, see *HP 5500 EI & 5500 SI Switch Series Security Configuration Guide-Release 2220*.

The server-assigned authorization VLAN takes precedence over the 802.1X voice VLAN on a port. The port will be assigned to the authorization VLAN if both VLANs coexist. For information about

802.1 X VLAN manipulations, see *HP 5500 EI & 5500 SI Switch Series Security Configuration Guide-Release 2220*.

Before you configure an 802.1X voice VLAN on a port, perform the following tasks:

- Enable 802.1X on the port.
- Set the port type to hybrid or trunk, because the port is assigned to the 802.1X voice VLAN as a tagged member. For information about port types, see *HP 5500 EI & 5500 SI Switch Series Layer 2—LAN Switching Configuration Guide-Release 2220*.
- Configure LLDP or CDP compatibility on the device. For information about the LLDP and CDP compatibility features, see *HP 5500 EI & 5500 SI Switch Series Layer 2—LAN Switching Configuration Guide-Release 2220*.

Examples

Configure VLAN 20 as the 802.1X voice VLAN on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x voice vlan 20
```

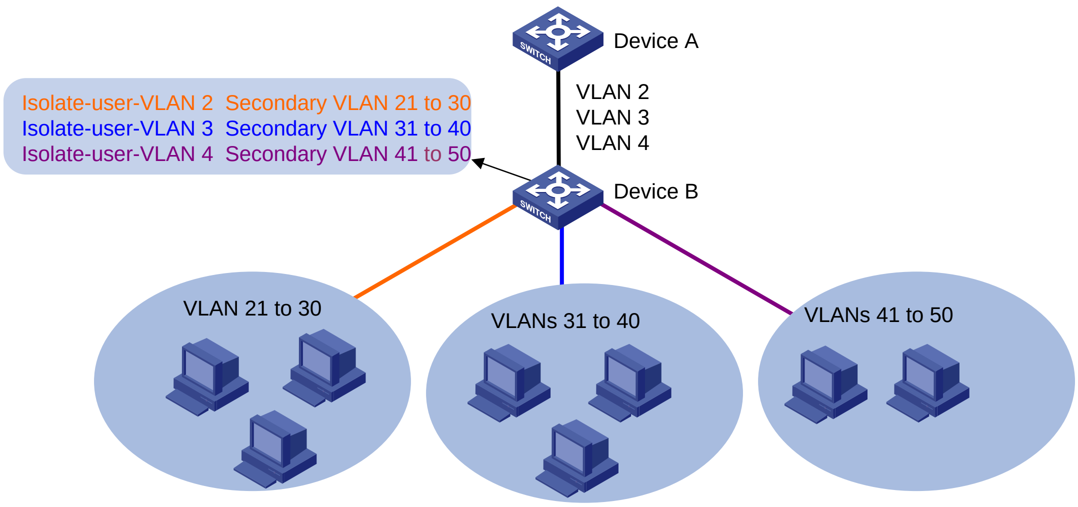
New feature: Configuring the uplink port to permit multiple isolate-user-VLANs

Configuring the uplink port to permit multiple isolate-user-VLANs

Overview

This feature configures the uplink port of a switch to permit packets from multiple isolate-user-VLANs to pass through tagged. As shown in Figure 1, VLANs 2, 3, and 4 are configured as isolate-user-VLANs on Device B. Secondary VLANs 21 through 30 are associated with isolate-user-VLAN 2, secondary VLANs 31 through 40 are associated with isolate-user-VLAN 3, and secondary VLANs 41 through 50 are associated with isolate-user-VLAN 4. Packets from isolate-user-VLANs 2, 3, and 4 pass through the uplink port (the port connecting Device B to Device A in Figure 1) tagged. Device A identifies only VLANs 2, 3, and 4.

Figure 1 Application scenario



Configuration procedure

To configure the uplink port to permit packets from multiple isolate-user-VLANs to pass through tagged:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a VLAN and enter VLAN view.	**vlan** *vlan-id*	N/A
3. Configure the VLAN as an isolate-user-VLAN.	**isolate-user-vlan enable**	By default, no isolate-user-VLAN exists.
4. Return to system view.	**quit**	N/A
5. Configure multiple VLANs in batch.	**vlan** { *vlan-id1* [**to** *vlan-id2*] | **all** }	N/A
6. Isolate ports in the same secondary VLAN at Layer 2.	**isolated-vlan enable**	Optional. By default, ports in the same secondary VLAN can communicate with each other at Layer 2. This configuration takes effect only after the ports in the secondary VLAN are configured to operate in host mode and the secondary VLAN is associated with an isolate-user-VLAN.
7. Return to system view.	**quit**	N/A
8. Configure the uplink port.	**a** Enter Layer-2 Ethernet interface view or Layer-2 aggregate interface view: **interface** *interface-type interface-number* **b** Configure the port to operate in promiscuous mode in the specified VLANs: **port isolate-user-vlan** *vlan-list* **trunk promiscuous**	By default, a port does not operate in promiscuous mode.
9. Configure the downlink port.	**a** Enter Layer-2 Ethernet interface view or Layer-2 aggregate interface view: **interface** *interface-type interface-number* **b** (Optional.) Configure the link type of the port: **port link-type** { **access** | **hybrid | trunk** } **c** Assign the downlink port to the specified secondary VLANs (use one of the commands depending on the link type): **port access vlan** *vlan-id* Or **port trunk permit vlan** { *vlan-list* | **all** } Or **port hybrid vlan** *vlan-list* { **tagged** | **untagged** } **d** Configure the downlink port to operate in host mode: **port isolate-user-vlan host**	By default, a port does not operate in host mode.

Step	Command	Remarks
10. Return to system view.	**quit**	N/A
11. Associate the specified secondary VLANs with an isolate-user-VLAN.	**isolate-user-vlan** *isolate-user-vlan-id* **secondary** *secondary-vlan-id* [**to** *secondary-vlan-id*]	By default, no isolate-user-VLAN is associated with a secondary VLAN.

CAUTION:

The **port isolate-user-vlan** *vlan-list* **trunk promiscuous** command and the **port isolate-user-vlan** *vlan-id* **promiscuous** command are mutually exclusive. The two commands are different as follows:

- The former configures a port to permit packets from multiple isolate-user-VLANs to pass through tagged.
- The latter configures a port to permit packets from only one isolate-user-VLAN to pass through untagged.

NOTE:

For more information about the isolate-user-VLAN configuration, see *Layer 2—LAN Switching Configuration Guide*.

Configuration example

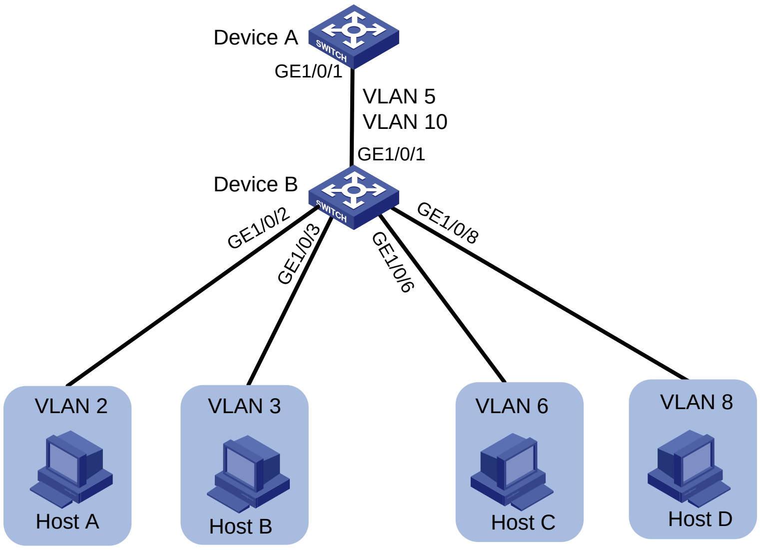
Network requirements

As shown in Figure 2, Device B is attached to Device A.

Configure the isolate-user-VLAN feature, so that:

- VLAN 5 and VLAN 10 are isolate-user-VLANs on Device B. The uplink port GigabitEthernet 1/0/1 permits packets from VLANs 5 and 10 to pass through tagged.
- On Device B, the downlink port GigabitEthernet 1/0/2 permits secondary VLAN 2 and the downlink port GigabitEthernet 1/0/3 permits VLAN 3. Secondary VLANs 2 and 3 are associated with isolate-user-VLAN 5.
- On Device B, the downlink port GigabitEthernet 1/0/6 permits secondary VLAN 6 and the downlink port GigabitEthernet 1/0/8 permits VLAN 8. Secondary VLANs 6 and 8 are associated with isolate-user-VLAN 10.
- Device A identifies only VLANs 5 and 10 on Device B.

Figure 2 Network diagram



Configuration procedure

1. Configure Device B:

   # Configure VLAN 5 and VLAN 10 as isolate-user-VLANs.

```
<DeviceB> system-view
[DeviceB] vlan 5
[DeviceB-vlan5] isolate-user-vlan enable
[DeviceB-vlan5] quit
[DeviceB] vlan 10
[DeviceB-vlan10] isolate-user-vlan enable
[DeviceB-vlan10] quit
```

   # Create VLANs 2, 3, 6, and 8.

```
[DeviceB] vlan 2 to 3
[DeviceB] vlan 6
[DeviceB-vlan6] quit
[DeviceB] vlan 8
[DeviceB-vlan8] quit
```

   # Configure the uplink port GigabitEthernet 1/0/1 to operate in promiscuous mode in VLANs 5 and 10.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port isolate-user-vlan 5 10 trunk promiscuous
[DeviceB-GigabitEthernet1/0/1] quit
```

   # Assign the downlink port GigabitEthernet 1/0/2 to VLAN 2, and configure the port to operate in host mode in VLAN 2. Assign the downlink port GigabitEthernet 1/0/3 to VLAN 3, and configure the port to operate in host mode in VLAN 3.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port access vlan 2
[DeviceB-GigabitEthernet1/0/2] port isolate-user-vlan host
[DeviceB-GigabitEthernet1/0/2] quit
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port access vlan 3
[DeviceB-GigabitEthernet1/0/3] port isolate-user-vlan host
```

```
[DeviceB-GigabitEthernet1/0/3] quit
```

Associate secondary VLANs 2 and 3 with isolate-user-VLAN 5.

```
[DeviceB] isolate-user-vlan 5 secondary 2 to 3
```

Assign the downlink port GigabitEthernet 1/0/6 to VLAN 6, and configure the port to operate in host mode in VLAN 6. Assign the downlink port GigabitEthernet 1/0/8 to VLAN 8, and configure the port to operate in host mode in VLAN 8.

```
[DeviceB] interface gigabitethernet 1/0/6
[DeviceB-GigabitEthernet1/0/6] port access vlan 6
[DeviceB-GigabitEthernet1/0/6] port isolate-user-vlan host
[DeviceB-GigabitEthernet1/0/6] quit
[DeviceB] interface gigabitethernet 1/0/8
[DeviceB-GigabitEthernet1/0/8] port access vlan 8
[DeviceB-GigabitEthernet1/0/8] port isolate-user-vlan host
[DeviceB-GigabitEthernet1/0/8] quit
```

Associate secondary VLANs 6 and 8 with isolate-user-VLAN 10.

```
[DeviceB] isolate-user-vlan 10 secondary 6 8
```

2. Configure Device A:

Create VLAN 5 and VLAN 10.

```
[DeviceA] vlan 5
[DeviceA-vlan5] quit
[DeviceA] vlan 10
[DeviceA-vlan10] quit
```

Configure GigabitEthernet 1/0/1 as a hybrid port, and configure the port to permit the packets from VLAN 5 and VLAN 10 to pass through tagged.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type hybrid
[DeviceA-GigabitEthernet1/0/1] port hybrid vlan 5 10 tagged
[DeviceA-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Display the configuration of isolate-user-VLAN 5. (The output for isolate-user-VLAN 10 is similar.)

```
[DeviceB] display isolate-user-vlan 5
 Isolate-user-VLAN VLAN ID : 5
 Secondary VLAN ID : 2-3

 VLAN ID: 5
 VLAN Type: static
 Isolate-user-VLAN type : isolate-user-VLAN
 Route Interface: not configured
 Description: VLAN 0005
 Name: VLAN 0005
 Tagged   Ports:
    GigabitEthernet1/0/1
 Untagged Ports:
    GigabitEthernet1/0/2          GigabitEthernet1/0/3

 VLAN ID: 2
 VLAN Type: static
```

```
Isolate-user-VLAN type : secondary
Route Interface: not configured
Description: VLAN 0002
Name: VLAN 0002
Tagged   Ports:
   GigabitEthernet1/0/1
Untagged Ports:
   GigabitEthernet1/0/2

VLAN ID: 3
VLAN Type: static
Isolate-user-VLAN type : secondary
Route Interface: not configured
Description: VLAN 0003
Name: VLAN 0003
Tagged   Ports:
   GigabitEthernet1/0/1
Untagged Ports:
   GigabitEthernet1/0/3
```

Command reference

port isolate-user-vlan trunk promiscuous

Use **port isolate-user-vlan** *vlan-list* **trunk promiscuous** to configure a port to operate in promiscuous mode in the specified VLANs and assign the port to the specified VLANs as a tagged member. If the specified VLANs are isolate-user-VLANs associated with existing secondary VLANs, this command automatically assigns the port to the associated secondary VLANs as a tagged member. You can configure the specified VLANs as isolate-user-VLANs before or after you execute this command.

Use **undo port isolate-user-vlan** *vlan-list* **trunk promiscuous** to remove the port from the specified VLANs and disable the promiscuous mode for the port in the specified VLANs. However, this command does not remove the port from the associated secondary VLANs or change the link type and PVID of the port. When the promiscuous mode is disabled for the port in all isolate-user-VLANs, the port does not operate in promiscuous mode in any VLAN.

Syntax

port isolate-user-vlan *vlan-list* **trunk promiscuous**

undo port isolate-user-vlan *vlan-list* **trunk promiscuous**

Default

A port does not operate in promiscuous mode in any VLAN.

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default command level

2: System level

Parameters

vlan-list: Specifies multiple isolate-user-VLANs in the format of *vlan-list* = { *vlan-id1* [**to** *vlan-id2*] }&<1-10>, where *vlan-id1* and *vlan-id2* each range from 1 to 4094, *vlan-id1* cannot be greater than *vlan-id2*, and &<1-10> indicates that you can specify up to ten *vlan-id1* [**to** *vlan-id2*] parameters.

Usage guidelines

When you execute the **port isolate-user-vlan** *vlan-list* **trunk promiscuous** command, follow these guidelines:

- If the port is an access port, this command configures the link type as hybrid, and keeps the PVID configuration; if the port is a trunk or hybrid port, this command does not change the link type and PVID configuration of the port.
- If the link type of the port has been hybrid or is changed from access to hybrid by this command, this command automatically assigns the port to the specified VLANs and the associated secondary VLANs as a tagged member (if the port has been assigned to some of the specified VLANs and the associated secondary VLANs as an untagged member, this command does not change untagged membership).

The **port isolate-user-vlan** *vlan-list* **trunk promiscuous** command is mutually exclusive with the **port isolate-user-vlan** *vlan-id* **promiscuous** command and the **port isolate-user-vlan host** command.

Examples

Configure the access port GigabitEthernet 1/0/1 to operate in promiscuous mode in isolate-user-VLANs 2 and 3, which are associated with VLANs 20 and 30, respectively. Then, disable the promiscuous mode for GigabitEthernet 1/0/1 in isolate-user-VLANs 2 and 3.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
#
return
[Sysname-GigabitEthernet1/0/1] port isolate-user-vlan 2 3 trunk promiscuous
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port isolate-user-vlan 2 3 trunk promiscuous
 port link-type hybrid
 port hybrid vlan 2 3 20 30 tagged
 port hybrid vlan 1 untagged
#
return
[Sysname-GigabitEthernet1/0/1] undo port isolate-user-vlan 2 3 trunk promiscuous
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 20 30 tagged
 port hybrid vlan 1 untagged
#
return
```

VLAN 10 is not an isolate-user-VLAN. Configure the access port GigabitEthernet 1/0/1 to operate in promiscuous mode in VLAN 10. Then, disable the promiscuous mode configuration for GigabitEthernet 1/0/1 in VLAN 10.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
#
return
[Sysname-GigabitEthernet1/0/1] port isolate-user-vlan 10 trunk promiscuous
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port isolate-user-vlan 10 trunk promiscuous
 port link-type hybrid
 port hybrid vlan 10 tagged
 port hybrid vlan 1 untagged
#
return
[Sysname-GigabitEthernet1/0/1] undo port isolate-user-vlan 10 trunk promiscuous
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 1 untagged
#
Return
```

New feature: TCP fragment attack protection

Enabling TCP fragment attack protection

The TCP fragment attack protection function enables the device to drop attack TCP fragments to prevent TCP fragment attacks. As defined in RFC 1858, attack TCP fragments refer to the following TCP fragments:

- First fragments in which the TCP header is smaller than 20 bytes.
- Non-first fragments with a fragment offset of 8 bytes (FO=1).

Traditional packet filter on the device detects the source and destination IP addresses, source and destination ports, and transport layer protocol of the first fragment of a TCP packet. If the first fragment passes the detection, all subsequent fragments of the TCP packet are allowed to pass through. An attacker can launch TCP fragment attacks through either of the following ways:

- Make the first fragment small enough to force some TCP header fields into the second fragment and set TCP flags illegally in the second fragment.
- Fabricate a non-first fragment in which the fragment offset is set to 8 bytes and the TCP flags are set differently and illegally from those in the first fragment. When the receiving host

reassembles the fragments, the illegal TCP flags in the non-first fragment overwrite the legal TCP flags in the first fragment.

Because the first fragment does not hit any match in the packet filter, the subsequent fragments can all pass through. After the receiving host reassembles the fragments, a TCP fragment attack occurs.

To enable TCP fragment attack protection:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable TCP fragment attack protection.	**attack-defense tcp fragment enable**	By default, TCP fragment attack protection is enabled.

Command reference

attack-defense tcp fragment enable

Use **attack-defense tcp fragment enable** to enable TCP fragment attack protection.

Use **undo attack-defense tcp fragment enable** to disable TCP fragment attack protection.

Syntax

attack-defense tcp fragment enable

undo attack-defense tcp fragment enable

Default

TCP fragment attack protection is enabled.

Views

System view

Default command level

2: System level

Usage guidelines

This command enables the device to drop attack TCP fragments to prevent TCP fragment attacks.

Examples

Enable TCP fragment attack protection.

```
<Sysname> System-view
[Sysname] attack-defense tcp fragment enable
```

New feature: Portal roaming

Enabling portal roaming

Portal roaming takes effect only on portal users logging in from VLAN interfaces.

If portal roaming is enabled on a VLAN interface, an online portal user can access resources from any Layer 2 port in the VLAN without re-authentication.

If portal roaming is disabled, to access external network resources from a Layer 2 port different from the current access port in the VLAN, the user must do the following:

- First log out from the current port.

- Then re-authenticate on the new Layer 2 port.

After configuring this feature, you must save the configuration and then restart the device to validate the configuration.

To enable portal roaming:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable portal roaming.	**portal-roaming enable**	By default, portal roaming is disabled.

Command reference

New command: portal-roaming enable

Use **portal-roaming enable** to enable portal roaming.

Use **undo portal-roaming enable** to disable portal roaming.

Syntax

portal-roaming enable

undo portal-roaming enable

Default

Portal roaming is disabled. An online portal user cannot roam in its VLAN.

Views

System view

Usage guidelines

After configuring this command, you must save the configuration and then restart the device to validate the configuration.

This command applies only to portal users that log in from VLAN interfaces.

If portal roaming is enabled, an online portal user can access network resources from any Layer 2 port in its local VLAN. If portal roaming is disabled, the portal user can access network resources only from the Layer 2 port on which it passes authentication.

Examples

Enable portal roaming.

```
<Sysname> system-view
[Sysname] portal-roaming enable
Please save. Configured portal-roaming enable mode will take effect after rebooting the device.
```

Modified feature: Username request timeout timer for 802.1X authentication

Feature change description

The minimum value for the 802.1X username request timeout timer was changed from 10 seconds to 1 second. This modification allows the device to send EAP-Request/Identity packets to initiate 802.1X authentication at a shorter interval.

Command changes

Modified command: dot1x timer

Syntax

dot1x timer tx-period *tx-period-value*

Views

System view

Change description

Before modification: The value range for the *tx-period-value* argument is 10 to 120 seconds.

After modification: The value range for the *tx-period-value* argument is 1 to 120 seconds.

Modified feature: Default configuration

Feature change description

The following changes are made to the default configuration in this release:

- The **interface vlan-interface1** command is added and VLAN-interface 1 is created.
- The **ip address dhcp-alloc client-identifier mac Vlan-interface1** command (VLAN interface 1 view) is added and VLAN-interface 1 uses its MAC address as the client ID for IP address acquisition.

The default configuration takes effect only when the switch starts up with no specific configuration file. Once you specify a specific startup configuration file for the switch, the switch uses the specific configuration file instead of the default configuration.

Command changes

None.

A5500EI-CMW520-R2221P02

This release has the following changes:

- New feature: Support for BPDU guard configuration in interface or port group view
- New feature: MAC re-authentication timer for users in guest VLAN
- New feature: Specifying the IPv4/IPv6 VRRP version
- New feature: MAC and port uniqueness check by the DHCP snooping device
- Modified feature: Auto status transition of dynamic secure MAC addresses
- Modified feature: The maximum number of gateways supported in MFF automatic mode

New feature: Support for BPDU guard configuration in interface or port group view

Configuring BPDU guard for an interface or port group

Before this feature was introduced, the device supported only global BPDU guard configuration (**stp bpdu-protection**). Global BPDU guard configuration takes effect on all edge ports. Edge ports are configured by using the **stp edged-port enable** command.

This feature allows you to perform the following tasks:

- Enable BPDU guard for an interface or port group when BPDU guard is globally disabled.
- Disable BPDU guard for an interface or port group when BPDU guard is globally enabled.

You must enable BPDU guard on a port that directly connects to a user terminal rather than another device or shared LAN segment.

Enabling BPDU guard for an interface or port group when BPDU guard is globally disabled

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view or port group view.	• Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: **interface** *interface-type interface-number* • Enter port group view: **port-group manual** *port-group-name*	Use one of the commands.
3. Enable BPDU guard.	**stp port bpdu-protection enable**	BPDU guard is disabled on all interfaces if it is globally disabled. By default, BPDU guard is globally disabled.

Disabling BPDU guard for an interface or port group when BPDU guard is globally enabled

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable BPDU guard globally.	**stp bpdu-protection**	By default, BPDU guard is globally disabled.
3. Enter interface view or port group view.	• Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: **interface** *interface-type interface-number* • Enter port group view: **port-group manual** *port-group-name*	Use one of the commands.
4. Disable BPDU guard.	**stp port bpdu-protection disable**	By default, BPDU guard is enabled on all edge ports if it is globally enabled.

Command reference

New command: stp port bpdu-protection

Use **stp port bpdu-protection** to configure BPDU guard on an interface.

Use **undo stp port bpdu-protection** to restore the default.

Syntax

stp port bpdu-protection { **enable** | **disable** }

undo stp port bpdu-protection

Default

BPDU guard is not configured on an interface. For an edge port, BPDU guard is enabled on the port if the function is globally enabled. BPDU guard is disabled on the port if the function is disabled globally.

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default command level

2: System level

Parameters

enable: Enables BPDU guard on the interface.

disable: Disables BPDU guard on the interface.

Usage guidelines

When the setting is configured in Layer 2 Ethernet interface view, it takes effect on only that interface.

When the setting is configured in Layer 2 aggregate interface view, it takes effect on only the aggregate interface.

When the setting is configured in port group view, it takes effect on all ports in the port group.

When the setting is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Enable BPDU guard on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp port bpdu-protection enable
```

Related commands

- **stp bpdu-protection**
- **stp edged-port**

For more information about these commands, see spanning tree commands in *Layer 2—LAN Switching Command Reference*.

New feature: MAC re-authentication timer for users in guest VLAN

Configuring MAC re-authentication timer for users in guest VLAN

The MAC re-authentication timer sets the interval that the device must wait before it can re-authenticate a user in the MAC authentication guest VLAN.

The device handles VLANs for users in the MAC authentication guest VLAN based on the following rules:

Authentication status	VLAN manipulation
A user fails MAC re-authentication because of unreachable servers.	• If a MAC authentication critical VLAN is available, the device assigns the user to the critical VLAN. • If no MAC authentication critical VLAN is configured, the user is still in the MAC authentication guest VLAN. The MAC re-authentication timer restarts for the user.
A user fails MAC re-authentication for any other reasons except for unreachable servers.	The user is still in the MAC authentication guest VLAN. The MAC re-authentication timer restarts for the user.
A user passes MAC re-authentication.	• The device removes the user from the MAC authentication guest VLAN and assigns the user to the authorization VLAN. • If the authentication server does not authorize a VLAN, the user is assigned to the initial VLAN. The initial VLAN refers to the VLAN to which the user belongs before it was assigned to the MAC authentication guest VLAN.

To configure the MAC re-authentication timer for users in the MAC authentication guest VLAN:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the MAC authentication guest VLAN on the port.	**mac-authentication guest-vlan** *vlan-id*	By default, no guest VLAN is configured on the port.

Step	Command	Remarks
4. Return to system view.	**quit**	N/A
5. Configure the MAC re-authentication timer for users in the guest VLAN.	**mac-authentication timer guest-vlan-reauth** *interval*	The default timer is 30 seconds.

Command reference

mac-authentication timer guest-vlan-reauth

Use **mac-authentication timer guest-vlan-reauth** to set the MAC re-authentication timer for users in the MAC authentication guest VLAN.

Use **undo mac-authentication timer guest-vlan-reauth** to restore the default.

Syntax

mac-authentication timer guest-vlan-reauth *interval*

undo mac-authentication timer guest-vlan-reauth

Default

The MAC re-authentication timer is 30 seconds for users in the MAC authentication guest VLAN.

Views

System view

Default command level

2: System view

Parameters

interval: Set the MAC re-authentication timer for users in the MAC authentication guest VLAN. The value range for this argument is 1 to 3600, in seconds.

Usage guidelines

When the MAC re-authentication timer expires, the device re-authenticates the users in the MAC authentication guest VLAN.

The device handles VLANs for users in the MAC authentication guest VLAN based on the following rules:

Authentication status	VLAN manipulation
A user fails MAC re-authentication because of unreachable servers.	• If a MAC authentication critical VLAN is available, the device assigns the user to the critical VLAN. • If no MAC authentication critical VLAN is configured, the user is still in the MAC authentication guest VLAN. The MAC re-authentication timer restarts for the user.
A user fails MAC re-authentication for any other reasons except for unreachable servers.	The user is still in the MAC authentication guest VLAN. The MAC re-authentication timer restarts for the user.

Authentication status	VLAN manipulation
A user passes MAC re-authentication.	• The device removes the user from the MAC authentication guest VLAN and assigns the user to the authorization VLAN. • If the authentication server does not authorize a VLAN, the user is assigned to the initial VLAN. The initial VLAN refers to the VLAN to which the user belongs before it was assigned to the MAC authentication guest VLAN.

Examples

Set the MAC re-authentication timer to 60 seconds for users in the MAC authentication guest VLAN.

```
<Sysname> system-view
[Sysname] mac-authentication timer guest-vlan-reauth 60
```

New feature: Specifying the IPv4/IPv6 VRRP version

Specifying the IPv4/IPv6 VRRP version

The VRRP version on all routers in a VRRP group must be the same.

If you specify VRRPv3 as the version for an interface, the authentication configuration on the VRRP group does not take effect.

VRRPv3 supports a maximum advertisement interval of 4095 centiseconds. If you configure an advertisement interval that is greater than 4095 centiseconds, the advertisement interval of 4095 centiseconds applies.

To specify the version of IPv4/IPv6 VRRP:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Specify the version of VRRP.	**vrrp version** *version-number*	By default, VRRPv2 is used.

Command reference

vrrp version

Use **vrrp version** to specify the version of VRRP on an interface.

Use **undo vrrp version** to restore the default.

Syntax

vrrp version *version-number*

undo vrrp version

Default

VRRPv2 is used.

Views

Interface view

Default command level

2: System level

Parameters

version-number: Specifies a VRRP version. The version number is 2 or 3. For more information, see the following table:

Value	VRRP version	RFC	Value of the version field in VRRP packets
2	IPv4 VRRPv2	RFC 2338	• 2 in standard protocol mode. • 8 in load balancing mode.
	IPv6 VRRPv2	RFC 3768	• 3 in standard protocol mode. • 9 in load balancing mode.
3	IPv4/IPv6 VRRPv3	RFC 5798	3 in standard protocol mode or load balancing mode.

NOTE:

The IPv6 VRRP packet format is not defined in RFC 3768. HP implemented IPv6 VRRPv2 based on RFC 3768.

Usage guidelines

The version of VRRP on all routers in a VRRP group must be the same.

If you specify VRRPv3 as the version for an interface, the authentication configuration on the VRRP group does not take effect.

For VRRPv3, if you configure an advertisement interval that is greater than 4095 centiseconds, the advertisement interval of 4095 centiseconds applies.

Examples

Specify VRRPv3 to run on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp version 3
```

New feature: MAC and port uniqueness check by the DHCP snooping device

Enabling MAC and port uniqueness check on the DHCP snooping device

This function allows the DHCP snooping device to maintain only one DHCP snooping entry for the same client's MAC address in one VLAN.

When receiving a DHCP REQUEST, the DHCP snooping device checks for a DHCP snooping entry that matches the client's MAC address (the **chaddr** field in the request). If an entry exists with the same MAC address and VLAN but different receiving port, the device updates the entry. When DHCP snooping entries are used by security modules, such as IP source guard, this function prevents clients from using the same MAC address to apply for multiple IP addresses.

To enable MAC and port uniqueness check on the DHCP snooping device:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable MAC and port uniqueness check on the DHCP snooping device.	**dhcp-snooping check mac-port**	By default, MAC and port uniqueness check is disabled on the DHCP snooping device.

Command reference

dhcp-snooping check mac-port

Use **dhcp-snooping check mac-port** to enable MAC and port uniqueness check on the DHCP snooping device.

Use **undo dhcp-snooping check mac-port** to disable MAC and port uniqueness check on the DHCP snooping device.

Syntax

dhcp-snooping check mac-port

undo dhcp-snooping check mac-port

Default

MAC and port uniqueness check is disabled on the DHCP snooping device.

Views

System view

Default command level

2: System level

Examples

Enable MAC and port uniqueness check on the DHCP snooping device.

```
<Sysname> system-view
[Sysname] dhcp-snooping check mac-port
```

Modified feature: Auto status transition of dynamic secure MAC addresses

Feature change description

Before modification: A dynamic secure MAC address entry will not be deleted if the port for the entry goes down.

After modification: The status of dynamic secure MAC address entries transits automatically based on the port status. The device deletes a dynamic secure MAC address entry if the port for the entry goes down. This MAC address is reported as an unknown source MAC address if it is detected on another port.

Command changes

None.

Modified feature: The maximum number of gateways supported in MFF automatic mode

Feature change description

In MFF automatic mode, the maximum number of gateways that can be learned in a VLAN was changed from 20 to 64. No more gateways can be learned when the limit is reached.

Command changes

None.

A5500EI-CMW520-R2221P01

This release has the following changes:

- New feature: Discarding IPv6 packets that contain extension headers

New feature: Discarding IPv6 packets that contain extension headers

Enabling a device to discard IPv6 packets that contain extension headers

This feature enables a device to discard a received IPv6 packet if the first extension header of the packet is Hop-by-Hop Options.

To enable a device to discard IPv6 packets that contain extension headers:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable the device to discard IPv6 packets that contain extension headers.	**ipv6 option drop enable**	By default, the device does not discard IPv6 packets that contain extension headers.

Command reference

New command: ipv6 option drop enable

Use **ipv6 option drop enable** to enable the device to discard IPv6 packets that contain extension headers.

Use **undo ipv6 option drop** to disable the device from discarding IPv6 packets that contain extension headers.

Syntax

ipv6 option drop enable

undo ipv6 option drop

Default

A device does not discard IPv6 packets that contain extension headers.

Views

System view

Default command level

2: System level

Usage guidelines

This feature enables a device to discard a received IPv6 packet if the first extension header of the packet is Hop-by-Hop Options.

Examples

Enable the device to discard IPv6 packets that contain extension headers.

```
<Sysname> system-view
[Sysname] ipv6 option drop enable
```

A5500EI-CMW520-R2221

This release has the following changes:

- New feature: SSL server policy association with the FTP service
- New feature: OpenFlow
- New feature: MFF
- Modified feature: Setting the device name
- Modified feature: Displaying brief interface information
- Modified feature: Displaying brief IP configuration for Layer 3 interfaces
- Modified feature: Configuring static multicast MAC address entries
- Modified feature: Specifying the username and password to log in to the SCP server
- Modified feature: Disabling an untrusted port from recording clients' IP-to-MAC bindings
- Modified feature: Customizing DHCP options

New feature: SSL server policy association with the FTP service

Configuration procedure

For two devices that support secure FTP, you can associate an SSL server policy with the FTP service on the FTP server. Then, the FTP connection will be established over an SSL connection.

Before associating an SSL server policy with the FTP service, you must create the policy and disable FTP server.

To associate an SSL server policy with the FTP service:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Associate an SSL server policy with the FTP server to ensure data security.	**ftp server ssl-server-policy** *policy-name*	By default, no SSL server policy is associated with the FTP server.

Command reference

ftp server ssl-server-policy

Syntax

ftp server ssl-server-policy *policy-name*

undo ftp server ssl-server-policy

Views

System view

Default level

2: System level

Parameters

policy-name: Specifies an SSL server policy by its name, a string of 1 to 16 characters.

Description

Use **ftp server ssl-server-policy** to associate an SSL server policy with the FTP server.

Use **undo ftp server ssl-server-policy** to remove the association.

By default ,no SSL server policy is associated with the FTP server.

Examples

Associate SSL server policy **myssl** with the FTP server.

```
<Sysname> system-view
[Sysname] ftp server ssl-server-policy myssl
```

New feature: OpenFlow

You cannot configure both OpenFlow and IRF on an switch.

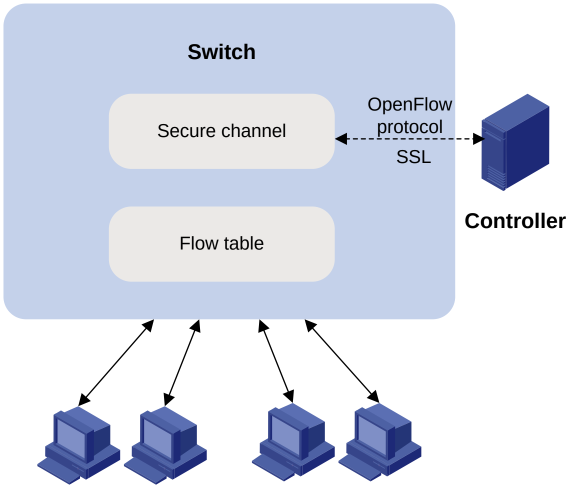
Software-Defined Networking (SDN) was developed to meet the growing requirements of virtualization technologies and data networks. SDN uses software to separate controlling functions from data forwarding, and provides simple, flexible device operations and high extensibility.

OpenFlow is the communication interface between a controller and network devices to implement SDN. With OpenFlow, you can perform centralized data forwarding management for physical and virtual devices.

Overview

OpenFlow separates the data forwarding and routing decision functions. It keeps the flow-based forwarding function and employs a separate controller to make routing decisions. A switch communicates with the controller through a secure channel.

Figure 1 OpenFlow network diagram



Basic concepts

OpenFlow switch

OpenFlow switches are classified into the following types:

- **OpenFlow-only**—Supports only OpenFlow operation.
- **OpenFlow-hybrid**—Supports both OpenFlow operation and traditional Ethernet switching operations. Switches of this series are OpenFlow-hybrid switches.

OpenFlow port

IMPORTANT:

The switch does not support aggregate interfaces, tunnel interfaces, and loopback interfaces.

OpenFlow supports the following types of ports:

- **Physical port**—Corresponds to a hardware interface of a switch, such as an Ethernet interface. A physical port can be either an ingress port or an output port.
- **Logical port**—Does not correspond to a hardware interface of a switch and might be defined by non-OpenFlow methods. A logical port can be either an ingress port or an output port.
- **Reserved port**—Defined by OpenFlow to specify forwarding actions. Reserved ports include the following types:
    - **All**—All OpenFlow ports that can be used to forward a packet. Only HP 5500-24G EI Switch with 2 Interface Slots(JD377A), HP 5500-24G EI TAA Switch with 2 Interface Slots(JG250A), HP 5500-24G-SFP EI Switch with 2 Interface Slots(JD374A), HP 5500-24G-SFP EI TAA Switch with 2 Interface Slots(JG249A), HP 5500-24G-PoE+ EI Switch with 2 Interface Slots(JG241A) and HP 5500-24G-PoE+ EI TAA Switch with 2 Interface Slots(JG252A) support this type.
    - **Controller**—OpenFlow controller.
    - **Table**—Flow table.
    - **In_Port**—Packet ingress port.
    - **Any**—Generic port description. The port cannot be used as an ingress port or output port.
    - **Local**—Local CPU.
    - **Normal**—Normal forwarding process.
    - **Flood**—Flooding. Only HP 5500-24G EI Switch with 2 Interface Slots(JD377A), HP 5500-24G EI TAA Switch with 2 Interface Slots(JG250A), HP 5500-24G-SFP EI Switch with 2 Interface Slots(JD374A), HP 5500-24G-SFP EI TAA Switch with 2 Interface Slots(JG249A), HP 5500-24G-PoE+ EI Switch with 2 Interface Slots(JG241A) and HP 5500-24G-PoE+ EI TAA Switch with 2 Interface Slots(JG252A) support this type.

  Except the **Any** type, all reserved ports can be used only as output ports.

OpenFlow flow table

An OpenFlow switch matches packets against one or more user-defined flow tables. A flow table consists of flow entries, and packets are matched based on the matching precedence of flow entries.

Figure 2 Components of a flow entry

Match Fields	Priority	Counters	Instructions	Timeouts	Cookie

A flow entry contains the following fields:

- **Match fields**—Matching rules of the flow entry. These consist of the ingress port, packet headers, and metadata specified by the previous table.
- **Priority**—Matching precedence of the flow entry. A packet is matched against the table and only the highest priority flow entry that matches the packet is selected.
- **Counters**—Counts of the packets that match the flow entry.
- **Instructions**—To modify the action set or pipeline processing. These include the following types:

- **Meter**—Directs the packets to the specified meter to limit the rate of the packets. When a meter entry is used by multiple flow entries, the switch creates a CAR action for each flow entry to limit the rate of packets.
- **Apply-Actions**—Applies the specified actions in the action list immediately.
- **Clear-Actions**—Clears all the actions in the action set immediately.
- **Write-Actions**—Modifies all the actions in the action set immediately.
- **Write-Metadata**—Modifies packets between two flow tables if there are multiple flow tables.
- **Goto-Table**—Indicates the next flow table in the processing line.

Actions are executed in one of the following ways:

- **Action Set**—When the instruction set of a flow entry does not contain a **Goto-Table** instruction, pipeline processing stops and the actions in the action set are executed. An action set contains a maximum of one action of each type.
- **Action List**—The actions in the action list are executed immediately in the order specified by the action list. The effect of those actions is cumulative.

- **Timeouts**—Maximum amount of idle time or hard time for the flow entry.
  - **Idle Time**—The flow entry is removed when it has matched no packets during the idle time.
  - **Hard Time**—The flow entry is removed when the hard time timeout is exceeded, regardless of whether or not it has matched packets.
- **Cookie**—Flow entry identifier specified by the controller.

Every flow table must support a table-miss flow entry to process table misses. The table-miss flow entry specifies how to process packets unmatched by other flow entries in the flow table. The table-miss flow entry wildcards all match fields (all fields omitted) and has the lowest priority 0. The table-miss flow entry behaves in most ways like any other flow entry.

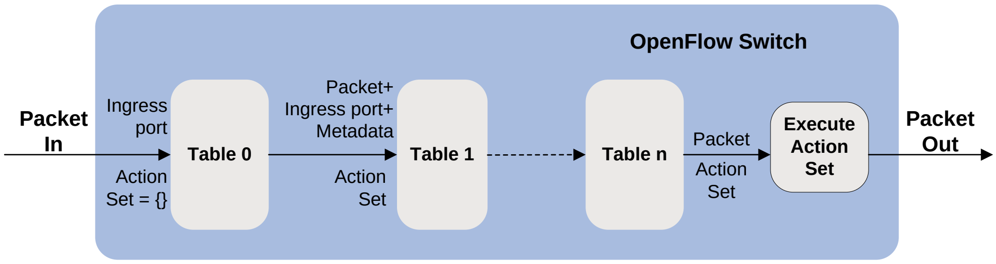
OpenFlow pipeline

The OpenFlow pipeline processing defines how packets interact with flow tables contained by a switch.

The flow tables of an OpenFlow switch are sequentially numbered, starting at 0. The packet is first matched against flow entries of first flow table: flow table 0. A flow entry can only direct a packet to a flow table number which is greater than its own flow table number.

When a packet matches a flow entry, the OpenFlow switch updates the action set for the packet and passes the packet to the next flow table. In the last flow table, the OpenFlow switch executes all actions to modify packet contents and specify the output port for packet forwarding. If the instruction set of one of the flow tables contains an action list, the OpenFlow switch executes the actions to modify a copy of the packet immediately in this table.

Figure 3 OpenFlow forwarding workflow



OpenFlow flow tables include the following types:

- **MAC-IP**—Combines the MAC address table and FIB table.

  A MAC-IP flow table provides the following match fields:
  - Destination MAC address

- VLAN
- Destination IP address

A MAC-IP flow table provides the following actions:

- Modifying the destination MAC address
- Modifying the source MAC address
- Modifying the VLAN
- Specifying the output port

- **Extensibility**—Provides more matching fields and actions than a MAC-IP flow table does.

Group table

IMPORTANT:

Only HP 5500-24G EI Switch with 2 Interface Slots(JD377A), HP 5500-24G EI TAA Switch with 2 Interface Slots(JG250A), HP 5500-24G-SFP EI Switch with 2 Interface Slots(JD374A), HP 5500-24G-SFP EI TAA Switch with 2 Interface Slots(JG249A), HP 5500-24G-PoE+ EI Switch with 2 Interface Slots(JG241A) and HP 5500-24G-PoE+ EI TAA Switch with 2 Interface Slots(JG252A) support group tables.

The ability for a flow entry to point to a group enables OpenFlow to represent additional methods of forwarding. A group table consists of group entries.

Figure 4 Components of a group entry

Group Identifier	Group Type	Counters	Action Buckets

A group entry contains the following fields:

- **Group Identifier**—A 32 bit unsigned integer uniquely identifying the group.
- **Group Type**—Type of the group.
- **Counters**—Updated when packets are processed by a group.
- **Action Buckets**—An ordered list of action buckets, where each action bucket contains a set of actions to execute and associated parameters.

Meter table

Meters enable OpenFlow to implement various simple QoS operations, such as rate-limiting. A meter table consists of meter entries.

Figure 5 Components of a meter entry

Meter Identifier	Meter Bands	Counters

A meter entry contains the following fields:

- **Meter Identifier**—A 32 bit unsigned integer uniquely identifying the meter.
- **Meter Bands**—Each meter can have one or more meter bands. Each band specifies the rate at which the band applies and the way packets should be processed. If the current rate of packets exceeds the rate of multiple bands, the band with the highest configured rate is used.
- **Counters**—Updated when packets are processed by a meter.

Figure 6 Components of a meter band

Band Type	Rate	Counters	Type Specific arguments

A meter band contains:

- **Band Type**—Defines how packets are processed. Packets that exceed the band rate are dropped.
- **Rate**—Used by the meter to select the meter band, defines the lowest rate at which the band can apply.
- **Counters**—Updated when packets are processed by a band.

Type Specific Arguments—Some band types have optional arguments.

OpenFlow instance

You can configure one or more OpenFlow instances on the same device. A controller considers each OpenFlow instance as a separate OpenFlow switch and deploys forwarding instructions to it.

In this chapter, an OpenFlow switch is the same as an OpenFlow instance, unless otherwise specified.

Associated VLAN

When an OpenFlow instance is associated with VLANs, the flow tables take effect on packets only within these VLANs.

Activation and reactivation

The controller can deploy flow entries only to OpenFlow instances that are activated.

An activated OpenFlow instance need be reactivated when any of the following parameters are changed:

- Associated VLANs
- Flow tables
- Maximum number of supported flow entries

After reactivation, the OpenFlow instance is disconnected from all controllers and reconnects to them.

OpenFlow instance port

An OpenFlow switch sends information about the following ports to the controller:

- Physical ports
- Logical ports
- Reserved ports of the local type

These ports belong to the VLANs that are associated with the OpenFlow instance only when all associated VLANs are within the list of the VLANs to which the ports are assigned. However, if the **loosen** mode is used, a port belongs to the OpenFlow instance when VLANs that are associated with the OpenFlow instance overlap with the VLANs to which the port is assigned.

Protocols and standards

OpenFlow Switch Specification Version 1.3.1

OpenFlow configuration task list

Task		**Remarks**
Configuring OpenFlow	Creating an OpenFlow instance	Required.

Task		Remarks
instances	Associating an OpenFlow instance with VLANs	
	Configuring flow table IDs	Optional.
	Setting the connection mode for an OpenFlow instance to establish connections to controllers	
	Configuring the maximum number of flow entries	
	Configuring in-band management VLANs	
	Disabling MAC address learning in the VLANs associated with an OpenFlow instance	
	Configuring the datapath ID for an OpenFlow instance	
	Activating or reactivating an OpenFlow instance	Required.
Configuring controllers for an OpenFlow switch	Configuring controllers and main connections	Required.
	Setting the connection interruption mode	Optional.
Setting OpenFlow timers		Optional.
Configuring OpenFlow to support dynamic MAC addresses		Optional.

Configuring OpenFlow instances

Creating an OpenFlow instance

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create an OpenFlow instance and enter OpenFlow instance view.	**openflow instance** *instance-id*	By default, no OpenFlow instance exists.
3. (Optional.) Specify a description for the OpenFlow instance.	**description** *text*	By default, an OpenFlow instance does not have a description.

Associating an OpenFlow instance with VLANs

When you associate an OpenFlow instance with VLANs, follow these guidelines:

- Do not associate multiple OpenFlow instances to the same VLAN. Otherwise, VLAN traffic cannot be correctly processed.
- When you activate an OpenFlow instance that is associated with non-existent VLANs, the system automatically creates the VLANs. Do not delete any of these VLANs after the OpenFlow instance is activated.
- VLANs that are associated with an OpenFlow instance cannot contain loopback interfaces.

To associate an OpenFlow instance with VLANs:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter OpenFlow instance view.	**openflow instance** *instance-id*	N/A
3.	Associate the OpenFlow instance with VLANs.	**classification vlan** *vlan-id* [**mask** *vlan-mask*] [**loosen**]	By default, an OpenFlow instance is not associated with any VLAN.

Configuring flow table IDs

You can configure one MAC-IP flow table and one extensibility flow table for an OpenFlow instance, and the MAC-IP flow table ID must be smaller than the extensibility flow table ID.

To configure flow table IDs for an OpenFlow instance:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter OpenFlow instance view.	**openflow instance** *instance-id*	N/A
3.	Configure the flow table ID.	**flow-table** { **extensibility** *table-id* | **mac-ip** *table-id* }*	By default, OpenFlow supports only one flow table with an ID of 0, which is the extensibility type.

Setting the connection mode for an OpenFlow instance to establish connections to controllers

The following connection modes are available for an OpenFlow instance to establish connections to controllers:

- **single**—When the connection mode is **single**, an OpenFlow establishes a connection to only one controller at a time, and the other controllers back up the controller. When the current connection is broken, the OpenFlow instance attempts to connect to the next controller until it successfully establishes a connection.
- **multiple**—When the connection mode is **multiple**, an OpenFlow can establish connections to multiple controllers at a time. When the OpenFlow instance fails to connect to a controller or the connection to a controller is broken, the OpenFlow instance attempts to reconnect to the controller after the reconnection interval expires until it successfully establishes a connection to the controller.

To set the connection mode for an OpenFlow instance to establish connections to controllers:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter OpenFlow instance view.	**openflow instance** *instance-id*	N/A
3.	Set the connection mode for the OpenFlow instance to establish connections to controllers.	**controller mode** { **multiple** | **single** }	By default, the connection mode is **multiple**.

Configuring the maximum number of flow entries

To improve OpenFlow availability, extensibility flow table can have a maximum number of flow entries. When entries in a table reaches the maximum number, the OpenFlow instance does not accept new flow entries for that table and sends a deployment failure notification to the controller.

To configure the maximum number of flow entries that each extensibility flow table supports:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter OpenFlow instance view.	**openflow instance** *instance-id*	N/A
3. Configure the maximum number of extensibility flow entries.	**flow-entry max-limit** *limit-value*	By default, an OpenFlow extensibility flow table supports at most 3000 flow entries.

Configuring in-band management VLANs

In-band management VLANs of an OpenFlow instance are part of the VLANs associated with the OpenFlow instance. In-band management VLANs are used to establish connections between the OpenFlow instance and controllers in an OpenFlow instance.

When the in-band management VLANs are configured, the data packets within the in-band management VLANs are not forwarded through OpenFlow, and the ports that are assigned to only in-band management VLANs are not OpenFlow ports. Before configuring in-band management VLANs, you must plan the network.

To configure in-band management VLANs:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter OpenFlow instance view.	**openflow instance** *instance-id*	N/A
3. Configure in-band management VLANs.	**in-band management vlan** *vlan-list*	By default, no in-band management VLAN is configured. The in-band management VLANs of an OpenFlow instance must be within the list of the VLANs that are associated with the OpenFlow instance.

Disabling MAC address learning in the VLANs associated with an OpenFlow instance

This configuration does not take effect on in-band management VLANs.

To disable MAC address learning in the VLANs associated with an OpenFlow instance:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter OpenFlow instance view.	**openflow instance** *instance-id*	N/A

Step	Command	Remarks
3. Disable MAC address learning in the VLANs associated with an OpenFlow instance.	**mac-learning forbidden**	By default, MAC address learning is enabled in the VLANs associated with an OpenFlow instance.

Configuring the datapath ID for an OpenFlow instance

In an OpenFlow network, each OpenFlow instance is uniquely identified by a datapath ID. By default, the datapath ID of an OpenFlow instance consists of the instance ID and the bridge MAC address. The datapath ID is configurable.

To configure the datapath ID for an OpenFlow instance:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter OpenFlow instance view.	**openflow instance** *instance-id*	N/A
3. Configure the datapath ID for the OpenFlow instance.	**datapath-id** *datapath-id*	By default, the datapath ID of an OpenFlow instance consists of the instance ID and the bridge MAC address. The upper 16 bits are the instance ID and the lower 48 bits are the bridge MAC address.

Activating or reactivating an OpenFlow instance

CAUTION:

Reactivating an OpenFlow instance refreshes the configuration data and interrupts communication with the controllers.

To activate or reactivate an OpenFlow instance:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter OpenFlow instance view.	**openflow instance** *instance-id*	N/A
3. Activate or reactivate the OpenFlow instance.	**active instance**	By default, an OpenFlow instance is not activated.

Configuring controllers for an OpenFlow switch

Configuring controllers and main connections

An OpenFlow switch supports up to 64 controllers. However, the OpenFlow channel between the OpenFlow switch and each controller can have only one main connection, which uses TCP or SSL. The main connection must be reliable and processes control messages to complete tasks such as deploying entries, obtaining data, and sending information.

To specify a controller for an OpenFlow switch and configure the main connection to the controller:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter OpenFlow instance view.	**openflow instance** *instance-id*	N/A
3. Specify a controller and configure the main connection to the controller.	**controller** *id* **address** { **ip** *ip-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**ssl** *ssl-policy-name*]	By default, an OpenFlow instance is not configured with any main connection.

Setting the connection interruption mode

An OpenFlow switch is set to either of the following modes when it is disconnected from all controllers:

- **Secure**—In this mode, the OpenFlow switch forwards traffic based on flow tables and does not delete unexpired flow entries.
- **Standalone**—The OpenFlow switch uses the normal forwarding process.

To set the connection interruption mode for an OpenFlow switch:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter OpenFlow instance view.	**openflow instance** *instance-id*	N/A
3. Set the connection interruption mode.	**fail-open mode** { **secure** | **standalone** }	By default, the **secure** mode is used.

Setting OpenFlow timers

An OpenFlow switch supports the following timers:

- **Connection detection interval**—Interval at which the OpenFlow switch sends two consecutive Echo Request messages to a controller. The OpenFlow switch can send up to three Echo Request messages. If none of the requests received a reply, the OpenFlow switch is disconnected from the controller.
- **Reconnection interval**—Interval for the OpenFlow switch to wait before it attempts to reconnect to a controller.

To set OpenFlow timers for an OpenFlow switch:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter OpenFlow instance view.	**openflow instance** *instance-id*	N/A
3. Set the interval at which the OpenFlow switch sends two consecutive Echo Request messages to a controller.	**controller echo-request interval** *interval-value*	The default setting is 5 seconds. To reduce the CPU load, HP recommends that you set the interval for the OpenFlow switch to send two consecutive Echo Request messages to a large value.

Step	Command	Remarks
4. Set the reconnection interval.	**controller connect interval** *interval-value*	The default setting is 60 seconds.

Configuring OpenFlow to support dynamic MAC addresses

On an OpenFlow switch that supports MAC-IP flow tables, you can configure OpenFlow to support query and deletion of dynamic MAC addresses in the flow tables.

To configure OpenFlow to support dynamic MAC addresses:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter OpenFlow instance view.	**openflow instance** *instance-id*	N/A
3. Configure OpenFlow to support dynamic MAC addresses.	**mac-ip dynamic-mac aware**	By default, OpenFlow prohibits controllers from querying and deleting dynamic MAC addresses.

Displaying and maintaining OpenFlow

Task	Command	Remarks
Display the detailed information for an OpenFlow instance.	**display openflow instance** [*instance-id*]	Available in any view
Display flow table entries for an OpenFlow instance.	**display openflow instance** *instance-id* **flow-table** [*table-id*]	Available in any view
Display controller information for an OpenFlow instance.	**display openflow instance** *instance-id* **controller**	Available in any view
Display group table information for an OpenFlow instance.	**display openflow instance** *instance-id* **group** [*group-id*]	Available in any view
Display meter information for an OpenFlow instance.	**display openflow instance** *instance-id* **meter** [*meter-id*]	Available in any view
Display summary OpenFlow instance information.	**display openflow summary**	Available in any view

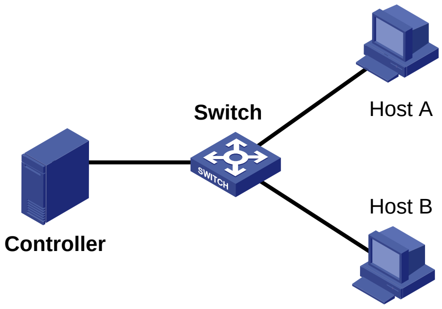
OpenFlow configuration example

Network requirements

As shown in Figure 7, perform the following configuration on the switch to enable OpenFlow communication with the controller in specific VLANs:

- Create OpenFlow instance 1, associate VLANs 4092 and 4094 with the OpenFlow instance, and activate the OpenFlow instance.
- Configure the controller's IP address to have the controller manage the OpenFlow switch.

Figure 7 Network diagram



Configuration procedure

Create VLANs 4092 and 4094.

```
<Switch> system-view
[Switch] vlan 4092
[Switch-vlan4092] quit
[Switch] vlan 4094
[Switch-vlan4092] quit
```

Create OpenFlow instance 1 and associate VLANs with it.

```
[Switch] openflow instance 1
[Switch-of-inst-1] classification vlan 4092 mask 4093
```

Specify a controller for the OpenFlow instance and activate the instance.

```
[Switch-of-inst-1] controller 1 address ip 192.168.49.49
[Switch-of-inst-1] active instance
```

Verifying the configuration

Display the detailed information for OpenFlow instance 1.

```
[Switch-of-inst-1] display openflow summary
Instance 1 information:

Configuration information:
 Description   : --
 Active status : active
 Inactive configuration:
  none
 Active configuration:
  Classification VLAN, total VLANs(2)
   4092, 4094
  In-band management VLAN, total VLANs(0)
   empty VLAN
  Connect mode: multiple
  Mac address learning: Enabled
  Flow table:
   Table ID(type): 0(Extensibility), count: 0
  Flow-entry max-limit: 3000
  Datapath ID: 0x00010cda415e232e
```

```
Port information:
 none
Active channel information:
 Failopen mode: secure
```

OpenFlow commands

active instance

Syntax

active instance

View

OpenFlow instance view

Default command level

2: System level

Description

Use **active instance** to activate or reactivate an OpenFlow instance.

By default, an OpenFlow instance is not activated.

An OpenFlow instance takes effect only after it is activated.

Reactivating an OpenFlow instance refreshes the configuration data and interrupts communication with the controllers.

Examples

Activate OpenFlow instance 1.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] active instance
```

classification vlan

Syntax

classification vlan *vlan-id* [**mask** *vlan-mask*] [**loosen**]

undo classification

View

OpenFlow instance view

Default command level

2: System level

Parameters

vlan-id: Specifies the VLAN ID in the range of 1 to 4094.

vlan-mask: Specifies a VLAN mask in the range of 0 to 4095. The default value is 4095.

loosen: Specifies the loosen mode for the OpenFlow instance-VLAN association.

Description

Use **classification vlan** to associate VLANs with an OpenFlow instance.

Use **undo classification** to cancel the association.

By default, an OpenFlow instance is not associated with any VLAN.

The system calculates the VLANs to be associated according to the specified VLAN ID and mask. To view the associated VLANs, use the **display openflow instance** command.

If you execute this command multiple times, the most recent configuration takes effect.

When the **loosen** keyword is specified, a port is an OpenFlow port only when the VLANs associated with the OpenFlow instance overlap with the VLANs permitted on the port.

When the **loosen** keyword is not specified, a port is an OpenFlow port only when the VLANs associated with the OpenFlow instance are a subset of the VLANs permitted on the port.

Examples

Associate an OpenFlow instance with a list of VLANs determined by VLAN ID 255 and VLAN mask 7.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] classification vlan 255 mask 7
```

Related commands

display openflow instance

controller address

Syntax

controller *controller-id* **address** { **ip** *ip-address* **|** **ipv6** *ipv6-address* } [**port** *port-number*] [**ssl** *ssl-policy-name*]

undo controller *controller-id* **address**

View

OpenFlow instance view

Default command level

2: System level

Parameters

Controller-id: Specifies a controller ID in the range of 0 to 63.

ip *ip-address*: Specifies the IPv4 address of the controller.

ipv6 *ipv6-address*: Specifies the IPv6 address of the controller.

port *port-number*: Sets the port number used to establish TCP connections to the controller. The value range of the port number is 0 to 65535. The default value is 6633.

ssl *ssl-policy-name*: Specifies the SSL client policy that the controller uses to authenticate the OpenFlow switch. The policy name is a case-insensitive string of 1 to 16 characters.

Description

Use **controller address** to specify a controller for an OpenFlow switch and configure the main connection to the controller.

Use **undo controller address** to remove the configuration.

By default, the main connection is not configured for an OpenFlow instance.

You can specify multiple controllers for an OpenFlow switch. The OpenFlow channel between the OpenFlow switch and each controller can have only one main connection.

The OpenFlow switch exchanges control messages with a controller through the main connection to:

- Receive flow table entries or data.
- Report information to the controller.

Examples

Specify controller 10 for OpenFlow instance 1. The controller's IP address is 1.1.1.1 and the port number is 6666.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] controller 10 address ip 1.1.1.1 port 6666
```

controller connect interval

Syntax

controller connect interval *interval-value*

undo controller connect interval

View

OpenFlow instance view

Default command level

2: System level

Parameters

interval-value: Sets a reconnection interval in seconds, in the range of 10 to 120.

Description

Use **controller connect interval** to set a reconnection interval for an OpenFlow switch.

Use **undo controller connect interval** to restore the default.

By default, the reconnection interval is 60 seconds.

The OpenFlow switch waits a reconnection interval before it attempts to reconnect to a controller.

Examples

Set the reconnection interval to 10 seconds for OpenFlow instance 1.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] controller connect interval 10
```

controller echo-request interval

Syntax

controller echo-request interval *interval-value*

undo controller echo-request interval

View

OpenFlow instance view

Default command level

2: System level

Parameters

interval-value: Sets a interval at which the OpenFlow switch sends two consecutive Echo Request messages to a controller in seconds. The value range is 1 to 10.

Description

Use **controller echo-request interval** to set an interval at which the OpenFlow switch sends two consecutive Echo Request messages to a controller.

Use **undo controller echo-request interval** to restore the default.

By default, the interval at which the OpenFlow switch sends two consecutive Echo Request messages to a controller is 5 seconds.

To reduce the CPU load, HP recommends that you set the interval for the OpenFlow switch to send two consecutive Echo Request messages to a large value.

Examples

Set the interval for OpenFlow instance 1 to send two consecutive Echo Request messages to 10 seconds.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] controller echo-request interval 10
```

controller mode

Syntax

controller mode { **multiple | single** }

undo controller mode

View

OpenFlow instance view

Default command level

2: System level

Parameters

multiple: Configures the connection mode as **multiple** for the OpenFlow instance to establish connections to controllers.

single: Configures the connection mode as **single** for the OpenFlow instance to establish connections to controllers.

Description

Use **controller mode** to configure the connection mode for an OpenFlow instance to establish connections to controllers.

Use **undo controller mode** to restore the default.

By default, the connection mode is **multiple**.

When the connection mode is **single**, an OpenFlow establishes a connection to only one controller at a time, and the other controllers back up the controller. When the connection is broken, the OpenFlow instance attempts to connect to the next controller until it successfully establishes a connection.

When the connection mode is **multiple**, an OpenFlow instance can establish connections to all controllers at a time. When one or more controllers fail or one or more controller connections are broken, the OpenFlow switch can operate correctly.

Examples

Configure the connection mode as **single** for OpenFlow instance 1.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] controller mode single
```

datapath-id

Syntax

datapath-id *datapath-id*

undo datapath-id

View

OpenFlow instance view

Default command level

2: System level

Parameters

datapath-id: Specifies the datapath ID for an OpenFlow instance. The argument is a hexadecimal number and the value range is 1 to 0xFFFFFFFFFFFFFFFF.

Description

Use **datapath-id** to configure the datapath ID for an OpenFlow instance.

Use **undo datapath-id** to restore the default.

By default, the datapath ID of an OpenFlow instance comprises the instance ID and the bridge MAC address. The upper 16 bits are the instance ID and the lower 48 bits are the bridge MAC address.

Examples

Set the datapath ID to 0x123456 for OpenFlow instance 1.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] datapath-id 123456
```

description

Syntax

description *text*

undo description

View

OpenFlow instance view

Default command level

2: System level

Parameters

text: Specifies description for the OpenFlow instance, which is a case-insensitive string of 1 to 255 characters and must start with an English letter.

Description

Use **description** to configure a description for an OpenFlow instance.

Use **undo description** to restore the default.

By default, an OpenFlow instance does not have a description.

Examples

Configure a description for OpenFlow instance 1 as **test-desc**.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] description test-desc
```

display openflow controller

Syntax

display openflow instance *instance-id* **controller** [*controller-id*]

View

Any view

Default command level

1: Monitor level

Parameters

instance-id: Specifies an OpenFlow instance ID in the range of 1 to 64.

controller-id: Specifies a controller by its ID in the range of 0 to 63. If no controller ID is specified, this command displays information about all controllers for an OpenFlow instance.

Description

Use **display openflow controller** to display controller information for an OpenFlow instance.

The controller information includes connection information and packet statistics.

Examples

Display controller information for OpenFlow instance 10.

```
<Sysname> display openflow instance 10 controller
Instance 10 controller information:
 Reconnect interval: 60 (s)
 Echo interval     : 5  (s)

 Controller ID           : 1
 Controller IP address   : 192.168.49.49
 Controller port         : 6633
 Controller role         : Equal
 Connect type            : TCP
 Connect state           : Established
 Packets sent            : 9
 Packets received        : 9
 SSL policy              : --
```

Table 3 Command output

Field	Description
Reconnect interval	Reconnection interval (in seconds) for an OpenFlow instance to re-connect to all controllers.

Field	Description
Echo interval	Interval (in seconds) at which an OpenFlow instance sends an Echo Request message to all controller.
Controller role	Role of the controller: • **Equal**—The controller has the same mode as other controllers that are specified for the OpenFlow instance. • **Master**—The controller is the master controller for the OpenFlow instance. • **Slave**—The controller is a slave controller for the OpenFlow instance. If the controller is not configured with any role, this field displays two hyphens (**--**).
Connect type	Type of the connection between the OpenFlow instance and the controller: **TCP** or **SSL**.
Connect state	State of the connection between the OpenFlow instance and the controller: **Idle** or **Established**.
Packets sent	Number of packets that have been sent to the controller.
Packets received	Number of packets that have been received from the controller.
SSL policy	Name of the SSL client policy used for SSL connections. If no SSL client policy controller is configured, this field displays two hyphens (**--**).

display openflow flow-table

Syntax

display openflow instance *instance-id* **flow-table** [*table-id*]

View

Any view

Default command level

1: Monitor level

Parameters

instance-id: Specifies an OpenFlow instance ID in the range of 1 to 64.

table-id: Specifies a flow table ID in the range of 0 to 254.

Description

Use **display openflow flow-table** to display flow table information for an OpenFlow instance.

If you do not specify the flow table ID, the command displays information about all flow tables for the specified OpenFlow instance.

Examples

Display information about all flow tables for OpenFlow instance 10.

```
<Sysname> display openflow instance 10 flow-table
Instance 10 flow table information:

Table 0 information:
 Table Type: MAC-IP, flow entry count: 1, total flow entry count: 2

MissRule (default) Flow entry information:
```

```
 cookie: 0x0, priority: 0, hard time: 0, idle time: 0, flags: reset_counts
 |no_pkt_counts|no_byte_counts, byte count: --, packet count: --
Match information: any
Instruction information:
 Write actions:
  Drop

Flow entry 1 information:
 cookie: 0x0, priority: 1, hard time: 0, idle time: 0, flags: none,
 byte count: --, packet count: --
Match information:
 Ethernet destination MAC address: 0000-0000-0001
 Ethernet destination MAC address mask: ffff-ffff-ffff
 VLAN ID: 100, mask: 0xfff
Instruction information:
 Write actions:
  Output interface: GE1/0/4
 Write metadata/mask: 0x0000000000000001/0xffffffffffffffff
 Goto table: 1

Table 1 information:
 Table Type: Extensibility, flow entry count: 2, total flow entry count: 2

MissRule (default)Flow entry information:
 cookie: 0x0, priority: 0, hard time: 0, idle time: 0, flags: none,
 byte count: --, packet count: 60
Match information: any
Instruction information:
 Write actions:
  Drop

Flow entry 1 information:
 cookie: 0x0, priority: 0, hard time: 0, idle time: 0, flags: flow_send_rem
 |check_overlap, byte count: --, packet count: 1
Match information:
 Input interface: GE1/0/3
 Ethernet source MAC address: 0000-0000-0001
 Ethernet source MAC address mask: ffff-ffff-ffff
Instruction information:
 Set meter: 100
 Apply actions:
  Output interface: GE1/0/4
 Write actions:
  Output interface: Controller, send length: 128 bytes
```

Table 4 Command output

Field	Description
Table Type	Type of the flow table: **MAC-IP** or **Extensibility**.

Field	Description
flow entry count	Number of flow entries deployed by controllers.
total flow entry count	Total number of flow entries in the table.
cookie	Cookie ID of the flow entry.
priority	Priority of the flow entry. The larger the value, the higher the priority.
hard time	Hard timeout of the flow entry, in seconds. The flow entry is aged out immediately after the hard timeout expires. If the flow entry has no hard timeout, the field displays **0**.
idle time	Idle timeout of the flow entry, in seconds. The flow entry is aged out if no packet matches the entry within the idle timeout. If the flow entry has no idle timeout, the field displays **0**.
flags	Flags that the flow entry includes: • **flow_send_rem**—Sends a flow removed message when the flow entry is removed or expires. • **check_overlap**—Checks for overlapping flow entries. • **reset_counts**—Resets flow table counters. • **no_pkt_counts**—Does not count packets. • **no_byte_counts**—Does not count bytes. If the flow entry does not include any flags, this field displays **none**.
byte count	Number of bytes that have matched the flow entry.
packet count	Number of packets that have matched the flow entry.
Match information	Contents in the Match field of the flow entry (see Table 5).
Instruction information	Contents in the Instruction field of the flow entry: • **Set meter**—Sends the matched packet to a specified meter. • **Write metadata/mask**—Writes the metadata value and mask into the metadata fields of the matched packet. • **Goto table**—Sends the matched packet to the next flow table for processing. • **Clear actions**—Clears all actions in the action set of the matched packet. • **Apply actions**—Applies specified actions in the action set of the matched packet. • **Write actions**—Writes specified actions into the action set of the matched packet. For more information about actions, see Table 6.

Table 5 Match information

Match field	Match field mask	Description
Input interface	N/A	Ingress port (see Table 7).
Physical input interface	N/A	Ingress physical port.

Match field	Match field mask	Description
Metadata	N/A	Meta data that is transmitted between flow tables. • **1**—Matches the destination MAC address in the metedata. • **2**—Matches the source MAC address in the metadata. • **4**—Matches the destination IP address in the metadata.
Ethernet destination MAC address	Mask	Ethernet destination MAC address and mask.
Ethernet source MAC address	Mask	Ethernet source MAC address and mask.
Ethernet type	N/A	Ethernet type of the OpenFlow packet payload.
VLAN ID	Mask	VLAN ID and mask.
VLAN PCP	N/A	VLAN priority.
IP DSCP	N/A	Differentiated Services Code Point (DSCP) value.
IP ECN	N/A	Explicit Congestion Notification (ECN) value in the IP header.
IP protocol	N/A	IPv4 or IPv6 protocol number.
IPv4 source address	Mask	IPv4 source address and mask.
IPv4 destination address	Mask	IPv4 destination address and mask.
TCP source port	Mask	TCP source port and mask.
TCP destination port	Mask	TCP destination port and mask.
UDP source port	Mask	UDP source port and mask.
UDP destination port	Mask	UDP destination port and mask.
ICMPv4 type	N/A	ICMPv4 type.
ICMPv4 code	N/A	ICMPv4 code.
ARP source IPv4 address	Mask	Sender IPv4 address and mask in the ARP payload.
ARP source MAC address	Mask	Sender MAC address and mask in the ARP payload.
IPv6 source address	Mask	Source IPv6 address and mask.
IPv6 destination address	Mask	Destination IPv6 address and mask.
IPv6 flow label	Mask	IPv6 flow label and mask.
ICMPv6 type	N/A	ICMPv6 type.
ICMPv6 code	N/A	ICMPv6 code.
IPv6 ND source MAC address	N/A	Source link-layer address in an IPv6 Neighbor Discovery message.
IPv6 ND target MAC address	N/A	Target link-layer address in an IPv6 Neighbor Discovery message.

Table 6 Actions

Field	Description
Drop	Drops the matched packet.
Output interface	Sends the packet through a specified port. For more information about ports, see Table 7.
send length	Specifies the length of bytes to be taken from the packet and be sent to the controller.
Group	Specifies a group to process the packet. This action is only applicable to HP 5500-24G EI Switch with 2 Interface Slots(JD377A), HP 5500-24G EI TAA Switch with 2 Interface Slots(JG250A), HP 5500-24G-SFP EI Switch with 2 Interface Slots(JD374A), HP 5500-24G-SFP EI TAA Switch with 2 Interface Slots(JG249A), HP 5500-24G-PoE+ EI Switch with 2 Interface Slots(JG241A) and HP 5500-24G-PoE+ EI TAA Switch with 2 Interface Slots(JG252A).
Set queue	Maps the flow entry to a queue specified by ID.
Set field	Modifies a specific field of the packet.

Table 7 Ports

Port name	Ingress port	Output port	Description
In_Port	Not supported.	Supported.	Ingress port of the packet.
Table	Not supported.	Supported.	Start flow table in the OpenFlow workflow.
Normal	Not supported.	Supported.	Normal forwarding workflow of the switch.
Flood	Not supported.	Supported.	Flooding workflow. This port name is only applicable to HP 5500-24G EI Switch with 2 Interface Slots(JD377A), HP 5500-24G EI TAA Switch with 2 Interface Slots(JG250A), HP 5500-24G-SFP EI Switch with 2 Interface Slots(JD374A), HP 5500-24G-SFP EI TAA Switch with 2 Interface Slots(JG249A), HP 5500-24G-PoE+ EI Switch with 2 Interface Slots(JG241A) and HP 5500-24G-PoE+ EI TAA Switch with 2 Interface Slots(JG252A).
All	Not supported.	Supported.	All ports. This port name is only applicable to HP 5500-24G EI Switch with 2 Interface Slots(JD377A), HP 5500-24G EI TAA Switch with 2 Interface Slots(JG250A), HP 5500-24G-SFP EI Switch with 2 Interface Slots(JD374A), HP 5500-24G-SFP EI TAA Switch with 2 Interface Slots(JG249A), HP 5500-24G-PoE+ EI Switch with 2 Interface Slots(JG241A) and HP 5500-24G-PoE+ EI TAA Switch with 2 Interface Slots(JG252A).
Controller	Supported.	Supported.	Channel connected to the controller.
Local	Supported.	Supported.	Local CPU.
Any	Not supported.	Not supported.	No port is specified. It cannot be ingress port or output port.
GE1/0/3 (port name)	Supported.	Supported.	Name of a physical or logical port.

display openflow group

Syntax

display openflow instance *instance-id* **group** [*group-id*]

View

Any view

Default command level

1: Monitor level

Parameters

instance-id: Specifies an OpenFlow instance by its ID in the range of 1 to 64.

group-id: Specifies a group entry by its ID in the range of 0 to 4294967040. If this argument is not specified, the command displays information about all group entries of the OpenFlow instance.

Description

Use **display openflow group** to display the group table information for an OpenFlow instance.

The group entries are referenced by flow entries to make the OpenFlow device support more packet forwarding functions, for example, multicast and broadcast. Each group table contains multiple action buckets. The actions in the buckets of a group entry are performed for packets matching the group entry.

You cannot configure group entries on the OpenFlow devices. Instead, you can configure group entries on the controller and issue the group entries to the OpenFlow device. Only HP 5500-24G EI Switch with 2 Interface Slots(JD377A), HP 5500-24G EI TAA Switch with 2 Interface Slots(JG250A), HP 5500-24G-SFP EI Switch with 2 Interface Slots(JD374A), HP 5500-24G-SFP EI TAA Switch with 2 Interface Slots(JG249A), HP 5500-24G-PoE+ EI Switch with 2 Interface Slots(JG241A) and HP 5500-24G-PoE+ EI TAA Switch with 2 Interface Slots(JG252A) support group tables.

Examples

Display the group table information for OpenFlow instance 10.

```
<Sysname> display openflow instance 10 group
Instance 10 group table information:
 Group count: 1

Group entry 4294967040:
 Type: All, byte count: 0, packet count: 0
 Bucket 1 information:
  Action count 1, watch port: GE1/0/1, watch group: 0
  Byte count 0, packet count 0
  Output interface: GE1/0/2
 Referenced information:
  Count: 1
  Flow table: 254
  Flow entry: 2
```

Table 8 Output description

Field	Description
Group count	Number of group entries contained in the OpenFlow instance.

Field	Description
Type	Group table type: **All**—Execute all buckets in the group. This group is used for multicast or broadcast forwarding.
bucket	Action buckets contained in the group table.
Action count	Number of actions in the action bucket.
Byte count	Number of bytes processed by the action bucket. Two hyphens (--) are displayed when the field is not supported.
packet count	Number of packets processed by the action bucket. Two hyphens (--) are displayed when the field is not supported.
watch port	Ports that affect the action bucket status.
watch group	Group table IDs of the ports that affect the action bucket status.
Output interface	Output interface in the group table.
Referenced information	Information about the flow entries referencing group entries.
Count	Number of flow entries that reference group entries.
Flow table	ID of the flow table to which the flow entries referencing the group entries belong.
Flow entry	IDs of flow entries referencing group entries.

display openflow instance

Syntax

display openflow instance [*instance-id*]

View

Any view

Default command level

1: Monitor level

Parameters

instance-id: Specifies an OpenFlow instance by its ID in the range of 1 to 64.

description

Use **display openflow instance** to display the detailed information for an OpenFlow instance.

Examples

Display the detailed information of OpenFlow instances.

```
<Sysname> display openflow instance
Instance 10 information:

Configuration information:
 Description   : test-desc
 Active status : active
 Inactive configuration:
  Classification VLAN, total VLANs(1)
   3
```

```
  Flow table:
   Table ID(type): 0(MAC-IP)
   Table ID(type): 1(Extensibility)
 Active configuration:
  Classification VLAN, loosen mode, total VLANs(1)
   2
  In-band management VLAN, total VLANs(0)
   empty VLAN
  Connect mode: multiple
  Mac address learning: Enabled
  Flow table:
   Table ID(type): 0(MAC-IP), count: 0
  Flow-entry max-limit: 3000
  Datapath ID: 0x0000001234567891
Port information:
 GigabitEthernet1/0/3
Active channel information:
 Controller 1 IP address: 192.168.49.49  port: 6633
 Controller 2 IP address: 192.168.43.49  port: 6633
```

Table 9 Command output

Field	Description
Description	Description of the OpenFlow instance.
Active status	Activation status of the OpenFlow instance.
Inactive configuration	Inactive OpenFlow instance configuration.
Active configuration	Active OpenFlow instance configuration.
Classification VLAN, loosen mode, total VLANs	VLANs associated with the OpenFlow instance, the total number of VLANs, and the loosen mode.
In-band management VLAN, total VLANs	In-band management VLANs and the total number of in-band management VLANs. **empty VLAN** is displayed when no in-band management VLAN is configured.
Connect mode	Connection mode for the OpenFlow instance to establish connections to controllers: • **multiple**—The connection mode is **multiple** for the OpenFlow instance to establish connections to controllers. • **single**—The connection mode is **single** for the OpenFlow instance to establish connections to controllers.
Mac-address learning	Whether MAC address learning is enabled in the VLANs associated with the OpenFlow instance: • **Enabled**—MAC address learning is enabled in the VLANs associated with the OpenFlow instance. • **Disabled**—MAC address learning is disabled in the VLANs associated with the OpenFlow instance.
Flow-entry max-limit	Maximum number of flow entries allowed in the extensibility flow table.
Datapath ID	Datapath ID of the OpenFlow instance.
Port information	Ports added to the OpenFlow instance.
Flow table	Flow table information of the OpenFlow instance.

Field	Description
Table ID(type)	Flow table ID (flow table type). The flow table type can be **MAC-IP** or **Extensibility**.
count	Total number of flow entries in the flow table.
Active channel information	Information about active control channels.
Controller id IP address: port:	Brief information of controllers which have established connections to the OpenFlow instance. This field is displayed only when the OpenFlow instance has established connections to controllers.
Failopen mode	Connection interruption mode when the OpenFlow instance is disconnected from all controllers (this field is displayed only when the OpenFlow instance is disconnected from all controllers): • **secure**—The OpenFlow switch uses flow tables for traffic forwarding after it is disconnected from all controllers. • **standalone**—The OpenFlow switch uses the normal forwarding process after it is disconnected from all controllers.

display openflow meter

Syntax

display openflow instance *instance-id* **meter** [*meter-id*]

View

Any view

Default command level

1: Monitor level

Parameters

instance-id: Specifies an OpenFlow instance by its ID in the range of 1 to 64.

meter-id: Specifies a meter by its ID in the range of 0 to 4294901760. If no meter ID is specified, this command displays information about all meter entries for an OpenFlow instance.

Description

Use **display openflow meter** to display meter entry information for an OpenFlow instance.

Examples

Display meter entry information for OpenFlow instance 10.

```
<Sysname> display openflow instance 10 meter
Meter flags: KBPS  -- Rate value in kb/s, PKTPS -- Rate value in packet/sec
             BURST -- Do burst size,      STATS -- Collect statistics

Instance 10 meter table information:
 meter entry count: 2

Meter entry 100 information:
 Meter flags: KBPS
 Band 1 information
 Type: drop, rate: 64kbps, burst size: 256kbps
 Byte count: --, packet count: 0
 Referenced information:
```

```
  Count: 3
  Flow table: 0
  Flow entry: 1, 2, 3

Meter entry 200 information:
 Meter flags: KBPS
 Band 1 information
 Type: drop, rate: 64kbps, burst size: 128kbps
 Byte count: --, packet count: 0
 Referenced information:
  Count: 0
```

Table 10 Command output

Field	Description
Group entry count	Total number of meter entries included in the OpenFlow instance.
Meter flags	Flags configured for the meter: • **KBPS**—The rate value is in kbps. • **PKTPS**—The rate value is in pps. • **BURST**—The burst size field in the band is used and the length of the packet or byte burst is determined by the burst size. • **STATS**—Meter statistics are collected.
Band	Bands included in the meter.
Type	Type of the band: • **drop**—Discard the packet. • **dscp remark**—Modify the drop precedence of the DSCP field in the IP header of the packet.
Rate	Rate value above which the corresponding band may apply to packets.
Burst size	Length of the packet or byte burst to consider for applying the meter.
Byte count	Number of bytes processed by a band. If this field is not supported, the field displays two hyphens (**--**).
packet count	Number of packets processed by a band. If this field is not supported, the field displays two hyphens (**--**).
Referenced information	Information about the meter entry referenced by flow entries.
Count	Total number of flow entries that reference the meter entry.
Flow table	Flow table to which the flow entries that reference the meter entry belong.
Flow entry	Flow entries that reference the meter entry.

display openflow summary

Syntax

display openflow instance summary

View

Any view

Default command level

1: Monitor level

Description

Use **display openflow summary** to display summary OpenFlow instance information, including OpenFlow instance ID, activation status, and datapath ID.

Examples

Display summary information about OpenFlow instances.

```
<Sysname> display openflow summary
Fail-open mode: Se - Secure mode, Sa - Standalone mode

ID     Status     Datapath-ID          Channel      Table-num  Port-num  Reactivate
1      Active     11000a0b0c0d0        Connected    2          8         Y
2      Active     21000a0b0c0d0        Connected    2          6         N
```

Table 11 Command output

Field	Description
ID	OpenFlow instance ID.
Status	Activation status of the OpenFlow instance: • **Active**—The OpenFlow instance is active. • **Inactive**—The OpenFlow instance is inactive.
Datapath-ID	Datapath ID of the OpenFlow instance. A hyphen (-) is displayed when the OpenFlow instance is inactive.
Channel	Status of the secure channel between the OpenFlow instance and the controller: • **Connected**—The secure channel between the OpenFlow instance and the controller has been established. • **Failed(Se)**—The secure channel between the OpenFlow instance and the controller has been disconnected, and the OpenFlow instance is operating in secure mode. • **Failed(Sa)**—The channel between the OpenFlow instance and the controller has been disconnected, and the OpenFlow instance is operating in standalone mode. A hyphen (-) is displayed when the OpenFlow instance is inactive.
Table-num	Number of flow tables in the OpenFlow instance. A hyphen (-) is displayed when the OpenFlow instance is inactive.
Port-num	Number of ports belonging to the OpenFlow instance. A hyphen (-) is displayed when the OpenFlow instance is inactive.
Reactivate	Indicates whether the OpenFlow instance needs to be reactivated: • **Y**—The OpenFlow instance needs to be reactivated. • **N**—The OpenFlow instance does not need to be reactivated. A hyphen (-) is displayed when the OpenFlow instance is inactive.

fail-open mode

Syntax

fail-open mode { **secure** | **standalone** }

undo fail-open mode

View

OpenFlow instance view

Default command level

2: System level

Parameters

secure: Configures the OpenFlow switch to use flow tables for traffic forwarding after it is disconnected from all controllers.

standalone: Configures the OpenFlow switch to use the normal forwarding process after it is disconnected from all controllers.

Description

Use **fail-open mode** to set the connection interruption mode for an OpenFlow switch.

Use **undo fail-open mode** to restore the default.

By default, the connection interruption mode is **secure**, and the controller deploys the table-miss flow entry (the action is **Drop**) to the OpenFlow instance.

Examples

Configure the connection interruption mode to **standalone** for OpenFlow instance 1.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] fail-open mode standalone
```

flow-entry max-limit

Syntax

flow-entry max-limit *limit-value*

undo flow-entry max-limit

View

OpenFlow instance view

Default command level

2: System level

Parameters

limit-value: Specifies the maximum number of flow entries, in the range of 1 to 3000.

Description

Use **flow-entry max-limit** to configure the maximum number of entries that every extensibility flow table can include.

Use **undo flow-entry max-limit** to restore the default.

By default, an extensibility flow table can include at most 3000 flow entries.

Examples

Configure OpenFlow instance 1 to include at most 256 entries in each extensibility flow table.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] flow-entry max-limit 256
```

flow-table

Syntax

flow-table { **extensibility** *extensibility-table-id* **|** **mac-ip** *mac-ip-table-id* }*

undo flow-table

View

OpenFlow instance view

Default command level

2: System level

Parameters

extensibility *extensibility-table-id*: Specifies an extensibility flow table ID in the range of 0 to 254.

mac-ip *mac-ip-table-id*: Specifies a MAC-IP flow table ID in the range of 0 to 254.

Description

Use **flow-table** to configure a flow table for an OpenFlow instance.

Use **undo flow-table** to restore the default.

By default, an OpenFlow instance has an extensibility flow table whose ID is 0.

You can specify only one MAC-IP flow table and one extensibility flow table for an OpenFlow instance, and the MAC-IP flow table ID must be smaller than the extensibility flow table ID.

Configure flow tables before you activate an OpenFlow instance.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure a MAC-IP flow table with ID 0 and an extensibility flow table with ID 1 for OpenFlow instance 1.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] flow-table mac-ip 0 extensibility 1
```

in-band management vlan

Syntax

in-band management vlan *vlan-list*

undo in-band management vlan

View

OpenFlow instance view

Default command level

2: System level

Parameters

vlan-list: Specifies a list of VLANs in the format of *vlan-list* = { *vlan-id1* [**to** *vlan-id2*] }<1-10>, where *vlan-id1* and *vlan-id2* are both in the range of 1 to 4094, *vlan-id2* cannot be smaller than *vlan-id1*, and <1-10> indicates that you can specify up to 10 *vlan-id1* [**to** *vlan-id2*] parameters.

Description

Use **in-band management vlan** to configure in-band management VLANs.

Use **undo in-band management vlan** to restore the default.

By default, no in-band management VLAN is configured.

The in-band management VLANs must be a subset of the VLANs associated with the OpenFlow instance.

Examples

Configure VLAN 10 as an in-band management VLAN in OpenFlow instance 1.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] in-band management vlan 10
```

mac-ip dynamic-mac aware

Syntax

mac-ip dynamic-mac aware

undo mac-ip dynamic-mac aware

View

OpenFlow instance view

Default command level

2: System level

Description

Use **mac-ip dynamic-mac aware** to configure OpenFlow to support dynamic MAC addresses.

Use **undo mac-ip dynamic-mac aware** to restore the default.

By default, an OpenFlow instance ignores dynamic MAC address messages sent from controllers.

When a MAC-IP flow table is configured for an OpenFlow switch, you can configure OpenFlow to support query and deletion of dynamic MAC addresses in the table.

When this command is configured, the OpenFlow switch does not send change events for the dynamic MAC addresses to controllers.

Examples

Configure OpenFlow instance 1 to support dynamic MAC addresses.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] mac-ip dynamic-mac aware
```

mac-learning forbidden

Syntax

mac-learning forbidden

undo mac-learning forbidden

View

OpenFlow instance view

Default command level

2: System level

Description

Use **mac-learning forbidden** to disable MAC address learning for the VLANs associated with the OpenFlow instance.

Use **undo mac-learning forbidden** to restore the default.

By default, MAC address learning is enabled in the VLANs associated with an OpenFlow instance.

Examples

Disable MAC address learning in the VLANs associated with OpenFlow instance 1.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] mac-learning forbidden
```

openflow instance

Syntax

openflow instance *instance-id*

undo openflow instance *instance-id*

View

System view

Default command level

2: System level

Parameters

instance-id: Specifies an OpenFlow instance ID in the range of 1 to 64.

Description

Use **openflow instance** to create an OpenFlow instance and enter OpenFlow instance view.

Use **undo openflow instance** to remove an OpenFlow instance.

By default, no OpenFlow instance exists.

Examples

Create OpenFlow instance 1, and enter the OpenFlow instance view.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1]
```

New feature: MFF

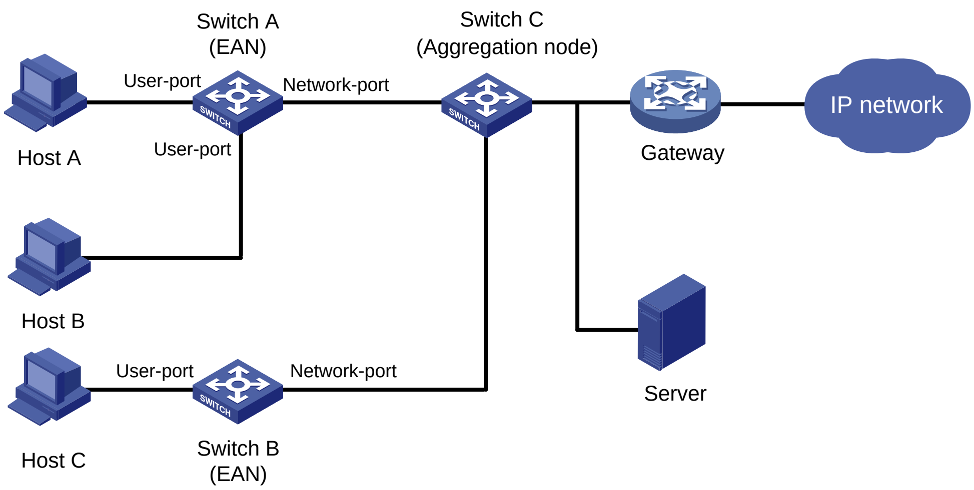
Overview

Traditional Ethernet networking solutions use the VLAN technology to isolate users at Layer 2 and to allow them to communicate at Layer 3. However, when a large number of hosts need to be isolated at Layer 2, many VLAN resources are occupied, and many IP addresses are used because you have to assign a network segment to each VLAN and an IP address to each VLAN interface for Layer 3 communication.

MAC-forced forwarding (MFF) provides a solution for Layer 2 isolation and Layer 3 communication between hosts in the same broadcast domain.

An MFF enabled device intercepts an ARP request and then returns the MAC address of a gateway (or server) to the sender. In this way, the sender is forced to send packets to the gateway for traffic monitoring and attack prevention.

Figure 8 Network diagram for MFF



As shown in Figure 8, hosts are connected to Switch C (aggregation node) through Switch A and Switch B (Ethernet access nodes, or EANs). The MFF enabled EANs forward packets from the hosts to the gateway for further forwarding. Thus, the hosts, isolated at Layer 2, can communicate at Layer 3 without knowing the MAC address of each other.

MFF is often used in cooperation with the DHCP snooping, ARP snooping, IP source guard, ARP detection, and VLAN mapping features to enhance network security by implementing traffic filtering, Layer 2 isolation, and Layer 3 communication on the access switches.

NOTE:

An MFF-enabled device and a host cannot ping each other.

Basic concepts

A device with MFF enabled provides two types of ports: user port and network port.

If you enable MFF for a VLAN, each port in the VLAN must be an MFF network or user port.

Link aggregation is supported by network ports in an MFF-enabled VLAN, but is not supported by user ports in the VLAN. You can add network ports to link aggregation groups, but cannot add user ports to link aggregation groups. For more information about link aggregation, see *Layer 2—LAN Switching Configuration Guide*.

User port

An MFF user port is directly connected to a host and processes the following packets differently:

- Allows DHCP packets and multicast packets to pass.
- Delivers ARP packets to the CPU.
- After learning gateways' MAC addresses, a user port allows only the unicast packets with the gateways' MAC addresses as the destination MAC addresses to pass. If no gateways' MAC addresses are learned, a user port discards all received unicast packets.

Network port

An MFF network port is connected to a networking device, such as an access switch, a distribution switch or a gateway. A network port processes the following packets differently:

- Allows multicast packets and DHCP packets to pass.
- Delivers ARP packets to the CPU.
- Denies broadcast packets.

You need to configure the following ports as network ports:

- Upstream ports connected to a gateway.
- Ports connected to the downstream MFF devices in a cascaded network (a network with multiple MFF devices connected to one another).
- Ports between devices in a ring network.

NOTE:

A network port is not always an upstream port.

Operation modes

Manual mode

The manual mode applies to the case where IP addresses are statically assigned to the hosts, and the hosts cannot obtain the gateway information through DHCP. A VLAN maintains only the MAC address of the default gateway.

In manual mode, after receiving an ARP request for a host's MAC address from the gateway, the MFF device directly replies the host's MAC address to the gateway according to the ARP snooping entries. The MFF device also forges ARP requests to get the gateway's MAC address based on ARP snooping entries.

After learning the gateway's MAC address and then receiving an ARP packet with a different source MAC address from the default gateway, the MFF device will replace the old MAC address with the new one.

Automatic mode

The automatic mode applies to the situation where hosts use DHCP to obtain IP addresses.

In MFF automatic mode, a VLAN can learn and maintain up to 20 gateways. The gateway IP addresses will not be updated, and the gateway information does not age out unless MFF is disabled.

With MFF automatic mode enabled, a DHCP snooping device, upon receiving a DHCP ACK message, resolves Option 3 in the message (Router IP option) to obtain a gateway for the client's IP-MAC snooping entry. If the DHCP ACK message contains multiple gateway addresses, only the first one is recorded for the entry. If the message contains no gateway IP address, the first gateway recorded by the current VLAN is used.

NOTE:

If the source MAC address of an incoming ARP packet from a gateway is different from that of the gateway, the MFF device uses the new MAC to replace the old one.

Working mechanism

Hosts connecting to an MFF device use the ARP fast-reply mechanism for Layer 3 communication. This mechanism helps reduce the number of broadcast messages.

The MFF device processes ARP packets in the following steps:

- After receiving an ARP request from a host, the MFF device sends the MAC address of the corresponding gateway to the host. In this way, hosts in the network have to communicate at Layer 3 through a gateway.

- After receiving an ARP request from a gateway, the MFF device sends the requested host's MAC address to the gateway if the corresponding entry is available; if the entry is not available, the MFF device will forward the ARP request.
- The MFF device forwards ARP replies between hosts and gateways.
- If the source MAC addresses of ARP requests from gateways are different from those recorded, the MFF device updates and broadcasts the IP and MAC addresses of the gateways.

Protocols and standards

RFC 4562, *MAC-Forced Forwarding*

Configuring MFF

Configuration prerequisites

- In MFF automatic mode, enable DHCP snooping on the device and configure DHCP snooping trusted ports.
- In MFF manual mode, enable ARP snooping on the device.

Enabling MFF

To enable MFF and specify an MFF operating mode:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter VLAN view.	**vlan** *vlan-id*	N/A
3. Enable MFF and specify an MFF operating mode.	**mac-forced-forwarding** { **auto** | **default-gateway** *gateway-ip* }	Disabled by default.

Configuring a network port

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter port view.	**interface** *interface-type interface-number*	N/A
3. Configure the port as a network port.	**mac-forced-forwarding network-port**	By default, the port is a user port.

Enabling periodic gateway probe

You can configure the MFF device to detect gateways periodically for the change of MAC addresses. This feature is supported by MFF manual mode and MFF automatic mode.

The time interval for sending gateway probes is 30 seconds. To get a gateway's MAC address, MFF in automatic mode uses the IP and MAC addresses of the first DHCP snooping entry corresponding to the gateway as the sender IP and MAC addresses of an ARP request, and sends the ARP request to the gateway. (In manual mode, MFF uses the IP and MAC addresses of the ARP snooping entry corresponding to the gateway.) After that, MFF will always use this entry to detect the gateway's MAC address, unless the entry is removed. If the entry is removed, MFF will look for another entry; if no other entry is found for the gateway, information about the gateway is removed.

To enable periodic gateway probe:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter VLAN view.	**vlan** *vlan-id*	N/A
3. Enable periodic gateway probe.	**mac-forced-forwarding gateway probe**	Disabled by default.

Specifying the IP addresses of servers

You need to maintain a server list on the MFF device. The list contains the IP addresses of servers in the network to ensure communication between the servers and clients.

You can specify a server's IP address in either manual or automatic MFF mode. The server can be a DHCP server, a server providing some other service, or the real IP address of a VRRP standby group. After you specify a server's IP address and then an ARP request from the server is received, the MFF device will search the IP-to-MAC address entries it has stored, and reply with the corresponding MAC address to the server. As a result, packets from a host to a server are forwarded by the gateway, but packets from a server to a host are not forwarded by the gateway.

To specify the IP addresses of servers:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter VLAN view.	**vlan** *vlan-id*	N/A
3. Specify the IP addresses of servers.	**mac-forced-forwarding server** *server-ip*&<1-10>	No server IP address is specified by default.

Displaying and maintaining MFF

<table>
<tr><th>Task</th><th>Command</th><th>Remarks</th></tr>
<tr><td>Display MFF port configuration information.</td><td>display mac-forced-forwarding interface [| { begin | exclude | include } regular-expression]</td><td>Available in any view</td></tr>
<tr><td>Display the MFF configuration information of a specified VLAN.</td><td>display mac-forced-forwarding vlan vlan-id [| { begin | exclude | include } regular-expression]</td><td>Available in any view</td></tr>
</table>

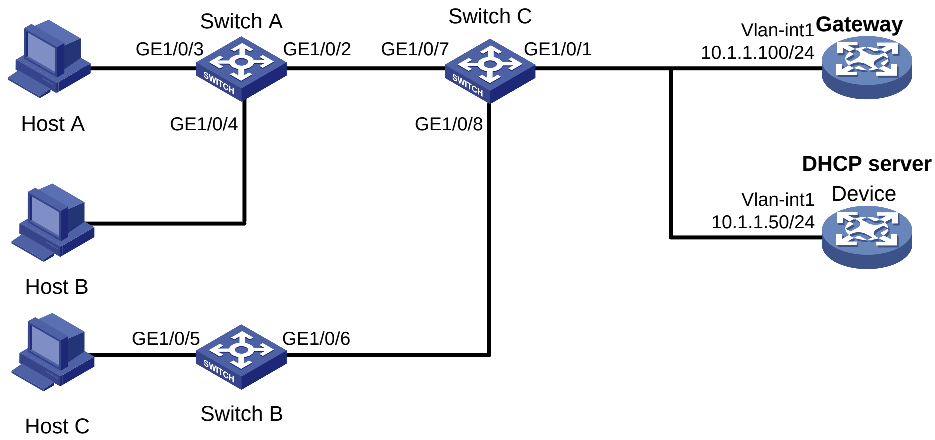
MFF configuration examples

Auto-mode MFF configuration example in a tree network

Network requirements

As shown in Figure 9, all the devices are in VLAN 100. Host A, Host B, and Host C obtain IP addresses from the DHCP server. They are isolated at Layer 2, and can communicate with each other through the gateway. MFF automatic mode is enabled on Switch A and Switch B.

Figure 9 Network diagram



Configuration procedure

1. Configure the IP address of VLAN-interface 1 on the gateway.

```
<Gateway> system-view
[Gateway] interface Vlan-interface 1
[Gateway-Vlan-interface1] ip address 10.1.1.100 24
```

2. Configure the DHCP server:

Enable DHCP, and configure a DHCP address pool.

```
<Device> system-view
[Device] dhcp enable
[Device] dhcp server ip-pool 1
[Device-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.0
```

Add the gateway's IP address into DHCP address pool 1.

```
[Device-dhcp-pool-1] gateway-list 10.1.1.100
[Device-dhcp-pool-1] quit
```

Configure the IP address of VLAN-interface 1.

```
[Device] interface Vlan-interface 1
[Device-Vlan-interface1] ip address 10.1.1.50 24
```

3. Configure Switch A:

Enable DHCP snooping.

```
<SwitchA> system-view
[SwitchA] dhcp-snooping
```

Enable MFF in automatic mode.

```
[SwitchA] vlan 100
[SwitchA-vlan-100] mac-forced-forwarding auto
[SwitchA-vlan-100] quit
```

Configure GigabitEthernet 1/0/2 as a network port.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] mac-forced-forwarding network-port
```

Configure GigabitEthernet 1/0/2 as a DHCP snooping trusted port.

```
[SwitchA-GigabitEthernet1/0/2] dhcp-snooping trust
```

4. Configure Switch B:

Enable DHCP snooping.

```
<SwitchB> system-view
[SwitchB] dhcp-snooping
```

Enable MFF in automatic mode.

```
[SwitchB] vlan 100
[SwitchB-vlan-100] mac-forced-forwarding auto
[SwitchB-vlan-100] quit
```

Configure GigabitEthernet 1/0/6 as a network port.

```
[SwitchB] interface gigabitethernet 1/0/6
[SwitchB-GigabitEthernet1/0/6] mac-forced-forwarding network-port
```

Configure GigabitEthernet 1/0/6 as a DHCP snooping trusted port.

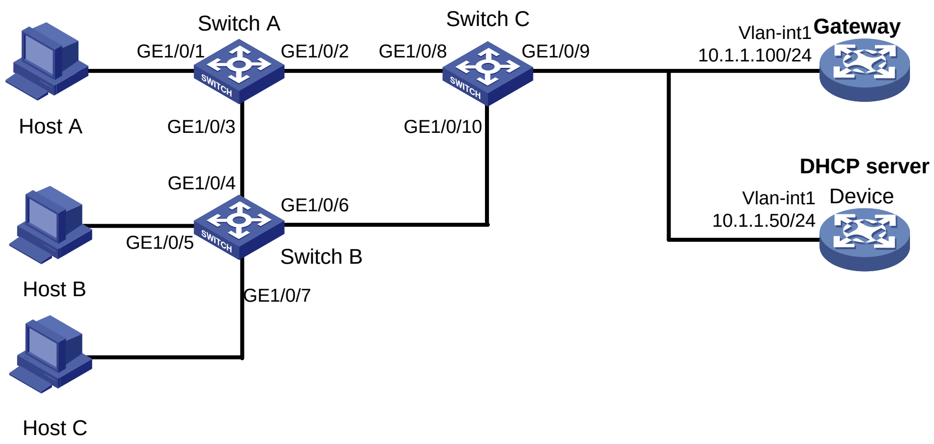
```
[SwitchB-GigabitEthernet1/0/6] dhcp-snooping trust
```

Auto-mode MFF configuration example in a ring network

Network requirements

As shown in Figure 10, all the devices are in VLAN 100, and the switches form a ring. Host A, Host B, and Host C obtain IP addresses from the DHCP server. They are isolated at Layer 2, and can communicate with each other through the gateway. MFF automatic mode is enabled on Switch A and Switch B.

Figure 10 Network diagram



Configuration procedure

1. Configure the IP address of VLAN-interface 1 on the gateway.

```
<Gateway> system-view
[Gateway] interface Vlan-interface 1
[Gateway-Vlan-interface1] ip address 10.1.1.100 24
```

2. Configure the DHCP server:

Enable DHCP and configure an address pool.

```
<Device> system-view
[Device] dhcp enable
[Device] dhcp server ip-pool 1
[Device-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.0
```

Add gateway's IP address into DHCP address pool 1.

```
[Device-dhcp-pool-1] gateway-list 10.1.1.100
[Device-dhcp-pool-1] quit
```

Configure the IP address of VLAN-interface 1.

```
[Device] interface Vlan-interface 1
[Device-Vlan-interface1] ip address 10.1.1.50 24
```

3. Configure Switch A:

Enable DHCP snooping.

```
<SwitchA> system-view
[SwitchA] dhcp-snooping
```

Enable STP.

```
[SwitchA] stp enable
```

Enable MFF in automatic mode.

```
[SwitchA] vlan 100
[SwitchA-vlan-100] mac-forced-forwarding auto
[SwitchA-vlan-100] quit
```

Configure GigabitEthernet 1/0/2 as a network port.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] mac-forced-forwarding network-port
```

Configure GigabitEthernet 1/0/2 as a DHCP snooping trusted port.

```
[SwitchA-GigabitEthernet1/0/2] dhcp-snooping trust
[SwitchA-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 as a network port.

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] mac-forced-forwarding network-port
```

Configure GigabitEthernet 1/0/3 as a DHCP snooping trusted port.

```
[SwitchA-GigabitEthernet1/0/3] dhcp-snooping trust no-user-binding
```

4. Configure Switch B:

Enable DHCP snooping.

```
<SwitchB> system-view
[SwitchB] dhcp-snooping
```

Enable STP.

```
[SwitchB] stp enable
```

Enable MFF in automatic mode.

```
[SwitchB] vlan 100
[SwitchB-vlan-100] mac-forced-forwarding auto
[SwitchB-vlan-100] quit
```

Configure GigabitEthernet 1/0/4 as a network port.

```
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] mac-forced-forwarding network-port
```

Configure GigabitEthernet 1/0/4 as a DHCP snooping trusted port.

```
[SwitchB-GigabitEthernet1/0/4] dhcp-snooping trust no-user-binding
[SwitchB-GigabitEthernet1/0/4] quit
```

Configure GigabitEthernet 1/0/6 as a network port.

```
[SwitchB] interface gigabitethernet 1/0/6
[SwitchB-GigabitEthernet1/0/6] mac-forced-forwarding network-port
```

Configure GigabitEthernet 1/0/6 as a DHCP snooping trusted port.

```
[SwitchB-GigabitEthernet1/0/6] dhcp-snooping trust
```

5. Enable STP on Switch C.

```
<SwitchC> system-view
```

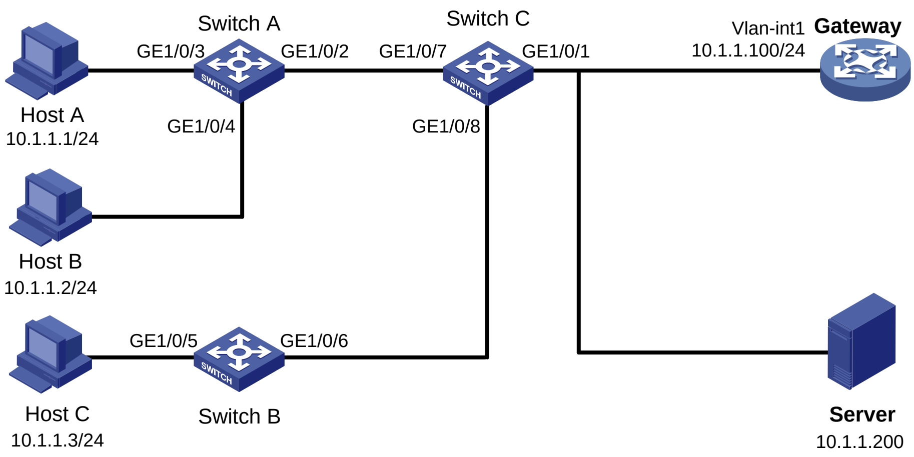
```
[SwitchC] stp enable
```

Manual-mode MFF configuration example in a tree network

Network requirements

As shown in Figure 11, all the devices are in VLAN 100. Host A, Host B, and Host C are configured with IP addresses manually. They are isolated at Layer 2, and can communicate with each other through the gateway. To ensure communication between hosts and the server, the IP address of the server is specified on the MFF devices manually.

Figure 11 Network diagram



Configuration procedure

1. Configure IP addresses of the hosts, as shown in Figure 11.
2. Configure the IP address of VLAN-interface 1 on the gateway.

```
<Gateway> system-view
[Gateway] interface Vlan-interface 1
[Gateway-Vlan-interface1] ip address 10.1.1.100 24
```

3. Configure Switch A:

Configure manual-mode MFF.

```
[SwitchA] vlan 100
[SwitchA-vlan-100] mac-forced-forwarding default-gateway 10.1.1.100
```

Specify the IP address of the server.

```
[SwitchA-vlan-100] mac-forced-forwarding server 10.1.1.200
```

Enable ARP snooping.

```
[SwitchA-vlan-100] arp-snooping enable
[SwitchA-vlan-100] quit
```

Configure GigabitEthernet 1/0/2 as a network port.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] mac-forced-forwarding network-port
```

4. Configure Switch B:

Configure manual-mode MFF.

```
[SwitchB] vlan 100
[SwitchB-vlan-100] mac-forced-forwarding default-gateway 10.1.1.100
```

Specify the IP address of the server.

```
[SwitchB-vlan-100] mac-forced-forwarding server 10.1.1.200
```

Enable ARP snooping.

```
[SwitchB-vlan-100] arp-snooping enable
[SwitchB-vlan-100] quit
```

Configure GigabitEthernet 1/0/6 as a network port.

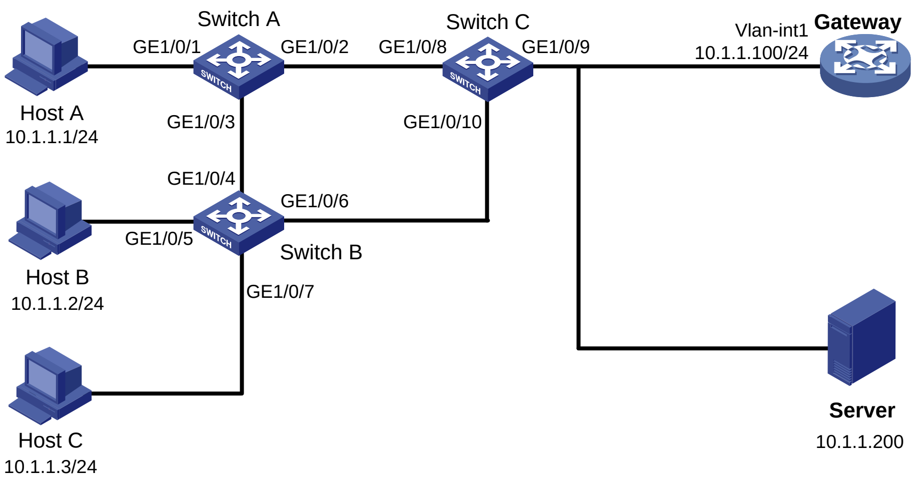
```
[SwitchB] interface gigabitethernet 1/0/6
[SwitchB-GigabitEthernet1/0/6] mac-forced-forwarding network-port
```

Manual-mode MFF configuration example in a ring network

Network requirements

As shown in Figure 12, all the devices are in VLAN 100, and the switches form a ring. Host A, Host B, and Host C are configured with IP addresses manually. They are isolated at Layer 2, and can communicate with each other through the gateway. To ensure communication between hosts and the server, the IP address of the server is specified on the MFF devices manually.

Figure 12 Network diagram



Configuration procedure

1. Configure IP addresses of the hosts, as in shown in Figure 12.
2. Configure the IP address of VLAN-interface 1 on the gateway.

```
<Gateway> system-view
[Gateway] interface Vlan-interface 1
[Gateway-Vlan-interface1] ip address 10.1.1.100 24
```

3. Configure Switch A:

Enable STP.

```
[SwitchA] stp enable
```

Configure manual-mode MFF.

```
[SwitchA] vlan 100
[SwitchA-vlan-100] mac-forced-forwarding default-gateway 10.1.1.100
```

Specify the IP address of the server.

```
[SwitchA-vlan-100] mac-forced-forwarding server 10.1.1.200
```

Enable ARP snooping.

```
[SwitchA-vlan-100] arp-snooping enable
[SwitchA-vlan-100] quit
```

Configure GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 as network ports.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] mac-forced-forwarding network-port
[SwitchA-GigabitEthernet1/0/2] quit
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] mac-forced-forwarding network-port
```

4. Configure Switch B:

   # Enable STP.

```
[SwitchB] stp enable
```

   # Configure manual-mode MFF.

```
[SwitchB] vlan 100
[SwitchB-vlan-100] mac-forced-forwarding default-gateway 10.1.1.100
```

   # Specify the IP address of the server.

```
[SwitchB-vlan-100] mac-forced-forwarding server 10.1.1.200
```

   # Enable ARP snooping.

```
[SwitchB-vlan-100] arp-snooping enable
[SwitchB-vlan-100] quit
```

   # Configure GigabitEthernet 1/0/4 and GigabitEthernet 1/0/6 as network ports.

```
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] mac-forced-forwarding network-port
[SwitchB- GigabitEthernet1/0/4] quit
[SwitchB] interface gigabitethernet 1/0/6
[SwitchB-GigabitEthernet1/0/6] mac-forced-forwarding network-port
```

5. Enable STP on Switch C.

```
<SwitchC> system-view
[SwitchC] stp enable
```

Command reference

display mac-forced-forwarding interface

Syntax

display mac-forced-forwarding interface [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display mac-forced-forwarding interface** to display MFF port configuration information.

Related commands: **mac-forced-forwarding network-port**.

Examples

Display MFF port configuration information.

```
<Sysname> display mac-forced-forwarding interface
Network Port:
  GE1/0/1                    GE1/0/2                    GE1/0/3
User Port:
  GE1/0/4                    GE1/0/5                    GE1/0/6
```

Table 12 Command output

Field	Description
Network Port	List of network ports.
User Port	List of user ports.

display mac-forced-forwarding vlan

Syntax

display mac-forced-forwarding vlan *vlan-id* [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

vlan-id: Specifies a VLAN by its number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display mac-forced-forwarding vlan** to display the MFF configuration information of a specified VLAN.

Related commands: **mac-forced-forwarding** and **mac-forced-forwarding server**.

Examples

Display the MFF configuration information of VLAN 1.

```
<Sysname> display mac-forced-forwarding vlan 1
VLAN 1
Mode: Auto/Single
Gateway:
-------------------------------------------------------------------------
192.168.1.42     (000f-e200-8046)

Server:
```

```
--------------------------------------------------------------------
192.168.1.48       192.168.1.49
```

Table 13 Command output

Field	Description
VLAN 1	ID of the VLAN to which the gateways belong.
Mode	MFF operating mode, which can be automatic (Auto), manual (Manual), and single-gateway (Single).
Gateway	IP and MAC addresses of gateways. If no information is learned, N/A is displayed.
Server	Server IP addresses.

mac-forced-forwarding

Syntax

mac-forced-forwarding { **auto** | **default-gateway** *gateway-ip* }

undo mac-forced-forwarding

View

VLAN view

Default level

2: System level

Parameters

auto: Specifies the automatic mode.

default-gateway *gateway-ip*: Specifies the IP address of the default gateway in the manual mode.

Description

Use **mac-forced-forwarding** to enable MFF and specify an MFF operating mode. To enable the manual mode, you need to specify a default gateway.

Use **undo mac-forced-forwarding** to disable MFF.

By default, MFF is disabled.

If you execute this command repeatedly, the last configuration takes effect.

If the automatic mode is specified, make sure that DHCP snooping works normally; if the manual mode is configured, make sure that ARP snooping works normally.

For a network (or VLAN) with IP addresses manually configured, the gateway IP address should be manually configured with the **mac-forced-forwarding default-gateway** *gateway-ip* command.

For a network (or VLAN) running DHCP, the gateway IP address can be manually configured with the **mac-forced-forwarding default-gateway** *gateway-ip* command, or can be resolved from the Option field in the DHCP messages.

Examples

Enable MFF in the automatic mode for VLAN 1.

```
<Sysname> system-view
[Sysname] vlan 1
[Sysname-vlan1] mac-forced-forwarding auto
```

mac-forced-forwarding gateway probe

Syntax

mac-forced-forwarding gateway probe

undo mac-forced-forwarding gateway probe

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **mac-forced-forwarding gateway probe** to enable periodic gateway MAC address probe. The probe interval is 30 seconds, and the probe mode can be manual or automatic.

Use **undo mac-forced-forwarding gateway probe** to restore the default.

By default, periodic gateway MAC address probe is disabled.

Make sure you have enabled MFF before enabling periodic gateway MAC address probe.

Examples

Enable periodic gateway MAC address probe.

```
<Sysname> system-view
[Sysname] vlan 1
[Sysname-vlan1] mac-forced-forwarding gateway probe
```

mac-forced-forwarding network-port

Syntax

mac-forced-forwarding network-port

undo mac-forced-forwarding network-port

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **mac-forced-forwarding network-port** to configure the Ethernet port as a network port.

Use **undo mac-forced-forwarding network-port** to restore the default.

By default, the port is a user port.

The upstream ports connecting to a gateway or the ports between devices in a ring network should be configured as network ports. You can configure multiple ports as network ports.

You can configure a port as a network port regardless of whether MFF is enabled for the VLAN of the port; however, the configuration takes effect only after MFF is enabled.

Link aggregation is supported by network ports in an MFF-enabled VLAN, but is not supported by user ports in the VLAN. If a network port is added to a link aggregation group belonging to an MFF-enabled VLAN, you need to remove the network port from the link aggregation group before you can cancel the network port configuration. For more information about link aggregation, see *Layer 2—LAN Switching Configuration Guide*.

Examples

Configure GigabitEthernet 1/0/1 as a network port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-forced-forwarding network-port
```

mac-forced-forwarding server

Syntax

mac-forced-forwarding server *server-ip*&<1-10>

undo mac-forced-forwarding server [*server-ip*&<1-10>]

View

VLAN view

Default level

2: System level

Parameters

server-ip&<1-10>: Specifies the IP address of a server in the network. &<1-10> means you can specify up to ten server IP addresses in one command line.

Description

Use **mac-forced-forwarding server** to specify the IP addresses of servers.

Use **undo mac-forced-forwarding server** to remove the specified or all server IP addresses.

By default, no server IP address is specified.

You can use this command (in either manual or automatic MFF operating mode) to specify the IP address of a DHCP server, the IP address of a server providing some other service, or the real IP address of a VRRP group.

If the MFF device receives an ARP request from a server, it will search the IP-to-MAC address entries it has stored, and reply the corresponding MAC address to the server. In this way, packets from a server to a host are not forwarded by the gateway, but packets from a host to a server are forwarded by the gateway.

MFF does not check whether the IP address of a server is on the same network segment as that of a gateway, but it checks whether the IP address of a server is all-zero or all-one. An all-zero or all-one server IP address is invalid.

If no server IP address is specified using this command, clients cannot communicate with any server.

Check that MFF is enabled before executing the **mac-forced-forwarding server** command.

If no IP address is specified in the **undo mac-forced-forwarding server** command, all specified server IP addresses are removed.

Examples

Specify the server at 192.168.1.100.

```
<Sysname> system-view
[Sysname] vlan 1
[Sysname-vlan1] mac-forced-forwarding server 192.168.1.100
```

Modified feature: Setting the device name

Feature change description

The allowed maximum device name length has changed.

Command changes

Modified command: sysname

Syntax

sysname *sysname*

Views

System view

Change description

Before modification: The device name can have 1 to 30 characters.

After modification: The device name can have 1 to 64 characters.

Modified feature: Displaying brief interface information

Feature change description

The **description** keyword was added to the **display interface** command.

If the interface description includes more than 27 characters and the **brief** keyword is specified for the **display interface** command, you can use the **description** keyword to display the full interface description for interfaces. The **display interface** command displays information about interfaces, such as Ethernet interfaces, aggregate interfaces, VLAN interfaces, loopback interfaces, and the null interface.

Command changes

Modified command: display interface

Old syntax

display interface [*interface-type*] [**brief** [**down**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

display interface *interface-type interface-number* [**brief**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

New syntax

display interface [*interface-type*] [**brief** [**down** | **description**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

display interface *interface-type interface-number* [**brief** [**description**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Change description

Before modification: The **display interface** command with the **brief** keyword specified displays at most the first 27 characters of an interface description.

After modification: If the interface description includes more than 27 characters and the **brief** keyword is specified for the **display interface** command, you must specify the **description** keyword to display the full description. Without the **description** keyword, the command displays only the first 27 characters.

Modified feature: Displaying brief IP configuration for Layer 3 interfaces

Feature change description

The **description** keyword was added to the **display interface brief** command.

If the interface description includes more than 12 characters, you can use this keyword to display the full interface description for Layer 3 interfaces.

Command changes

Modified command: display ip interface brief

Old syntax

display ip interface [*interface-type* [*interface-number*]] **brief** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

New syntax

display ip interface [*interface-type* [*interface-number*]] **brief** [**description**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Change description

Before modification: If the interface description includes more than 12 characters, only the first 9 characters of an interface description are displayed, followed by an ellipsis (…).

After modification: If the interface description includes more than 12 characters, you must specify the **description** keyword to display the full description. Without the **description** keyword, only the first 9 characters are displayed, followed by an ellipsis (...).

Modified feature: Configuring static multicast MAC address entries

Feature change description

In this release, you can configure a multicast MAC address in the value range of 0100-5Exx-xxxx and 3333-xxxx-xxxx in a static multicast MAC address entry. The x octet represents an arbitrary hexadecimal number from 0 to F.

The multicast MAC addresses used in protocol packets are in this multicast MAC adress range. If the multicast MAC address of a protocol packet matches a configured static multicast MAC address entry on the device, one of the following occurs:

- If the protocol packet needs to be processed by the CPU, the configuration of the static multicast MAC address entry does not take effect.
- If the protocol packet needs to be transparently transmitted by the device, the device forwards the packet through the outgoing port in the matching static multicast MAC address entry.

Command changes

Modified command: mac-address multicast

Syntax

In system view:

mac-address multicast *mac-address* **interface** *interface-list* **vlan** *vlan-id*

undo mac-address [**multicast**] [[*mac-address* [**interface** *interface-list*]] **vlan** *vlan-id*]

In Ethernet interface view or Layer 2 aggregate interface view:

mac-address multicast *mac-address* **vlan** *vlan-id*

undo mac-address [**multicast**] *mac-address* **vlan** *vlan-id*

In port group view:

mac-address multicast *mac-address* **vlan** *vlan-id*

undo mac-address multicast *mac-address* **vlan** *vlan-id*

Views

System view, Ethernet interface view, Layer 2 aggregate interface view, port group view

Change description

Before modification: The value of the *mac-address* argument is any legal multicast MAC address except 0100-5Exx-xxxx and 3333-xxxx-xxxx. A multicast MAC address is the MAC address in which the least signification bit of the most significant octet is 1.

After modification: The value of the *mac-address* argument is any legal multicast MAC address. A multicast MAC address is the MAC address in which the least signification bit of the most significant octet is 1.

Modified command: display mac-address multicast

Syntax

display mac-address [*mac-address* [**vlan** *vlan-id*] **|** [**multicast**] [**vlan** *vlan-id*] [**count**]] [**|** { **begin | exclude | include** } *regular-expression*]

Views

Any view

Change description

Before modification: The value of the *mac-address* argument is any legal multicast MAC address except 0100-5Exx-xxxx and 3333-xxxx-xxxx. A multicast MAC address is the MAC address in which the least signification bit of the most significant octet is 1.

After modification: The value of the *mac-address* argument is any legal multicast MAC address. A multicast MAC address is the MAC address in which the least signification bit of the most significant octet is 1.

Modified feature: Specifying the username and password to log in to the SCP server

Feature change description

Before you transfer files through SCP, you can log in to the SCP server by using one of the following methods for **password**, **password-publickey**, or **any** authentication:

- Entering the username and password as prompted
- Specifying the username and password in the **scp** command

Command changes

Modified command: SCP

Old syntax

In non-FIPS mode:

scp [**ipv6**] *server* [*port-number*] { **get** | **put** } *source-file-path* [*destination-file-path*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

In FIPS mode:

scp [**ipv6**] *server* [*port-number*] { **get** | **put** } *source-file-path* [*destination-file-path*] [**identity-key rsa** | **prefer-ctos-cipher** { **aes128** | **aes256** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** } | **prefer-kex dh-group14** | **prefer-stoc-cipher** { **aes128** | **aes256** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** }] *

New syntax

In non-FIPS mode:

scp [**ipv6**] *server* [*port-number*] { **get** | **put** } *source-file-path* [*destination-file-path*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **username** *username* **password** *password*] *

In FIPS mode:

scp [**ipv6**] *server* [*port-number*] { **get** | **put** } *source-file-path* [*destination-file-path*] [**identity-key rsa** | **prefer-ctos-cipher** { **aes128** | **aes256** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** } | **prefer-kex dh-group14** | **prefer-stoc-cipher** { **aes128** | **aes256** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** } | **username** *username* **password** *password*] *

Views

User view

Change description

Before modification: The **username** *username* **password** *password* option is not supported. You can enter the username and password only as prompted.

After modification: The **username** *username* **password** *password* option is supported. In addition to entering the username and password as prompted, you can also specify the username and password in the **scp** command.

The *username* argument specifies the username. It is a case-sensitive string of 1 to 80 characters.

The *password* argument specifies the password in plain text. It is a string of 1 to 63 characters.

Modified feature: Disabling an untrusted port from recording clients' IP-to-MAC bindings

Feature change description

In previous releases, you can disable only trusted ports from recording clients' IP-to-MAC bindings. In this release, both trusted and untrusted ports can be disabled from recording clients' IP-to-MAC bindings.

Command changes

Modified command: dhcp-snooping trust

Old syntax

dhcp-snooping trust [**no-user-binding**]

undo dhcp-snooping trust

New syntax

dhcp-snooping trust

undo dhcp-snooping trust

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Change description

Before modification: You can use the **dhcp-snooping trust** command to configure a port as a trusted port, and specify the **no-user-binding** keyword to disable the trusted port from recording clients' IP-to-MAC bindings. Untrusted ports on the DHCP snooping device always record clients' IP-to-MAC bindings, and this function cannot be disabled.

After modification: The **no-user-binding** keyword is removed from the **dhcp-snooping trust** command. You can use the new command **dhcp-snooping no-user-binding** to disable a port from recording clients' IP-to-MAC bindings. The port can be either a trusted port or an untrusted port.

New command: dhcp-snooping no-user-binding

Use **dhcp-snooping no-user-binding** to disable a port (either trusted or untrusted) from recording clients' IP-to-MAC bindings.

Use **undo dhcp-snooping no-user-binding** to restore the default.

Syntax

dhcp-snooping no-user-binding

undo dhcp-snooping no-user-binding

Default

With DHCP snooping enabled, all ports record clients' IP-to-MAC bindings.

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default command level

2: System level

Examples

Disable GigabitEthernet 1/0/1 from recording clients' IP-to-MAC bindings.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping no-user-binding
```

Modified feature: Customizing DHCP options

Feature change description

Changed the value range for the *code* argument.

Command changes

Modified command: option

Syntax

option *code* { **ascii** *ascii-string* **|** **hex** *hex-string*<1-16> **|** **ip-address** *ip-address*<1-8> }

undo option *code*

Views

DHCP address pool view

Change description

Before modification: The value range for the *code* argument is 2 to 254, excluding 12, 50 through 55, 57 through 61, and 82.

After modification: The value range for the code argument is 2 to 254, excluding 50 through 54, 58, 59, 61, and 82.

A5500EI-CMW520-R2220P11

This release has the following changes:

- Modified feature: ACL-based packet filtering on a VLAN interface

Modified feature: ACL-based packet filtering on a VLAN interface

Feature change description

In versions prior to Release 2220P11, the ACL applied to a VLAN interface filters packets forwarded at Layer 3. In Release 2220P11 and later versions, the ACL applied to a VLAN interface filters packets forwarded at Layer 3 and packets forwarded at Layer 2.

Command changes

Modified command: packet-filter

Syntax

packet-filter { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

Views

Interface view

Change description

Before modification, the ACL applied to a VLAN interface filters packets forwarded at Layer 3.

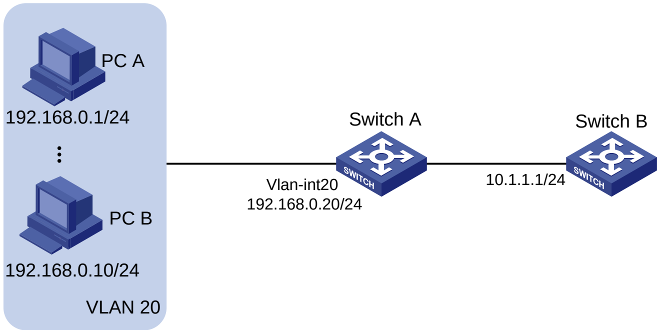
After modification, the ACL applied to a VLAN interface filters packets forwarded at Layer 3 and packets forwarded at Layer 2.

Examples

As shown in Figure 1, configure packet filtering on Switch A to meet the following requirements:

- Allow only packets from PC A to Switch B to pass through.
- Allow PC A and PC B to communicate at Layer 2.

Figure 1 Network diagram



- In versions before Release 2220P11, the configuration on Switch A is as follows:

```
<SwitchA>system-view
```

```
System View: return to User View with Ctrl+Z.
[SwitchA]acl number 3000
[SwitchA-acl-adv-3000]rule permit ip source 192.168.0.1 0 destination 10.1.1.1
0.0.0.255
[SwitchA-acl-adv-3000]rule deny ip
[SwitchA-acl-adv-3000]quit
[SwitchA]interface Vlan-interface 20
[SwitchA-Vlan-interface20]packet-filter 3000 inbound
```

Because the ACL does not take effect on packets forwarded at Layer 2, you just need to configure two rules in the following order:

a. A permit rule that permits packets from PC A to Switch B.

b. A deny rule that denies all packets.

- In Release 2220P11 and later versions, the configuration on Switch A is as follows:

```
<SwitchA>system-view
System View: return to User View with Ctrl+Z.
[SwitchA]acl number 3000
[SwitchA-acl-adv-3000]rule permit ip source 192.168.0.1 0 destination 10.1.1.1
0.0.0.255
[SwitchA-acl-adv-3000]rule permit ip source 192.168.0.1 0.0.0.255 destination
192.168.0.10 0.0.0.255
[SwitchA-acl-adv-3000]rule deny ip
[SwitchA-acl-adv-3000]quit
[SwitchA]interface Vlan-interface 20
[SwitchA-Vlan-interface20]packet-filter 3000 inbound
```

Because the ACL takes effect on packets forwarded at Layer 3 and packets forwarded at Layer 2, you need to configure one more permit rule to permit packets from PC A to PC B. Configure the rules in the following order:

a. A permit rule that permits packets from PC A to Switch B.

b. A permit rule that permits packets from PC A to PC B.

c. A deny rule that denies all packets.

A5500EI-CMW520-R2220P10

This release has the following changes:

- Modified feature: Specifying multiple public keys for an SSH user

Modified feature: Specifying multiple public keys for an SSH user

Feature change description

When the SSH server uses the digital signature to authentication an SSH user, up to six public keys can be assigned to the user. The SSH server authenticates the user through the first matching public key.

Command changes

Modified command: ssh user

Old syntax

In non-FIPS mode:

ssh user *username* **service-type stelnet authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* }

ssh user *username* **service-type** { **all** | **scp** | **sftp** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* **work-directory** *directory-name* }

undo ssh user *username*

In FIPS mode:

ssh user *username* **service-type stelnet authentication-type** { **password** | **password-publickey assign publickey** *keyname* }

ssh user *username* **service-type** { **all** | **scp** | **sftp** } **authentication-type** { **password** | **password-publickey assign publickey** *keyname* **work-directory** *directory-name* }

undo ssh user *username*

New syntax

In non-FIPS mode:

ssh user *username* **service-type stelnet authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname*&<1-6> }

ssh user *username* **service-type** { **all** | **scp** | **sftp** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname*&<1-6> **work-directory** *directory-name* }

undo ssh user *username*

In FIPS mode:

ssh user *username* **service-type stelnet authentication-type** { **password** | **password-publickey assign publickey** *keyname*&<1-6> }

ssh user *username* **service-type** { **all** | **scp** | **sftp** } **authentication-type** { **password** | **password-publickey assign publickey** *keyname*&<1-6> **work-directory** *directory-name* }

undo ssh user *username*

Views

System view

Change description

Before modification: You can assign only one public key to an SSH user. The **assign publickey** *keyname* option is used to specify this public key.

After modification: You can assign multiple public keys to an SSH user. The **assign publickey** *keyname*&<1-6> option is used to specify these public keys, and &<1-6> indicates that up to six public keys can be specified. When multiple public keys are used, the SSH server authenticates the user through the first matching public key.

A5500EI-CMW520-R2220P09

This release has the following changes:

- Modified feature: Specifying multiple secondary HWTACACS servers

Modified feature: Specifying multiple secondary HWTACACS servers

Feature change description

In this release, you can specify one primary HWTACACS server and up to 16 secondary HWTACACS servers in the same HWTACACS scheme. When the primary HWTACACS server is unreachable, the device uses a secondary HWTACACS server to process AAA requests.

You can configure a shared key for each HWTACACS server, primary or secondary. The device uses the shared keys to ensure secure communication with HWTACACS servers.

Command changes

Modified command: primary accounting

Old syntax

primary accounting *ip-address* [*port-number* **|** **vpn-instance** *vpn-instance-name*] *

undo primary accounting

New syntax

primary accounting *ip-address* [*port-number* **|** **key** [**cipher** **|** **simple**] *key* **|** **vpn-instance** *vpn-instance-name*] *

undo primary accounting

Views

HWTACACS scheme view

Change description

The **key** [**cipher** **|** **simple**] *key* part is added to the **primary accounting** command. You can specify a shared key for secure communication between the device and the primary HWTACACS accounting server. Make sure the shared key configured on the device is the same as the one configured on the server.

- **cipher** *key*: Sets a ciphertext shared key. The *key* argument is case sensitive.
  - In non-FIPS mode, the key is a string of 1 to 373 characters.
  - In FIPS mode, the key is a string of 8 to 373 characters.
- **simple** *key*: Sets a plaintext shared key. The *key* argument is case sensitive.
  - In non-FIPS mode, the key is a string of 1 to 255 characters.
  - In FIPS mode, the key is a string of 8 to 255 characters and must contain digits, uppercase letters, lowercase letters, and special characters.

NOTE:

If you specify neither the **cipher** keyword nor the **simple** keyword, the shared key is set in plain text.

Modified command: primary authentication

Old syntax

primary authentication *ip-address* [*port-number* **| vpn-instance** *vpn-instance-name*] *

undo primary authentication

New syntax

primary authentication *ip-address* [*port-number* **| key** [**cipher | simple**] *key* **| vpn-instance** *vpn-instance-name*] *

undo primary authentication

Views

HWTACACS scheme view

Change description

The **key** [**cipher | simple**] *key* part is added to the **primary authentication** command. You can specify a shared key for secure communication between the device and the primary HWTACACS authentication server. Make sure the shared key configured on the device is the same as the one configured on the server.

- **cipher** *key*: Sets a ciphertext shared key. The *key* argument is case sensitive.
  - In non-FIPS mode, the key is a string of 1 to 373 characters.
  - In FIPS mode, the key is a string of 8 to 373 characters.
- **simple** *key*: Sets a plaintext shared key. The *key* argument is case sensitive.
  - In non-FIPS mode, the key is a string of 1 to 255 characters.
  - In FIPS mode, the key is a string of 8 to 255 characters and must contain digits, uppercase letters, lowercase letters, and special characters.

NOTE:

If you specify neither the **cipher** keyword nor the **simple** keyword, the shared key is set in plain text.

Modified command: primary authorization

Old syntax

primary authorization *ip-address* [*port-number* **| vpn-instance** *vpn-instance-name*] *

undo primary authorization

New syntax

primary authorization *ip-address* [*port-number* **| key** [**cipher | simple**] *key* **| vpn-instance** *vpn-instance-name*] *

undo primary authorization

Views

HWTACACS scheme view

Change description

The **key** [**cipher | simple**] *key* part is added to the **primary authorization** command. You can specify a shared key for secure communication between the device and the primary HWTACACS authorization server. Make sure the shared key configured on the device is the same as the one configured on the server.

- **cipher** *key*: Sets a ciphertext shared key. The *key* argument is case sensitive.
  - In non-FIPS mode, the key is a string of 1 to 373 characters.
  - In FIPS mode, the key is a string of 8 to 373 characters.
- **simple** *key*: Sets a plaintext shared key. The *key* argument is case sensitive.
  - In non-FIPS mode, the key is a string of 1 to 255 characters.
  - In FIPS mode, the key is a string of 8 to 255 characters and must contain digits, uppercase letters, lowercase letters, and special characters.

NOTE:

If you specify neither the **cipher** keyword nor the **simple** keyword, the shared key is set in plain text.

Modified command: secondary accounting

Old syntax

secondary accounting *ip-address* [*port-number* | **vpn-instance** *vpn-instance-name*] *

undo secondary accounting

New syntax

secondary accounting *ip-address* [*port-number* | **key** [**cipher** | **simple**] *key* | **vpn-instance** *vpn-instance-name*] *

undo secondary accounting [*ip-address*]

Views

HWTACACS scheme view

Change description

This command has the following modifications:

- The **key** [**cipher** | **simple**] *key* part is added to the **secondary accounting** command. You can use this command to specify a shared key for secure communication between the device and a secondary HWTACACS accounting server. Make sure the shared key configured on the device is the same as the one configured on that server.
  - **cipher** *key*: Sets a ciphertext shared key. The *key* argument is case sensitive.
    - In non-FIPS mode, the key is a string of 1 to 373 characters.
    - In FIPS mode, the key is a string of 8 to 373 characters.
  - **simple** *key*: Sets a plaintext shared key. The *key* argument is case sensitive.
    - In non-FIPS mode, the key is a string of 1 to 255 characters.
    - In FIPS mode, the key is a string of 8 to 255 characters and must contain digits, uppercase letters, lowercase letters, and special characters.

NOTE:

If you specify neither the **cipher** keyword nor the **simple** keyword, the shared key is set in plain text.

- The *ip-address* argument is added to the **undo secondary accounting** command. You can remove a secondary HWTACACS accounting server with this command by specifying its IP address.

Modified command: secondary authentication

Old syntax

secondary authentication *ip-address* [*port-number* | **vpn-instance** *vpn-instance-name*] *

undo secondary authentication

New syntax

secondary authentication *ip-address* [*port-number* | **key** [**cipher** | **simple**] *key* | **vpn-instance** *vpn-instance-name*] *

undo secondary authentication [*ip-address*]

Views

HWTACACS scheme view

Change description

This command has the following modifications:

- The **key** [**cipher | simple**] *key* part is added to the **secondary authentication** command. You can specify a shared key for secure communication between the device and a secondary HWTACACS authentication server. Make sure the shared key configured on the device is the same as the one configured on the server.
  - **cipher** *key*: Sets a ciphertext shared key. The *key* argument is case sensitive.
    - In non-FIPS mode, the key is a string of 1 to 373 characters.
    - In FIPS mode, the key is a string of 8 to 373 characters.
  - **simple** *key*: Sets a plaintext shared key. The *key* argument is case sensitive.
    - In non-FIPS mode, the key is a string of 1 to 255 characters.
    - In FIPS mode, the key is a string of 8 to 255 characters and must contain digits, uppercase letters, lowercase letters, and special characters.

NOTE:

If you specify neither the **cipher** keyword nor the **simple** keyword, the shared key is set in plain text.

- The *ip-address* argument is added to the **undo secondary authentication** command. You can remove a secondary HWTACACS authentication server with this command by specifying its IP address.

Modified command: secondary authorization

Old syntax

secondary authorization *ip-address* [*port-number* | **vpn-instance** *vpn-instance-name*] *

undo secondary authorization

New syntax

secondary authorization *ip-address* [*port-number* | **key** [**cipher** | **simple**] *key* | **vpn-instance** *vpn-instance-name*] *

undo secondary authorization [*ip-address*]

Views

HWTACACS scheme view

Change description

This command has the following modifications:

- The **key** [**cipher** | **simple**] *key* part is added to the **secondary authorization** command. You can specify a shared key for secure communication between the device and a secondary HWTACACS authorization server. Make sure the shared key configured on the device is the same as the one configured on the server.
    - **cipher** *key*: Sets a ciphertext shared key. The *key* argument is case sensitive.
        - In non-FIPS mode, the key is a string of 1 to 373 characters.
        - In FIPS mode, the key is a string of 8 to 373 characters.
    - **simple** *key*: Sets a plaintext shared key. The *key* argument is case sensitive.
        - In non-FIPS mode, the key is a string of 1 to 255 characters.
        - In FIPS mode, the key is a string of 8 to 255 characters and must contain digits, uppercase letters, lowercase letters, and special characters.

NOTE:

If you specify neither the **cipher** keyword nor the **simple** keyword, the shared key is set in plain text.

- The *ip-address* argument is added to the **undo secondary authorization** command. You can remove a secondary HWTACACS authorization server with this command by specifying its IP address.

A5500EI-CMW520-R2220P07

This release has the following changes:

- New feature: Configuring the ARP detection logging function
- Modified feature: CWMP

New feature: Configuring the ARP detection logging function

The ARP detection logging function enables a device to generate ARP detection log messages when ARP packet attacks are detected. An ARP detection log message can include the following information:

- Receiving interface of the ARP packets.
- Sender IP address.
- Total number of ARP packets dropped.

The following is an example of an ARP detection log message:

Detected an inspection occurred on interface GigabitEthernet 1/0/1 with IP address 172.18.48.55 (Totally 10 packets dropped).

Configuring the ARP detection logging function

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. (Optional) Enable the ARP detection logging function.	**arp detection log enable**	By default, the ARP detection logging function is enabled.

Command reference

arp detection log enable

Use **arp detection log enable** to enable logging for ARP detection.

Use **undo detection log enable** to disable the logging function for ARP detection

Syntax

arp detection log enable

undo arp detection log enable

Default

Logging is enabled for ARP detection

View

System view

Default level

3: Manage level

Examples

Enable logging for ARP detection.

```
<Sysname> system-view
[Sysname] arp detection enable
```

Modified feature: CWMP

Feature change description

The following changes to file upload were introduced:

- In addition to the authentication performed during CWMP connection setup, the CPE must pass a file transfer authentication before it can upload a file to the ACS.
- The CPE uses HTTPS or HTTP to upload files.

Command changes

None.

A5500EI-CMW520-R2220L06

This chapter includes following contents:

New feature: 802.1X-based dynamic IPv4 source guard binding entries

Overview

To protect 802.1X users from IP attacking, you can enable 802.1X to cooperate with IP source guard. This IP source guard feature generates dynamic IPv4 source guard binding entries based on 802.1X secure entries. It can filter out IPv4 packets from unauthenticated 802.1X users.

To deny any online authenticated 802.1X users to change their IP addresses, you can enable the 802.1X IP freezing function on the authentication port. The port saves the IP addresses of 802.1X users when they get online, and it does not update these IP addresses even if the IP addresses of these users have changed. If an online authenticated 802.1X user changes its IP address, the port denies the user to access the network, because the user's IP address does not match any IPv4 source guard binding entries.

Configuration procedure

Configuration task list

Task	Remarks
Enabling 802.1X	For more information about 802.1X, see *Security Configuration Guide*.
Enabling the 802.1X IP freezing function	Optional.
Enabling a port to generate 802.1X-based dynamic IPv4 source guard binding entries	N/A
Enabling the IPv4 source guard function on an interface	See the **ip verify source** { **ip-address** | **ip-address mac-address** | **mac-address** } command. For more information about IP source guard, see *Security Configuration Guide*.

Enabling the 802.1X IP freezing function

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step		Command	Remarks
2.	Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3.	Enable the 802.1X IP freezing function.	**dot1x user-ip freeze**	By default, the port saves the IP address received from an 802.1X user and updates the IP address when it receives a different IP address from the same user.

Enabling a port to generate 802.1X-based dynamic IPv4 source guard binding entries

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3.	Enable the port to generate 802.1X-based dynamic IPv4 source guard binding entries.	**ip verify source dot1x**	By default, this function is disabled.

NOTE:

If the 802.1X client does not upload users' IP addresses to the device, you must enable DHCP snooping or ARP snooping on the device. Then 802.1X can obtain the IP addresses of 802.1X users for the device to generate 802.1X-based dynamic IP source guard binding entries.

Command reference

dot1x user-ip freeze

Syntax

dot1x user-ip freeze

undo dot1x user-ip freeze

View

Layer 2 Ethernet interface view

Default level

2: System level

Description

Use **dot1x user-ip freeze** to enable the 802.1X IP freezing function.

Use **undo dot1x user-ip freeze** to restore the default.

By default, a port saves the IP address received from an 802.1X user and updates the IP address when it receives a different IP address from the same user.

Examples

Enable 802.1X IP freezing on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x user-ip freeze
```

ip verify source dot1x

Syntax

ip verify source dot1x

undo ip verify source dot1x

View

Layer 2 Ethernet interface view

Default level

2: System level

Description

Use **ip verify source dot1x** to enable a port to generate 802.1X-based dynamic IPv4 source guard binding entries.

Use **undo ip verify source dot1x** to remove the 802.1X-based dynamic IPv4 source guard binding entries.

By default, a Layer 2 Ethernet port generates dynamic IPv4 source guard binding entries based on DHCP snooping.

Executing the **undo ip verify source dot1x** command or disabling 802.1X on the port will remove all 802.1X-based dynamic IPv4 source guard binding entries on the port.

The port will remove the dynamic IPv4 source guard binding entry of an 802.1X user after the user gets offline.

Example

Enable port GigabitEthernet 1/0/1 to generate 802.1X-based dynamic IPv4 source guard binding entries.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip verify source dot1x
```

New feature: Multicast ND

Configuring multicast ND

Microsoft NLB is a load balancing technology for server clustering developed on Windows Server.

NLB supports load sharing and redundancy among servers within a cluster. To implement fast failover, NLB requires that the switch forwards network traffic to all servers or specified servers in the cluster, and each server filters out unexpected traffic. In a medium or small data center that uses the Windows Server operating system, the proper cooperation of the switch and NLB is very important. For more information about NLB, see the related documents for Windows Server.

Microsoft NLB provides the following packet sending modes to make the switch forward network traffic to all servers or specified servers:

- **Unicast mode**—NLB assigns each cluster member a common MAC address, which is the cluster MAC address, and changes the source MAC address of each sent packet. The switch cannot add the cluster MAC address to its MAC table. In addition, because the cluster MAC address is unknown to the switch, packets destined to it are forwarded on all ports of the switch.

- **Multicast mode**—NLB uses a multicast MAC address that is a virtual MAC address for network communication (for example 0300-5e11-1111).
- **Internet Group Management Protocol (IGMP) multicast mode**—The switch sends packets only out of the ports that connect to the cluster members rather than all ports.

NOTE:

Multicast ND is applicable to only multicast-mode NLB.

To configure multicast ND:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure a static neighbor entry.	**ipv6 neighbor** *ipv6-address mac-address vlan-id port-type port-number* [**vpn-instance** *vpn-instance-name*]	Optional.
3. Configure a static multicast MAC address entry.	**mac-address multicast** *mac-address* **interface** *interface-list* **vlan** *vlan-id*	No static multicast MAC address entries exist by default.

Command reference

For more information about the **mac-address multicast** command, see "IGMP Snooping Commands" in *HP A5500 EI & A5500 SI Switch Series IP Multicast Command Reference-R2208*.

For more information about the **ipv6 neighbor** command, See "IPv6 basics configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Command Reference-R2208*.

New feature: Configuring packet capture

Overview

The packet capture feature facilitates network problem identification. Packets captured are stored in the packet capture buffer on the device. You can display the packets at the CLI, or export them to a **.pcap** file and analyze them by using packet analysis software such as Ethereal or Wireshark.

Configuring the packet capture function

When you configure this function, follow these guidelines:

- After you enable packet capture which uses an ACL, you cannot modify the ACL rules, including adding, deleting, and modifying rules.
- When you enable packet capture which uses an ACL, the actions in the ACL are ignored, and the ACL is only used for traffic classification.
- To release system resources after finishing packet capture, use the **undo packet capture** command to disable this function.

To configure the packet capture function:

Step	Command	Remarks
1. Set packet capture parameters.	**packet capture** { **acl** { *acl-number* | **ipv6** *acl6-number* } | **buffer-size** *size* | **length** *capture-length* | **mode** { **circular** | **linear** } }*	Optional.
2. Enable packet capture.	• (Approach 1) Start packet capture immediately: **packet capture start** [**acl** { *acl-number* | **ipv6** *acl6-number* } | **buffer-size** *size* | **length** *capture-length* | **mode** { **circular** | **linear** } | [**packets** *packet-number* | **seconds** *second-number*]]* • (Approach 2) Configure a packet capture schedule: **packet capture schedule datetime** *time date*	Use either approach. You can set packet capture parameters at the same time when you use approach 1. By default, packet capture is disabled, and no packet capture schedule is configured. If you use approach 1, the existing packet capture schedule is invalid.
3. Stop packet capture.	**packet capture stop**	Optional. Stop packet capture before you display, save, or clear the buffered contents. The device automatically stops packet capture when: • The packet capture function operates in linear mode, and the packet capture buffer is full. • The number of packets captured exceeds the upper limit. • The duration of the packet capture process exceeds the upper limit.
4. Save the contents in the packet capture buffer.	**packet capture buffer save** [*filename*]	Optional. Save the file with a filename in **.pcap** format.

Displaying and maintaining packet capture

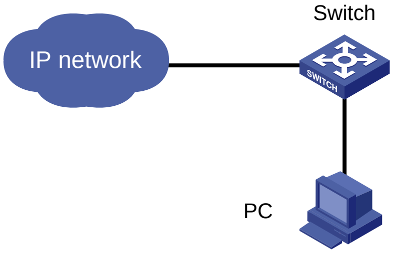
Task	Command	Remarks
Display the current packet capture status.	**display packet capture status**	Available in any view.
Display the buffered contents.	**display packet capture buffer** [*start-index* [*end-index*]] [**length** *display-length*]	Available in any view.
Clear the buffered contents.	**reset packet capture buffer**	Available in user view.

Packet capture configuration example

Network requirements

As shown in Figure 1, the switch captures the packets from 192.168.1.0/24, and saves the result in a **.pcap** file so that the PC can download the file for packet analysis.

Figure 1 Network diagram



Configuration procedure

1. Enable the packet capture function on the switch:

   # Create an ACL rule for IPv4 basic ACL 2000 to permit packets with a source address in 192.168.1.0/24.

```
<Switch> system-view
[Switch] acl number 2000
[Switch-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Switch-acl-basic-2000] quit
[Switch] quit
```

   # Configure the switch to capture packets based on ACL 2000, and start packet capture immediately.

```
<Switch> packet capture start acl 2000
```

   # Display the packet capture status.

```
<Switch> display packet capture status
  Current status :            In process
  Mode :                      Linear
  Buffer size :               2097152 (bytes)
  Buffer used :               1880 (bytes)
  Max capture length :        68 (bytes)
  ACL information :           Basic or advanced IPv4 ACL 2000
  Schedule datetime:          Unspecified
  Upper limit of duration :   Unspecified (seconds)
  Duration :                  13 (seconds)
  Upper limit of packets :    Unspecified
  Packets count :             10
```

   The output shows that packet capture is ongoing.

2. Save the packet capture result:

   # Stop packet capture.

```
<Switch> packet capture stop
```

   # Save the contents in the packet capture buffer to file **test.pcap**.

```
<Switch> packet capture buffer save test.pcap
```

   # Display the contents and file information in the current directory.

```
<Switch> dir
Directory of flash:/

   0     -rw-      1860  Sep 21 2012 12:52:58   test.pcap
   1     drw-         -  Apr 26 2012 12:00:38   seclog
   2     -rw-  10479398  Apr 26 2012 12:26:39   logfile.log
```

The output shows that the buffered contents are successfully saved.

Stop packet capture, and release system resources after packet capture is completed.

```
<Switch> undo packet capture
```

The PC can access the switch through FTP or TFTP, save file **test.pcap**, and analyze the packets through packet analysis software such as Wireshark.

Command reference

display packet capture buffer

Syntax

display packet capture buffer [*start-index* [*end-index*]] [**length** *display-length*]

View

Any view

Default level

1: Monitor level

Parameters

start-index: Specifies a start packet record by its index in the packet capture buffer. If you do not specify this argument, the earliest packet record is displayed the first in the packet capture buffer by default.

end-index: Specifies an end packet record by its index in the packet capture buffer. If you do not specify this argument, the latest packet record is displayed the last in the packet capture buffer by default.

length *display-length*: Specifies the maximum length of data that can be displayed for a single packet record, in the range of 14 to 256 bytes. The default value is 68.

Description

Use **display packet capture buffer** to display the contents in the packet capture buffer.

- If you do not specify any option, the command displays all packet records in the packet capture buffer.
- This command limits the length of data that can be displayed for a single packet record. To display complete packet records, use the **packet capture buffer save** command to save the contents in a **.pcap** file, and display the contents by using the corresponding software.
- Do not use this command during the packet capturing process.

Related commands: **packet capture start** and **packet capture buffer save**.

Examples

Display all contents in the packet capture buffer.

```
<Sysname> display packet capture buffer
2012-07-26 12:03:15:318  Index 1  GE1/0/2  64 (original 64) Bytes captured
  01 80 c2 00 00 03 1c bd b9 e3 b5 02 81 00 00 01
  88 8e 01 01 00 00 00 00 00 00 00 00 00 00 00 00
```

```
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
2012-07-26 12:03:25:749  Index 2  GE1/0/2  68 (original 90) Bytes captured
  33 33 00 00 00 12 00 00 5E 00 02 50 86 DD 6E 00
  00 00 00 20 70 FF FE 80 00 00 00 00 00 00 00 00
  00 00 00 00 00 81 FF 02 00 00 00 00 00 00 00 00
  00 00 00 00 00 12 31 50 64 01 02 58 6A AE FE 80
  00 00 00 00
```

display packet capture status

Syntax

display packet capture status

View

Any view

Default level

1: Monitor level

Parameters

None

Description

Use **display packet capture status** to display the current packet capture status.

Examples

Display the current packet capture status.

```
<Sysname> display packet capture status
  Current status :          In process
  Mode :                    Linear
  Buffer size :             2097152 (bytes)
  Buffer used :             0 (bytes)
  Max capture length :      68 (bytes)
  ACL information :         Ethernet frame header ACL 4200
  Schedule datetime:        Unspecified
  Upper limit of duration : Unspecified (seconds)
  Duration :                60 (seconds)
  Upper limit of packets :  Unspecified
  Packets count :           0
```

Table 14 Command output

Field	Description
Current status	Packet capture status: • **In process**—The packet capturing process is ongoing. • **Scheduled**—The packet capture schedule is configured, but does not start. • **Paused**—Packet capture is stopped temporarily, and you can display, save, and clear the contents in the packet capture buffer.
Mode	Packet capture mode: • Linear. • Circular.

Field	Description
Buffer size	Packet capture buffer size.
Buffer used	Packet capture buffer size in use. One packet record comprises a packet header that records the incoming port, capture time, length of the captured packet and the actual length of the packet, and the data, so it occupies more buffer memory than the maximum captured data.
Max capture length	Maximum length of data that can be captured for a packet.
ACL information	ACL type and number for packet capture.
Schedule datetime	Start time of the packet capture schedule.
Upper limit of duration	Upper limit of the packet capture duration.
Duration	Packet capture duration.
Upper limit of packets	Maximum number of packets that can be captured.
Packets count	Number of packets that has been captured.

packet capture

Syntax

packet capture { **acl** { *acl-number* **| ipv6** *acl6-number* } **| buffer-size** *size* **| length** *capture-length* **| mode** { **circular | linear** } }*

undo packet capture [**acl |buffer-size** | **length** | **mode**]

View

User view

Default level

1: Monitor level

Parameters

acl: Specifies an ACL for packet capture. If you do not specify this keyword, this command captures all packets that the device receives.

acl-number: Specifies the number of an IPv4 ACL:

- 2000 to 2999 for IPv4 basic ACLs
- 3000 to 3999 for IPv4 advanced ACLs
- 4000 to 4999 for Ethernet frame header ACLs

acl6-number: Specifies the number of an IPv6 ACL:

- 2000 to 2999 for IPv6 basic ACLs
- 3000 to 3999 for IPv6 advanced ACLs

buffer-size *size*: Specifies the packet capture buffer size in the range of 32 to 65535 KB. The default value is 2048.

length *capture-length*: Specifies the maximum length of the data that can be captured for a packet, calculated from the first byte of the packet, in the range of 16 to 4000 bytes. The default value is 68. The data out of the range of the maximum length is not recorded.

circular: Specifies the circular packet capture mode. In this mode, packet capture continues even if the buffer is full, and the newly captured packet overwrites the previous records, starting from the earliest one.

linear: Specifies the linear packet capture mode. In this mode, packet capture pauses when the buffer is full. The default mode is linear mode.

Description

Use **packet capture** to set packet capture parameters.

Use **undo packet capture** to restore the default settings, and disable the packet capture function.

- Do not change packet capture parameters during the packet capturing process.
- After you enable packet capture which uses an ACL, you cannot modify the ACL rules, including adding, deleting, and modifying rules.
- When you enable packet capture which uses an ACL, the actions in the ACL are ignored, and the ACL is only used for traffic classification.
- If you specify a keyword for the **undo packet capture** command, the command restores the default setting for the specified keyword. If you do not specify any keyword, the command restores the default settings for all keywords, and disables the packet capture function.

Related commands: **packet capture start**.

Examples

Set the size of the packet capture buffer to 4096 KB, the source address of packets to be captured to 192.168.1.0/24, and start packet capture immediately.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] quit
<Sysname> packet capture buffer-size 4096
<Sysname> packet capture acl 2000
<Sysname> packet capture start
```

Restore the default settings for packet capture parameters, and disable packet capture.

```
<Sysname> undo packet capture
```

packet capture buffer save

Syntax

packet capture buffer save [*filename*]

View

User view

Default level

1: Monitor level

Parameters

filename: Specifies the name of the file to be saved. The filename cannot contain special characters such as backslash (\), slash (/), colon (:), asterisk (*), quotation marks (" "), single quotes (' '), less-than sign (<), greater-than sign (>), and vertical bar (|). If you do not specify this argument, the command saves the file in the default filename **pcapbuffer.pcap**.

Description

Use **packet capture buffer save** to save the contents in the packet capture buffer.

- Save the file with a filename in the **.pcap** format.
- Do not use this command during the packet capturing process.

Related commands: **packet capture**.

Examples

Save the contents in the packet capture buffer to file **example.pcap**.

```
<Sysname> packet capture buffer save example.pcap
```

packet capture schedule

Syntax

packet capture schedule datetime *time date*

undo packet capture schedule

View

User view

Default level

1: Monitor level

Parameters

time: Sets the time in the format of **HH:MM:SS**. **HH** takes a value range of 0 to 23, and **MM** and **SS** take a value range of 0 to 59.

date: Sets the date in the format of **MM/DD/YYYY** or **YYYY/MM/DD**. **MM** takes a value range of 1 to 12, **YYYY** takes a value range of 2000 to 2035, and the value range of **DD** depends on which month the day is in.

Description

Use **packet capture schedule** to configure a packet capture schedule.

Use **undo packet capture schedule** to invalidate the configured packet capture schedule.

By default, no packet capture schedule is configured.

- You can use the **packet capture start** command to enable packet capture as in this command.
- You can use the **packet capture** command to change packet capture parameters before the packet capture schedule starts, or use the **packet capture start** command to start packet capture immediately, and the existing packet capture schedule is invalidated.
- To disable packet capture and invalidate the configured packet capture schedule, execute the **undo packet capture start** command or the **undo packet capture** command without any keyword.

Related commands: **packet capture**.

Examples

Configure a packet capture schedule.

```
<Sysname> packet capture schedule datetime 12:00:00 2012/12/25
```

packet capture start

Syntax

packet capture start [**acl** { *acl-number* | **ipv6** *acl6-number* } | **buffer-size** *size* | **length** *capture-length* | **mode** { **circular** | **linear** } | [**packets** *packet-number* | **seconds** *second-number*]]*

undo packet capture start

View

User view

Default level

1: Monitor level

Parameters

acl: Specifies an ACL for packet capture. If you do not specify this keyword, this command captures all packets that the device receives.

acl-number: Specifies the number of an IPv4 ACL:

- 2000 to 2999 for IPv4 basic ACLs
- 3000 to 3999 for IPv4 advanced ACLs
- 4000 to 4999 for Ethernet frame header ACLs

acl6-number: Specifies the number of an IPv6 ACL:

- 2000 to 2999 for IPv6 basic ACLs
- 3000 to 3999 for IPv6 advanced ACLs

buffer-size *size*: Specifies the packet capture buffer size in the range of 32 to 65535 KB. The default value is 2048.

length *capture-length*: Specifies the maximum length of the data that can be captured for a packet, calculated from the first byte of the packet, in the range of 16 to 4000 bytes. The default value is 68. The data out of the range of the maximum length is not recorded.

circular: Specifies the circular packet capture mode. In this mode, packet capture continues even if the buffer is full, and the newly captured packet overwrites the previous records, starting from the earliest one.

linear: Specifies the linear packet capture mode. In this mode, packet capture pauses when the buffer is full. The default mode is linear mode.

packets *packet-number*: Sets the upper limit of packets that can be captured, in the range of 1 to 4294967295. The default value is 4294967295. Packet capture pauses when the number of captured packets reaches the upper limit.

seconds *second-number*: Sets the upper limit for packet capture duration, in the range of 1 to 4294967295 seconds. The default value is 4294967295 seconds. Packet capture pauses when the packet capture duration reaches the upper limit.

Description

Use **packet capture start** to start packet capture, and set packet capture parameters at the same time.

Use **undo packet capture start** to disable packet capture.

By default, packet capture is disabled.

- Do not start packet capture again or change parameters, or use the **display packet capture buffer**, **reset packet capture buffer** and **packet capture buffer save** commands during the packet capturing process. To do so, use the **packet capture stop** command to temporarily stop packet capture.
- If packet capture is enabled and an ACL number is specified, but the specified ACL does not exist, no packet is captured. If you modify the ACL rule for the specified ACL, the result of packet capture is not affected. The modified ACL rule takes effect after the **packet capture start** command is successfully executed.
- The **undo packet capture start** command stops packet capture, but the packet capture parameters configured are still effective, and you do no need to reconfigure them when you start packet capture again.

Related commands: **packet capture stop**, **display packet capture status**, and **display packet capture buffer**.

Examples

Set the maximum length of the packet captured as 256 bytes, and start packet capture.

```
<Sysname> packet capture length 256 start
```

packet capture stop

Syntax

packet capture stop

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use **packet capture stop** to temporarily stop packet capture.

- After packet capture is stopped, if you use the **packet capture** command to change packet capture parameters, the contents in the capture buffer are cleared.
- This command does not take effect if packet capture is not started.
- After packet capture is stopped, you can use the **display packet capture buffer**, **reset packet capture buffer**, or **packet capture buffer save** command to display or perform operations on the contents in the packet capture buffer, and use the **packet capture start** command to start packet capture again.

Related commands: **packet capture**, **packet capture start**, **display packet capture buffer**, **reset packet capture buffer**, and **packet capture buffer save**.

Examples

Stop packet capture.

```
<Sysname> packet capture stop
```

reset packet capture buffer

Syntax

reset packet capture buffer

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use **reset packet capture buffer** to clear the contents in the packet capture buffer.

Do not use this command during the packet capturing process.

Related commands: **packet capture start**.

Examples

Clear the contents in the packet capture buffer.

```
<Sysname> reset packet capture buffer
```

New feature: Enabling MAC authentication multi-VLAN mode

Overview

By default, a MAC authentication-enabled port forwards packets for an authenticated user only in the VLAN where the user is authenticated. If the user forwards packets in a different VLAN, the port must re-authenticate the user. After the user passes re-authentication, the port will update the MAC and VLAN mapping of the user. For a user that sends various types of traffic (for example, data, video, and audio) in multiple VLANs, frequent MAC re-authentication can downgrade the system performance and affect data transmission quality.

The MAC authentication multi-VLAN mode enables a MAC authentication-enabled port to forward packets for an authenticated user in up to five VLANs without re-authentication.

For example, an IP phone can send tagged and untagged frames, the IP phone is connected to a MAC authentication-enabled port, and the port receives tagged frames in VLAN 2 and untagged frames in VLAN 1. Before you enable the multi-VLAN mode on the port, the port must re-authenticate the IP phone repeatedly, because it sends tagged frames and untagged frames alternately in different VLANs. After you enable the multi-VLAN mode, the port can receive tagged and untagged frames alternately from the IP phone without triggering a MAC re-authentication. The multi-VLAN mode improves the transmission quality of data that is vulnerable to delay and interference.

Configuration procedure

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Enable MAC authentication multi-VLAN mode.	**mac-authentication host-mode multi-vlan**	By default, A MAC-authenticated user only can forward packets in the VLAN where it was authenticated.

Command reference

mac-authentication host-mode multi-vlan

Syntax

mac-authentication host-mode multi-vlan

undo mac-authentication host-mode multi-vlan

View

Layer 2 Ethernet interface view

Default level

2: System level

Description

Use **mac-authentication host-mode multi-vlan** to enable MAC authentication multi-VLAN mode on a port.

Use **undo mac-authentication host-mode multi-vlan** to restore the default.

By default, the MAC authentication multi-VLAN mode is disabled on a port.

The multi-VLAN mode enables a MAC-authenticated user to forward packets in multiple VLANs on the port without re-authentication. The device supports a maximum of four such VLANs on a port.

Examples

Enable MAC authentication multi-VLAN mode on port GigabitEthernet 1/0/2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] mac-authentication host-mode multi-vlan
```

New feature: Binding IP, MAC, and port on Web

Overview

None.

Command reference

None.

Modified feature: Configuring system information for the SNMP agent

Feature change description

Modify the maximum string length of the *sys-contact* and *sys-location* arguments.

Command changes

Modified command: snmp-agent sys-info

Syntax

snmp-agent sys-info { **contact** *sys-contact* **|** **location** *sys-location* **|** **version** { **all** **|** { **v1** **|** **v2c** **|** **v3** }***** } }

Views

System view

Change description

Before modification: Both the *sys-contact* and *sys-location* arguments specify a string of 1 to 200 characters.

After modification: Both the *sys-contact* and *sys-location* arguments specify a string of 1 to 255 characters.

A5500EI-CMW520-R2220P02

This chapter includes following contents:

Modified feature: Enabling/disabling FIPS mode

Feature change description

Added prompt information for the **fips mode enable** and **undo fips mode enable** commands:

```
[Sysname] fips mode enable
FIPS mode change requires a device reboot. Continue?[Y/N]:y
Change the configuration to meet FIPS mode requirements, save the configuration to the
next-startup configuration file, and then reboot to enter FIPS mode.
[Sysname] undo fips mode enable
FIPS mode change requires a device reboot. Continue?[Y/N]:y
Change the configuration to meet non-FIPS mode requirements, save the configuration to
the next-startup configuration file, and then reboot to enter non-FIPS mode.
```

Command changes

None

Modified feature: Setting the IRF link down report delay

Feature change description

Changed the value range of the *interval* argument.

Command changes

Modified command: irf link-delay

Syntax

irf link-delay *interval*

Views

System view

Change description

Before modification: The value range (in milliseconds) for the *interval* argument is 0 to 3000.

After modification: The value range (in milliseconds) for the *interval* argument is 0 to 10000.

Modified feature: Setting the minimum password length

Feature change description

Changed the value range of the minimum password length.

Command changes

Modified command: password-control length

Syntax

password-control length *length*

undo password-control length

Views

System view, user group view, local user view

Change description

Before modification: The value range for the *length* argument is 8 to 32.

After modification: The value range for the *length* argument is 8 to 32 in FIPS mode and 4 to 32 in non-FIPS mode.

Modified feature: Switching the user privilege level

Feature change description

Changed the user privilege level switching control mechanism.

Command changes

Modified command: super

Syntax

super [*level*]

Views

User view

Change description

Before modification: If a scheme authentication user fails to provide the correct password for the higher privilege level during 3 consecutive attempts, the system does not lock the switching function.

After modification: If a scheme authentication user fails to provide the correct password for the higher privilege level during 5 consecutive attempts, the system locks the switching function, and the user must wait 15 minutes before trying again. Trying again before the 15-minute period elapses restores the wait timer to 15 minutes and restarts the timer.

Modified feature: Upgrading a subordinate member

Feature change description

Changed the value range of the absolute-path string length for the *upgrading-filename* argument.

Command changes

Modified command: issu load

Syntax

issu load file *upgrading-filename* **slot** *slot-number* [**force**]

Views

System view

Change description

Before modification: The absolute-path string length for the *upgrading-filename* argument must be in the range of 1 to 136.

After modification: The absolute-path string length for the *upgrading-filename* argument must be in the range of 1 to 64.

Modified feature: Implementing ACL-based IPsec

Feature change description

ACL-based IPsec can protect only traffic that is generated by the device and traffic that is destined for the device. You cannot use an ACL-based IPsec tunnel to protect user traffic. In the ACL that is used to identify IPsec protected traffic, ACL rules that match traffic forwarded through the device do not take effect. For example, an ACL-based IPsec tunnel can protect log messages the device sends to a log server, but it cannot protect traffic that is forwarded by the device for two hosts, even if the host-to-host traffic matches an ACL permit rule.

Command changes

None

Modified feature: Cluster management

Cluster management is not supported in FIPS mode.

A5500EI-CMW520-R2220

This chapter includes following contents:

New feature: Disabling password recovery capacity

Disabling password recovery capacity

Password recovery capability controls console user access to the device configuration and NVRAM from BootWare menus.

If password recovery capability is enabled, a console user can access the device configuration without authentication and reconfigure the console login password and user privilege level passwords.

If password recovery capability is disabled, a console user must restore the factory-default configuration before configuring new passwords. Restoring the factory-default configuration deletes the next-startup configuration files.

To enhance system security:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Disable password recovery capacity.	**undo password-recovery enable**	By default, password recovery capability is enabled.

For more information about BootWare menus and password recovery capacity, see appendix B in *HP A5500EI-CMW520-R2220* Release Notes *Release Notes*.

Command reference

password-recovery enable

Syntax

password-recovery enable

undo password-recovery enable

View

System view

Default level

3: Manage level

Description

Use **password-recovery enable** to enable password recovery capability.

Use **undo password-recovery enable** to disable password recovery capability.

By default, password recovery capability is enabled.

To enhance system security, disable password recovery capability.

Examples

Disable password recovery capability.

```
<Sysname> system-view
[Sysname] undo password-recovery enable
```

New feature: Configuring a port to forward 802.1X EAPOL packets untagged

Configuring a port to forward 802.1X EAPOL packets untagged

After an 802.1X user passes authentication, the 802.1X server assigns authorization attributes to the access device. If the port is assigned to a VLAN as a tagged member, the port that connects the clients forwards packets tagged. 802.1X defines EAP over LAN (EAPOL) for passing EAP packets between the client and the network access device over a wired or wireless LAN. An EAPOL-format 802.1X packet cannot carry any VLAN tag in its header. To ensure the communication between the client and the network access device, you can configure the port that connects the client and the network access device to forward 802.1X EAPOL packets after removing the tag.

To configure a port to forward 802.1X EAPOL packets untagged:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the port to forward 802.1X EAPOL packets untagged.	**dot1x eapol untag**	Optional. By default, whether the port forwards 802.1X EAPOL packets with the VLAN tag depends on the port configuration and the server-assigned VLAN setting.

NOTE:

- An access port cannot be a tagged member of any VLAN.
- The device does not change the PVID of a hybrid or trunk port when the port is assigned to the VLAN as a tagged member.

Command reference

dot1x eapol untag

Syntax

dot1x eapol untag

undo dot1x eapol untag

View

Layer 2 Ethernet interface view

Default level

3: Manage level

Description

Use **dot1x eapol untag** to configure a port to forward 802.1X EAPOL packets untagged.

By default, whether the port forwards 802.1X EAPOL packets with the VLAN tag depends on the port configuration and the server-assigned VLAN setting.

Examples

Configure GigabitEthernet 1/0/1 to forward 802.1X EAPOL packets untagged.

```
<Sysname> system-view
[Sysname]interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x eapol untag
```

New feature: Enabling source IP conflict prompt

Enabling source IP conflict prompt

When the sender IP address in a gratuitous ARP packet is the same as the IP address of the receiving switch, the switch operates as follows:

- If the source IP conflict prompt is enabled, the receiving switch immediately displays a message telling that IP address conflict occurs.
- If the source IP conflict prompt is disabled, the receiving switch sends a gratuitous ARP packet. After the switch is informed of the conflict by an ARP reply, it displays a message telling that IP address conflict occurs.

To enable source IP conflict prompt:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable source IP conflict prompt.	**arp ip-conflict prompt**	Optional. By default, the function is disabled.

Command reference

arp ip-conflict prompt

Use **arp ip-conflict prompt** to enable source IP conflict prompt.

Use **undo arp ip-conflict prompt** to restore the default.

Syntax

arp ip-conflict prompt

undo arp ip-conflict prompt

Default

The source IP conflict prompt function is disabled.

Views

System view

Default command level

2: System level

Parameters

None

Examples

Enable source IP conflict prompt.

```
<Sysname> system-view
[Sysname] arp ip-conflict prompt
```

New feature: Delaying the MAC authentication

When both 802.1X authentication and MAC authentication are enabled on a port, you can delay the MAC authentication, so that 802.1X authentication is preferentially triggered. Configure the function as needed according to the network conditions.

Configuring the MAC authentication delay

To configure the MAC authentication delay:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the MAC authentication delay.	**mac-authentication timer auth-delay** *time*	By default, MAC authentication is not delayed.

Command reference

mac-authentication timer auth-delay

Syntax

mac-authentication timer auth-delay *time*

undo mac-authentication timer auth-delay

Views

Layer 2 Ethernet port view

Default command level

2: System level

Parameters

time: Specifies the MAC authentication delay, which ranges from 1 to 180 seconds.

Description

Use **mac-authentication timer auth-delay** to configure the MAC authentication delay.

Use **undo mac-authentication timer auth-delay** to restore the default.

By default, MAC authentication is not delayed.

Examples

Set the MAC authentication delay to 30 seconds on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication timer auth-delay 30
```

New feature: Disabling MAC entry aging timer refresh based on destination MAC address

Disabling MAC entry aging timer refresh based on destination MAC address

To accommodate network changes, the MAC address table keeps updating. Each dynamic MAC address entry has an aging timer. When the device receives a packet with the source or destination MAC address matching a dynamic MAC address entry, it restarts the aging timer for the entry.

If you want the device to restart the aging timer of dynamic entries for only matching source MAC addresses, disable MAC entry aging timer refresh based on destination MAC address.

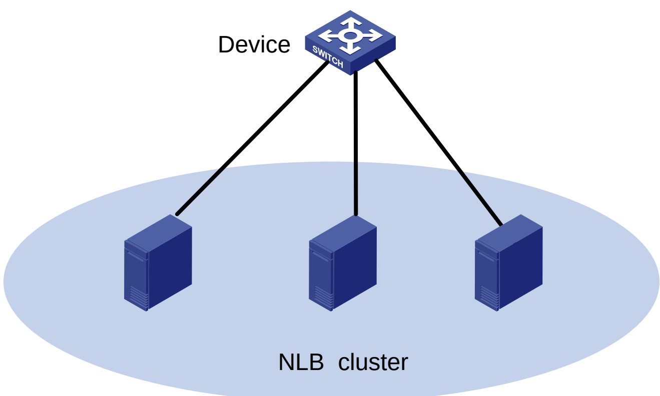
To disable MAC entry aging timer refresh based on destination MAC address:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Disable MAC entry aging timer refresh based on destination MAC address.	**mac-address destination-hit disable**	By default, MAC entry aging timer refresh based on destination MAC address is enabled.

Application example

Microsoft Network Load Balancing (NLB) is a load balancing technology for server clustering developed on Windows Server.

Figure 1 NLB cluster



NLB supports load sharing and redundancy among servers within a cluster. To implement fast failover, NLB requires that the switch forwards network traffic to all servers or specified servers in the cluster, and each server filters out unexpected traffic.

In NLB unicast mode, when a server joins the cluster or a failover occurs, a packet with a virtual source MAC address is sent. The switch then adds the virtual MAC address to its MAC address table, and packets destined for the server use the virtual MAC address (although not used by the server) as their destination address. If the virtual MAC address never ages out, the switch forwards packets only through the port associated with the virtual MAC address rather than all ports connected to the servers within the cluster.

To address this issue, disable MAC entry aging timer refresh based on destination MAC address to age out the virtual MAC address, so that the switch can forward packets to all servers within the cluster.

Command reference

mac-address destination-hit disable

Use **mac-address destination-hit disable** to disable MAC entry aging timer refresh based on destination MAC address.

Use **undo mac-address destination-hit disable** to restore the default.

Syntax

mac-address destination-hit disable

undo mac-address destination-hit disable

Default

MAC entry aging timer refresh based on destination MAC address is enabled.

View

System view

Default command level:

2: System level

Examples

Disable MAC entry aging timer refresh based on destination MAC address.

```
<Sysname> system-view
[Sysname] mac-address destination-hit disable
```

New feature: Setting the deletion delay time for SAVI

Setting the deletion delay time for SAVI

The SAVI feature enables the access switch to check the validity of the source addresses of DHCPv6 protocol packets, ND protocol packets, and IPv6 data packets against the ND snooping entries, DHCPv6 snooping entries, and IP source guard bindings.

After a port is down, the switch can wait for a period of delay time before deleting the DHCPv6 snooping entries and ND snooping entries for that port. The deletion delay time is configurable. This delay ensures a valid IPv6 user to access the port for the event that a port goes down and resumes during that period.

Table 15 Setting the deletion delay time for SAVI

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable SAVI.	**ipv6 savi strict**	By default, SAVI is disabled.
3. Setting the deletion delay time for SAVI.	**ipv6 savi down-delay** *time*	The default setting is 30 seconds.

Command reference

ipv6 savi down-delay

Use **ipv6 savi down-delay** to set the deletion delay time for SAVI.

Use **undo ipv6 savi down-delay** to restore the default.

Syntax

ipv6 savi down-delay *time*

undo ipv6 savi down-delay

Default

The deletion delay time is 30 seconds.

Views

System view

Default command level

2: System level

Parameters

time: Specifies the delay time in the range of 0 to 86400 seconds.

Usage guidelines

If a port is down for a period of time that exceeds the deletion delay time, the switch deletes the DHCPv6 snooping entries and ND snooping entries for that port.

Examples

Set the deletion delay time for SAVI to 360 seconds.

```
<Sysname> system-view
[Sysname] ipv6 savi down-delay 360
```

A5500EI-CMW520-F2218L02

This release has the following changes:

- Modified feature: Changing the VRF instances per VLAN interface from 128 to 1023

Modified feature: Changing the VRF instances per VLAN interface from 128 to 1023

Feature change description

Changing the VRF instances per VLAN interface from 128 to 1023.

Command changes

None.

A5500EI-CMW520-F2218P01

This release has the following changes:

- Modified feature: Default configuration

Modified feature: Default configuration

Feature change description

The following changes are made to the default configuration in this release:

- The **telnet server enable** command is deleted and Telnet service is disabled.
- The **interface vlan-interface1** command is deleted and VLAN-interface 1 does not exist.
- The **ip address dhcp-alloc client-identifier mac Vlan-interface1** command is deleted and VLAN-interface 1 does not apply for an IP address.
- The **undo ip http enable** command is added and HTTP service is disabled.
- The **undo cwmp enable** command is added and CWMP service is disabled.
- Deleted the default RADIUS scheme system, which included the following commands: **radius scheme system**, **server-type extended**, **primary authentication** 127.0.0.1 1645, **primary accounting** 127.0.0.1 1646, and **user-name-format without-domain**.

The default configuration takes effect only when the switch starts up with no specific configuration file. Once you specify a specific startup configuration file for the switch, the switch uses the specific configuration file instead of the default configuration.

Command changes

None

A5500EI-CMW520-F2218

This release has the following changes:

- New feature: Supporting using a self-signed certificate for HTTPS
- New feature: Setting the maximum number of 802.1X authentication attempts for MAC authentication users
- New feature: Support of 802.1X for issuing VLAN groups
- New feature: Enabling MAC address migration log notifying
- Modified feature: Cluster management
- Removed feature: WiNet

New feature: Supporting using a self-signed certificate for HTTPS

The switch supports simplified HTTPS login. To make the switch operate in this mode, you only need to enable HTTPS service on the switch. The switch will use a self-signed certificate (a certificate that is generated and signed by the switch itself, rather than a CA). If you specify an SSL server policy for the HTTPS service before enabling HTTPS service but do not specify the PKI domain for the SSH server, the switch still uses self-signed certificate. After you specify a PKI domain for the SSH server, the switch uses the PKI domain to obtain a certificate for the SSH server from the CA and uses the obtained certificate.

New feature: Setting the maximum number of 802.1X authentication attempts for MAC authentication users

Setting the maximum number of 802.1X authentication attempts for MAC authentication users

When both MAC authentication and 802.1X authentication are enabled on a port, if a MAC-authenticated user sends an EAP packet to the device for 802.1X authentication, the device performs 802.1X authentication for the user by default. If the user passes 802.1X authentication, the user goes online as an 802.1X user. If the user fails 802.1X authentication, the user might to try the authentication multiple times, depending on the configuration on the client. If you do not want such users to try 802.1X authentication for too many times, you can perform the following task on the device to limit the number of authentication failures.

To set the maximum number of 802.1X authentication attempts for MAC authentication users:

Step	Command
1. Enter system view.	**system-view**
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*
3. Set the maximum number of 802.1X authentication attempts for MAC authentication users.	**dot1x attempts max-fail** *unsuccessful-attempts*

Command reference

dot1x attempts max-fail

Use **dot1x attempts max-fail** to set the maximum number of 802.1X authentication attempts that a MAC-authenticated user can try.

Use **undo dot1x attempts max-fail** to restore the default.

Syntax

dot1x attempts max-fail *unsuccessful-attempts*

undo dot1x attempts max-fail

Default

The device allows a user that have passed MAC authentication to perform 802.1X authentication, and the maximum number of 802.1X authentication attempts that the user can try is determined by the configuration on the authentication client.

Views

Layer 2 Ethernet interface view

Default command level:

2: System level

Parameters

unsuccessful-attempts: Sets the maximum number of 802.1X authentication attempts that a MAC-authenticated user can try. The value range for this argument is 1 to 50.

Examples

On interface GigabitEthernet 1/0/1, set the maximum number of 802.1X authentication attempts that a MAC-authenticated user can try to 3.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x attempts max-fail 3
```

New feature: Support of 802.1X for issuing VLAN groups

Support of 802.1X for issuing VLAN groups

After an 802.1X user passes the authentication on the server, the server delivers the authorization information to the device. If the server has specified the VLAN which is to be assigned to the user, the server contains the VLAN information in the authorization information to be delivered to device. Then, the device assigns the port through which the user performs authentication and logs in to the server-assigned VLAN.

The authentication server running the earlier releases issues a VLAN ID or VLAN name, and supports issuing only the specified VLAN. In this release or later, you can configure a VLAN group on the device, and the authentication server issues a VLAN group name. After the authentication server issues a VLAN group name, the access device selects a VLAN ID in the VLAN group and assigns the VLAN ID to a user.

The access device selects a VLAN ID from the VLAN group following these rules:

1. Select a VLAN with the least users.
2. Select the first queried VLAN if multiple VLANs have the same number of users.

For example, a VLAN group contains VLAN 2 and VLAN 3, VLAN 3 has been assigned to three users who have passed the authentication, and VLAN 2 has been assigned to two users who have passed the authentication. When a user passes the authentication, VLAN 2 is assigned to the user.

By issuing a VLAN group, you can balance the number of users in each VLAN, reduce the broadcasts in each VLAN, and improve the efficiency.

Configuring a VLAN group

You can create a VLAN group and add multiple VLAN IDs to a VLAN group.

To configure a VLAN group:

Step	Command
1. Enter system view.	**system-view**
2. Create a VLAN group and enter VLAN group view.	**vlan-group** *group-name*
3. Assign the specified VLANs to the VLAN group.	**vlan-list** *vlan-list*

NOTE:

If a super VLAN is added to a VLAN group, the device ignores the super VLAN when selecting a server-assigned VLAN for a user passing the authentication.

Command reference

vlan-group

Use **vlan-group** to create a VLAN group and enter VLAN group view.

Use **undo vlan-group** to delete the specified VLAN group.

Syntax

vlan-group *group-name*

undo vlan-group *group-name*

Default

No VLAN group exists.

Views

System view

Default command level

3: Manage level

Parameters

group-name: VLAN group name, which is a case-insensitive string of 1 to 31 characters and must start with a letter.

Usage guidelines

You can configure up to 100 VLAN groups.

Examples

Create a VLAN group named **test**, and enter VLAN group view.

```
<Sysname> system-view
[Sysname] vlan-group test
```

vlan-list

Use **vlan-list** to configure member VLANs for the VLAN group.

Use **undo vlan-list** to delete member VLANs from the VLAN group.

Syntax

vlan-list *vlan-list*

undo vlan-list *vlan-list*

Views

VLAN group view

Default command level

3: Manage level

Parameters

vlan-list: Specifies a VLAN list in the form of *vlan-list* = { *vlan-id1* [**to** *vlan-id2*] }&<1-10>, where *vlan-id1* and *vlan-id2* each range from 1 to 4094 and *vlan-id1* cannot be greater than *vlan-id2*. &<1-10> indicates that you can specify up to ten { *vlan-id1* [**to** *vlan-id2*] } parameters.

Usage guidelines

You can add VLANs that have not been created to a VLAN group.

You can add a VLAN to multiple VLAN groups.

Repeat this command to configure multiple member VLANs for a VLAN group.

If a super VLAN is added to a VLAN group, the device ignores the super VLAN when selecting a server-assigned VLAN for a user passing the authentication.

Examples

Add VLANs 6, 7, and 8 to the VLAN group named **test**.

```
<Sysname> system-view
[Sysname] vlan-group test
[Sysname-vlan-group-test] vlan-list 6 7 8
```

New feature: Enabling MAC address migration log notifying

Enabling MAC address migration log notifying

This feature records and notifies MAC address migration information, including MAC addresses that migrate, IDs of VLANs to which MAC addresses belong, source interfaces from which MAC addresses migrate, and current interfaces with which MAC addresses associate, last migration time, and migration times in the last one minute.

MAC address migration refers to this process: a device learns a MAC address from an interface, Port A for example, and the device later learns the MAC address from another interface, Port B for example. If Port A and Port B belong to the same VLAN, the outgoing interface in the entry for the MAC address is changed to Port B from Port A, which means that the MAC address migrates from Port A to Port B.

To enable MAC address migration log notifying:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable MAC address migration log notifying.	**mac-flapping notification enable**	By default, MAC address migration log notifying is disabled.

The MAC address migration logs of the last one minute are displayed once every one minute.

Command reference

mac-flapping notification enable

Use **mac-flapping notification enable** to enable MAC address migration log notifying.

Use **undo mac-flapping notification enable** to disable the MAC address migration notifying.

Syntax

mac-flapping notification enable

undo mac-flapping notification enable

Default

MAC address migration log notifying is disabled.

Views

System view

Default command level:

2: System level

Usage guidelines

A MAC address migration log contains a MAC address, ID of the VLAN to which the MAC address belongs, source interface from which the MAC address migrates, and the current interface with which the MAC address associates.

After enabling MAC address migration log notifying, the MAC address migration log of the last 1 minute are displayed once every 1 minute.

Up to 10 logs can be saved on each card in 1 minute.

Examples

Enable MAC address migration log notifying.

```
<Sysname> system-view
[Sysname] mac-flapping notification enable
[Sysname]
%Sep 21 14:09:22:420 2012 HP MAC/5/MAC_FLAPPING: MAC address 0000-0012-0034 in vlan 500
has flapped from port GigabitEthernet1/0/16 to port GigabitEthernet1/0/1 1 time(s).
```

The output shows that the MAC address 0000-0012-0034 belongs to VLAN 500, the source interface from which the MAC address migrates from is GE1/0/16, the current interface with which the MAC address associates is GE1/0/1, and the MAC address migrates one time in the last one minute.

Modified feature: Cluster management

Feature change description

Changed the default state of the Cluster function, NDP, and NTDP from enabled to disabled.

Command changes

Modified command: cluster enable

Syntax

cluster enable

undo cluster enable

Views

System view

Change description

Before modification: By default, the cluster function is enabled.

After modification: By default, the cluster function is disabled.

Modified command: ndp enable

Syntax

In Layer 2 Ethernet port view or Layer 2 aggregate interface view:

ndp enable

undo ndp enable

In system view:

ndp enable [**interface** *interface-list*]

undo ndp enable [**interface** *interface-list*]

Views

System view, Layer 2 Ethernet port view, Layer 2 aggregate interface view

Change description

Before modification: By default, NDP is enabled globally and also on all ports.

After modification: By default, NDP is disabled globally and also on all ports.

Modified command: ntdp enable

Syntax

ntdp enable

undo ntdp enable

Views

System view, Layer 2 Ethernet port view, Layer 2 aggregate interface view

Change description

Before modification: By default, NTDP is enabled globally and also on all ports.

After modification: By default, NTDP is disabled globally and also on all ports.

Removed feature: WiNet

Feature change description

Removed the WiNet feature.

Removed commands

None

A5500EI-CMW520-F2217

This release has the following changes:

- New feature: Automatic configuration file backup for software downgrading
- New feature: FIPS
- New feature: Configuring ACL-based IPsec
- New feature: IKE
- New feature: Verifying the correctness and integrity of the file
- Modified feature: Configuring a password for the local user
- Modified feature: Clearing all users from the password control blacklist
- Modified feature: 802.1X critical VLAN
- Modified feature: MAC authentication critical VLAN
- Modified feature: Modifying CLI configuration commands executed in FIPS mode for CC evaluation
- Modified feature: Modifying login management commands executed in FIPS mode for CC evaluation
- Modified Feature: Modifying software upgrade commands executed in FIPS mode for CC evaluation
- Modified Feature: Modifying configuration file management commands executed in FIPS mode for CC evaluation
- Modified Feature: Modifying security commands executed in FIPS mode for CC evaluation
- Modified feature: Modifying SNMP commands executed in FIPS mode for CC evaluation

New feature: Automatic configuration file backup for software downgrading

Configuring automatic configuration file backup for software downgrading

After a software upgrade, the first time you use the **save** [**safely**] [**backup** | **main**] [**force**] command to save configuration to a configuration file that was created before the upgrade, the system verifies the compatibility of the configuration file with the software version.

If any incompatibility is found, the system uses the running configuration to overwrite the configuration file after backing up the file to the Flash memory on each member device for future rollback. The backup file is named in the *old-filename*_**bak.cfg** format. For example, if the old configuration file is named config.cfg, the backup file is named config_bak.cfg.

If the backup attempt fails on an IRF member device, choose one of the following failure handling actions at prompt:

- **Give up saving the configuration**—In this approach, the system does not save the configuration on any member device.
- **Overwrite the configuration file**—In this approach, the system uses the running configuration to overwrite the configuration file on the member device without backing up the file. You can copy the backup configuration file from the master device to this member device for future rollback.

To load the backup configuration file after a software downgrade, specify the file as the next-startup configuration file before performing the downgrade.

Command reference

None.

New feature: FIPS

Overview

Federal Information Processing Standards (FIPS), developed by the National Institute of Standard and Technology (NIST) of the United States, specify the requirements for cryptography modules. FIPS 140-2 defines four levels of security, simply named "Level 1" to "Level 4" from low to high. Currently, the switch supports Level 2.

Unless otherwise noted, *FIPS* in the document refers to FIPS 140-2.

FIPS self-tests

When the device operates in FIPS mode, it has self-test mechanisms, including the power-up self-test and conditional self-tests, to ensure the normal operation of cryptography modules. You can also trigger a self-test. If a self-test fails, the device restarts.

CAUTION:

If the switch reboots repeatedly, it might be caused by software failures or hardware damages. Contact technical support engineers to upgrade the software or repair the damaged hardware.

Power-up self-test

The power-up self-test, also called "known-answer test", examines the availability of FIPS-allowed cryptographic algorithms. A cryptographic algorithm is run on data for which the correct output is already known. The calculated output is compared with the known answer. If they are not identical, the known-answer test fails.

Conditional self-tests

A conditional self-test runs when an asymmetrical cryptographic module or a random number generator module is invoked. Conditional self-tests include the following types:

- **Pair-wise consistency test**—This test is run when a DSA/RSA asymmetrical key-pair is generated. It uses the public key to encrypt a plain text, and uses the private key to decrypt the encrypted text. If the decryption is successful, the test succeeds. Otherwise, the test fails.
- **Continuous random number generator test**—This test is run when a random number is generated in FIPS mode. If two consecutive random numbers are different, the test succeeds. Otherwise, the test fails.

Triggering a self-test

To examine whether the cryptography modules operate normally, you can use a command to trigger a self-test on the cryptographic algorithms. The triggered self-test is the same as the power-up self-test.

If the self-test fails, the device automatically reboots.

Configuring FIPS

To configure FIPS, complete the following tasks:

1. Remove the existing key pairs and certificates.
2. Enable the FIPS mode.
3. Enable the password control function.
4. Configure local user attributes (including local username, service type, password, and so on) on the switch.
5. Save the configuration.

After you finish the above configurations, reboot the switch. The switch works in FIPS mode that complies with the FIPS 140-2 standard after it starts up. For Common Criteria (CC) evaluation in FIPS mode, the switch also works in a operating mode that complies with the CC standard.

The switch does not support an upgrade from a FIPS-incompatible version to a FIPS-compatible version.

Enabling the FIPS mode

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable the FIPS mode.	**fips mode enable**	Disabled by default.

After you enable the FIPS mode and reboot the switch, the switch works in FIPS mode after it starts up and the following changes occur.

- FTP/TFTP is disabled.
- Telnet is disabled.
- The HTTP server is disabled.
- SNMPv1 and SNMPv2c are disabled. Only SNMPv3 is available.
- The SSL server only supports TLS1.0.
- The SSH server does not support SSHv1 clients
- SSH only supports RSA.
- The generated RSA key pairs must have a modulus length of 2048 bits. The generated DSA key pair must have a modulus of at least 1024 bits.
- SSH, SNMPv3, IPsec and SSL do not support DES, 3DES, RC4, or MD5.

Triggering a self-test

To examine whether the cryptography modules operate normally, you can use a command to trigger a self-test on the cryptographic algorithms. The triggered self-test is the same as the power-up self-test.

If the self-test fails, the device automatically reboots.

To trigger a self-test:

Task	Command
1. Enter system view.	**system-view**
2. Trigger a self-test.	**fips self-test**

Displaying and maintaining FIPS

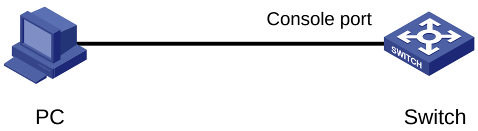
Task	Command	Remarks
Display FIPS mode state	**display fips status**	Available in any view.

FIPS configuration example

Network requirements

PC connects to Switch through a console port. Configure Switch to operate in FIPS mode and create a local user for PC so that PC can log in to the switch.

Figure 1 Network diagram



Configuration procedure

1. Configure Switch:

Enable the FIPS mode.

```
<Sysname> system-view
[Sysname] fips mode enable
```

Enable the password control function.

```
[Sysname] password-control enable
```

Create a local user named **test**, and set its service type as **terminal**, privilege level as **3**, and password as **AAbbcc1234%**. The password is a string of at least 10 characters by default and must contain both uppercase and lowercase letters, digits, and special characters.

```
[Sysname] local-user test
[Sysname-luser-test] service-type terminal
[Sysname-luser-test] authorization-attribute level 3
[Sysname-luser-test] password
Password:***********
Confirm :***********
Updating user(s) information, please wait...........
[Sysname-luser-test] quit
```

Save the configuration.

```
[Sysname] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
 Validating file. Please wait..........................
 Saved the current configuration to mainboard device successfully.
 Configuration is saved to device successfully.
[Sysname] quit
```

Reboot the switch.

```
<Sysname> reboot
```

CAUTION:

After you enable the FIPS mode, be sure to create a local user and its password before you reboot the switch. Otherwise, you cannot log in to the switch. If you cannot log in to the switch, reboot the switch without the configuration file (by ignoring or removing the configuration file) so that the switch works in non-FIPS mode, and then make correct configurations.

2. Verify the configuration:

After the switch reboots, enter the username (test) and password (AAbbcc1234%). The system prompts that your first login is successful, and asks you to enter a new password. Enter a new password which has at least four characters different than the previous one and confirm the password. Then, the system displays the <Sysname> prompt.

```
User interface aux0 is available.


Please press ENTER.


Login authentication


Username:test
Password:
Info: First logged in. For security reasons you will need to change your password.
 Please enter your new password.
Password:**********
Confirm :**********
Updating user(s) information, please wait...........
<Sysname>
```

Display the current FIPS mode. You can see that the FIPS mode is enabled.

```
<Sysname> display fips status
 FIPS mode is enabled
```

Command reference

fips mode enable

Use **fips mode enable** to enable the FIPS mode.

Use **undo fips mode enable** to disable the FIPS mode.

Syntax

fips mode enable

undo fips mode enable

Default

The FIPS mode is disabled.

Views

System view

Default command level

2: System level

Parameters

None

Usage guidelines

After you enable the FIPS mode, reboot the switch to make your configuration effective. After the switch starts up, the switch works in FIPS mode. The FIPS mode complies with the FIPS 140-2 standard.

Examples

Enable the FIPS mode.

```
<Sysname> system-view
[Sysname] fips mode enable
```

Related commands

display fips status

display fips status

Use **display fips status** to display the current FIPS mode.

Syntax

display fips status

Views

Any view

Default command level

1: Monitor level

Examples

Display the current FIPS mode.

```
<Sysname> display fips status
FIPS mode is enabled
```

Related commands

fips mode enable

fips self-test

Use **fips self-test** to trigger a self-test on the password algorithms.

Syntax

fips self-test

Views

System view

Default command level

3: Manage level

Usage guidelines

To examine whether the cryptography modules operate normally, you can use a command to trigger a self-test on the cryptographic algorithms. The triggered self-test is the same as the power-up self-test.

If the self-test fails, the device automatically reboots.

Examples

Trigger a self-test on the cryptographic algorithms.

```
<Sysname> system-view
[Sysname] fips self-test
Self-tests are running. Please wait...
Self-tests succeeded.
```

New feature: Configuring ACL-based IPsec

NOTE:

- The term *router* in this document refers to both routers and switches.
- IKE configuration is available for only the switches in FIPS mode. For information about the FIPS mode, see New feature: FIPS.
- A switch in IRF mode does not support IPsec automatic negotiation.

Configuring ACL-based IPsec

Feature restrictions

ACL-based IPsec is designed to protect only traffic that is generated by the device and traffic that is destined for the device. Providing IPsec protection for user traffic will severely decrease performance. To avoid this issue, HP recommends that you not include any rules in the security ACL to match traffic forwarded through the device. For example, you can configure an ACL-based IPsec tunnel to protect log messages the device sends to a log server. However, do not use an IPsec tunnel to protect traffic that is forwarded by the device for two hosts. For more information about configuring an ACL for IPsec, see "Configuring ACLs."

Typically, IKE uses UDP port 500 for communication, and AH and ESP use the protocol numbers 51 and 50 respectively. Make sure that flows of these protocols are not denied on the interfaces with IKE or IPsec configured.

ACL-based IPsec configuration task list

The following is the generic configuration procedure for implementing ACL-based IPsec:

1. Configure ACLs for identifying data flows to be protected.
2. Configure IPsec proposals to specify the security protocols, authentication and encryption algorithms, and encapsulation mode.
3. Configure IPsec policies to associate data flows with IPsec proposals and specify the SA negotiation mode, the peer IP addresses (the start and end points of the IPsec tunnel), the required keys, and the SA lifetime.
4. Apply the IPsec policies to interfaces to finish IPsec configuration.

To configure ACL-based IPsec:

Task	Remarks
Configuring ACLs	Required. Basic IPsec configuration.
Configuring an IPsec proposal	
Configuring an IPsec policy	
Applying an IPsec policy group to an interface	
Configuring the IPsec session idle timeout	Optional.
Enabling ACL checking of de-encapsulated IPsec packets	Optional.

Task	Remarks
Configuring the IPsec anti-replay function	Optional.
Configuring packet information pre-extraction	Optional.

Configuring ACLs

ACLs can be used to identify traffic. They are widely used in scenarios where traffic identification is desired, such as QoS and IPsec.

Keywords in ACL rules

IPsec uses ACLs to identify data flows. An ACL is a collection of ACL rules. Each ACL rule is a deny or permit statement. A permit statement identifies a data flow protected by IPsec, and a deny statement identifies a data flow that is not protected by IPsec. With IPsec, a packet is matched against the referenced ACL rules and processed according to the first rule that it matches:

- Each ACL rule matches both the outbound traffic and the returned inbound traffic. Suppose there is a rule **rule 0 permit ip source 1.1.1.0 0.0.0.255 destination 2.2.2.0 0.0.0.255**. This rule matches both traffic from 1.1.1.0 to 2.2.2.0 and traffic from 2.2.2.0 to 1.1.1.0.
- In the outbound direction, if a permit statement is matched, IPsec considers that the packet requires protection and continues to process it. If a deny statement is matched or no match is found, IPsec considers that the packet does not require protection and delivers it to the next function module.
- In the inbound direction:
    - Normal IP packets that match a permit statement are dropped.
    - IPsec packets that match a permit statement and are destined for the device itself are de-encapsulated and matched against the rule again. Only those that match a permit statement are processed by IPsec.

When you configure an ACL for IPsec, follow these guidelines:

- Permit only data flows that need to be protected and use the **any** keyword with caution. With the **any** keyword specified in a permit statement, all outbound traffic matching the permit statement will be protected by IPsec and all inbound IPsec packets matching the permit statement will be received and processed, but all inbound non-IPsec packets will be dropped. This will cause the inbound traffic that does not need IPsec protection to be all dropped.
- Avoid statement conflicts in the scope of IPsec policy groups. When creating a deny statement, be careful with its matching scope and matching order relative to permit statements. The policies in an IPsec policy group have different match priorities. ACL rule conflicts between them are prone to cause mistreatment of packets. For example, when configuring a permit statement for an IPsec policy to protect an outbound traffic flow, you must avoid the situation that the traffic flow matches a deny statement in a higher priority IPsec policy. Otherwise, the packets will be sent out as normal packets; if they match a permit statement at the receiving end, they will be dropped by IPsec.
- An ACL can be specified for only one IPsec policy. ACLs referenced by IPsec policies cannot be used by other services.
- You must create a mirror image ACL rule at the remote end for each ACL rule created at the local end. Otherwise, IPsec may protect traffic in only one direction.

Mirror image ACLs

To make sure that SAs can be set up and the traffic protected by IPsec can be processed correctly at the remote peer, on the remote peer, create a mirror image ACL rule for each ACL rule created at the local peer.

If the ACL rules on peers do not form mirror images of each other, SAs can be set up only when both of the following requirements are met:

- The range specified by an ACL rule on one peer is covered by its counterpart ACL rule on the other peer.
- The peer with the narrower rule initiates SA negotiation. If a wider ACL rule is used by the SA initiator, the negotiation request may be rejected because the matching traffic is beyond the scope of the responder.

Protection modes

The switch supports IPsec for data flows in standard mode. In standard mode, one tunnel protects one data flow. The data flow permitted by an ACL rule is protected by one tunnel that is established solely for it.

For more information about ACL configuration, see *ACL and QoS Configuration Guide*.

NOTE:

To use IPsec in combination with QoS, make sure IPsec's ACL classification rules match the QoS classification rules. If the rules do not match, QoS may classify the packets of one IPsec SA to different queues, causing packets to be sent out of order. When the anti-replay function is enabled, IPsec will discard the packets beyond the anti-replay window in the inbound direction, resulting in packet loss. For more information about QoS classification rules, see *ACL and QoS Configuration Guide*.

Configuring an IPsec proposal

This section is not newly added. In this version, related commands that are executed in FIPS mode were modified.

An IPsec proposal, part of an IPsec policy or an IPsec profile, defines the security parameters for IPsec SA negotiation, including the security protocol, the encryption and authentication algorithms, and the encapsulation mode.

To configure an IPsec proposal:

Step	Command	Remarks
1. Enter system view	**system-view**	N/A
2. Create an IPsec proposal and enter its view	**ipsec proposal** *proposal-name*	By default, no IPsec proposal exists.
3. Specify the security protocol for the proposal	**transform** { **ah** | **ah-esp** | **esp** }	Optional. ESP by default.

Step	Command	Remarks
4. Specify the security algorithms	• Specify the encryption algorithm for ESP: ○ In non-FIPS mode: **esp encryption-algorithm** { **3des** | **aes** [*key-length*] | **des** } ○ In FIPS mode: **esp encryption-algorithm aes** [*key-length*] • Specify the authentication algorithm for ESP: ○ In non-FIPS mode: **esp authentication-algorithm** { **md5** | **sha1** } ○ In FIPS mode: **esp authentication-algorithm sha1** • Specify the authentication algorithm for AH: ○ In non-FIPS mode: **ah authentication-algorithm** { **md5** | **sha1** } ○ In FIPS mode: **ah authentication-algorithm sha1**	Optional. For ESP, the default encryption algorithm is DES in non-FIPS mode and is AES-128 in FIPS mode. For ESP and AH, the default authentication algorithm is MD5 in non-FIPS mode and is SHA1 in FIPS mode.
5. Specify the IP packet encapsulation mode for the IPsec proposal	**encapsulation-mode** { **transport** | **tunnel** }	Optional. Tunnel mode by default. Transport mode applies only when the source and destination IP addresses of data flows match those of the IPsec tunnel. IPsec for IPv6 routing protocols supports only the transport mode.

NOTE:

- Changes to an IPsec proposal affect only SAs negotiated after the changes. To apply the changes to existing SAs, execute the **reset ipsec sa** command to clear the SAs so that they can be set up using the updated parameters.
- Only when a security protocol is selected, can you configure security algorithms for it. For example, you can specify the ESP-specific security algorithms only when you select ESP as the security protocol. ESP supports three IP packet protection schemes: encryption only, authentication only, or both encryption and authentication. For the CC evaluation in FIPS mode, you must use both ESP encryption and authentication.

Configuring an IPsec policy

IPsec policies define which IPsec proposals should be used to protect which data flows. An IPsec policy is uniquely identified by its name and sequence number.

IPsec policies fall into two categories:

- **Manual IPsec policy**—The parameters are configured manually, such as the keys, the SPIs, and the IP addresses of the two ends in tunnel mode.
- **IPsec policy that uses IKE**—The parameters are automatically negotiated through IKE.

This section is not newly added. In this version, IKE negotiation was added and related commands that are executed in FIPS mode were modified. For more information, see "Command reference."

Configuring a manual IPsec policy

To guarantee successful SA negotiations, follow these guidelines when configuring manual IPsec policies at the two ends of an IPsec tunnel:

- The IPsec policies at the two ends must have IPsec proposals that use the same security protocols, security algorithms, and encapsulation mode.
- The remote IP address configured on the local end must be the same as the IP address of the remote end.
- At each end, configure parameters for both the inbound SA and the outbound SA and make sure that different SAs use different SPIs.
- The local inbound SA must use the same SPI and keys as the remote outbound SA. The same is true of the local outbound SA and remote inbound SA.
- The keys for the local and remote inbound and outbound SAs must be in the same format. For example, if the local inbound SA uses a key in characters, the local outbound SA and remote inbound and outbound SAs must use keys in characters.

Follow these guidelines when you configure an IPsec policy for an IPv6 routing protocol:

- You do not need to configure ACLs or IPsec tunnel addresses.
- Within a certain routed network scope, the IPsec proposal referenced by the IPsec policies on all devices must use the same security protocol, security algorithm, and packet encapsulation, and the SAs on all devices must use the same SPI and keys. For OSPFv3, the scope can be directly connected neighbors or an OSPFv3 area. For RIPng, the scope can be directly connected neighbors or a RIPng process. For IPv6 BGP, the scope can be directly connected neighbors or a peer group.
- All SAs (both inbound and outbound) within the routed network scope must use the same SPI and keys.
- Configure the keys on all routers within the routed network scope in the same format. For example, if you enter the keys in hexadecimal format on one router, do so across the routed network scope.

Before you configure a manual IPsec policy, configure ACLs used for identifying protected traffic and IPsec proposals. ACLs are not required for IPsec policies for an IPv6 protocol.

When you configure a manual IPsec policy, follow these guidelines:

- An IPsec policy can reference only one ACL. If you apply multiple ACLs to an IPsec policy, only the last one takes effect.
- A manual IPsec policy can reference only one IPsec proposal. To change an IPsec proposal for an IPsec policy, you must remove the proposal reference first.
- At each end, configure parameters for both the inbound and the outbound SAs, and make sure different SAs use different SPIs.
- If you configure a key in two modes: string and hexadecimal, the last configured one is used.
- You cannot change the creation mode of an IPsec policy from manual to through IKE, or vice versa. To create an IPsec policy that uses IKE, delete the manual IPsec policy, and then use IKE to configure an IPsec policy.

To configure a manual IPsec policy:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a manual IPsec policy and enter its view.	**ipsec policy** *policy-name seq-number* **manual**	By default, no IPsec policy exists.

Step	Command	Remarks
3. Assign an ACL to the IPsec policy.	**security acl** *acl-number*	Not needed for IPsec policies to be applied to IPv6 routing protocols and required for other applications. By default, an IPsec policy references no ACL. The ACL supports match criteria of the VPN attribute.
4. Assign an IPsec proposal to the IPsec policy.	**proposal** *proposal-name*	By default, an IPsec policy references no IPsec proposal.
5. Configure the two ends of the IPsec tunnel.	• Configure the local address of the tunnel: **tunnel local** *ip-address* • Configure the remote address of the tunnel: **tunnel remote** *ip-address*	Configuring the local address of the tunnel is not needed for IPsec policies to be applied to IPv6 routing protocols and required for other applications. Configuring the remote address of the tunnel is required. Both the local and remote addresses are not configured by default.
6. Configure the SPIs for the SAs.	**sa spi** { **inbound** | **outbound** } { **ah** | **esp** } *spi-number*	By default, SPIs for the SAs do not exist.
7. Configure keys for the SAs.	• Configure an authentication key in hexadecimal: **sa authentication-hex** { **inbound** | **outbound** } { **ah** | **esp** } [**cipher** | **simple**] *hex-key* • Configure an authentication key in characters: **sa string-key** { **inbound** | **outbound** } { **ah** | **esp** } [**cipher** | **simple**] *string-key* • Configure a key in characters for ESP: **sa string-key** { **inbound** | **outbound** } **esp** *string-key* • Configure an encryption key in hexadecimal for ESP: **sa encryption-hex** { **inbound** | **outbound** } **esp** [**cipher** | **simple**] *hex-key*	Use either command. For ESP, if you configure an authentication key, the system automatically generates an authentication key and an encryption key. If you configure an encryption key in characters for ESP, the system automatically generates an authentication key and an encryption key for ESP. The **sa string-key** command is not supported in FIPS mode.

Configuring an IPsec policy that uses IKE (only in FIPS mode)

To configure an IPsec policy that uses IKE, directly configure it by configuring the parameters in IPsec policy view.

Before you configure an IPsec policy that uses IKE, configure the ACLs and the IKE peer for the IPsec policy. For more information about IKE configuration, see the chapter "IKE configuration."

The parameters for the local and remote ends must match.

When you configure an IPsec policy that uses IKE, follow these guidelines:

- An IPsec policy can reference only one ACL. If you apply multiple ACLs to an IPsec policy, only the last one takes effect.
- With SAs to be established through IKE negotiation, an IPsec policy can reference up to six IPsec proposals. During negotiation, IKE searches for a fully matched IPsec proposal at the two ends of the expected IPsec tunnel. If no match is found, no SA can be set up and the packets expecting to be protected will be dropped.
- During IKE negotiation for an IPsec policy with PFS enabled, an additional key exchange is performed. If the local end uses PFS, the remote end must also use PFS for negotiation and both ends must use the same Diffie-Hellman (DH) group; otherwise, the negotiation will fail.
- An SA uses the global lifetime settings when it is not configured with lifetime settings in IPsec policy view. When negotiating to set up SAs, IKE uses the local lifetime settings or those proposed by the peer, whichever are smaller.
- You cannot change the creation mode of an IPsec policy directly. To create an IPsec policy in another creation mode, delete the current one and then configure a new IPsec policy.

To directly configure an IPsec policy that uses IKE:

Step	Command	Remark
1. Enter system view.	**system-view**	N/A
2. Create an IPsec policy that uses IKE and enter its view.	**ipsec policy** *policy-name* *seq-number* **isakmp**	By default, no IPsec policy exists.
3. Configure an IPsec connection name.	**connection-name** *name*	Optional. By default, no IPsec connection name is configured.
4. Assign an ACL to the IPsec policy.	**security acl** *acl-number*	By default, an IPsec policy references no ACL.
5. Assign IPsec proposals to the IPsec policy.	**proposal** *proposal-name*&<1-6>	By default, an IPsec policy references no IPsec proposal.
6. Specify an IKE peer for the IPsec policy.	**ike-peer** *peer-name*	An IPsec policy cannot reference any IKE peer that is already referenced by an IPsec profile, and vice versa.
7. Enable and configure the perfect forward secrecy feature for the IPsec policy.	**pfs** { **dh-group2** | **dh-group5** | **dh-group14** }	Optional. By default, the PFS feature is not used for negotiation. For more information about PFS, see the chapter "IKE configuration."
8. Set the SA lifetime.	**sa duration** { **time-based** *seconds* | **traffic-based** *kilobytes* }	Optional. By default, the global SA lifetime is used.
9. Enable the IPsec policy.	**policy enable**	Optional. Enabled by default.
10. Return to system view.	**quit**	N/A

Step	Command	Remark
11. Set the global SA lifetime.	**ipsec sa global-duration** { **time-based** *seconds* | **traffic-based** *kilobytes* }	Optional. 3600 seconds for time-based SA lifetime by default. 1843200 kilobytes for traffic-based SA lifetime by default.

Applying an IPsec policy group to an interface

This feature is supported only in FIPS mode.

An IPsec policy group is a collection of IPsec policies with the same name but different sequence numbers. In an IPsec policy group, an IPsec policy with a smaller sequence number has a higher priority.

You can apply an IPsec policy group to a logical or physical interface to protect certain data flows. To cancel the IPsec protection, remove the application of the IPsec policy group.

For each packet to be sent out an IPsec protected interface, the system looks through the IPsec policies in the IPsec policy group in ascending order of sequence numbers. If an IPsec policy matches the packet, the system uses the IPsec policy to protect the packet. If no match is found, the system sends the packet out without IPsec protection.

To apply an IPsec policy group to an interface:

Step	Command
1. Enter system view.	**system-view**
2. Enter interface view.	**interface** *interface-type interface-number*
3. Apply an IPsec policy group to the interface.	**ipsec policy** *policy-name*

NOTE:

- IPsec policies can be applied only to VLAN interfaces and Layer 3 Ethernet interfaces on the switch.
- An interface can reference only one IPsec policy group. An IPsec policy can be applied to only one interface.

Configuring the IPsec session idle timeout

This feature is supported only in FIPS mode.

An IPsec session is created when the first packet matching an IPsec policy arrives. Also created is an IPsec session entry, which records the quintuplet (source IP address, destination IP address, protocol number, source port, and destination port) and the matched IPsec tunnel.

An IPsec session is automatically deleted after the idle timeout expires.

Subsequent data flows search the session entries according to the quintuplet to find a matched item. If found, the data flows are processed according to the tunnel information; otherwise, they are processed according to the original IPsec process: search the policy group or policy at the interface, and then the matched tunnel.

The session processing mechanism of IPsec saves intermediate matching procedures, improving the IPsec forwarding efficiency.

To set the IPsec session idle timeout:

Step	Command	Remark
1. Enter system view.	**system-view**	N/A
2. Set the IPsec session idle timeout.	**ipsec session idle-time** *seconds*	Optional. 300 seconds by default.

Enabling ACL checking of de-encapsulated IPsec packets

This feature is supported only in FIPS mode.

In tunnel mode, the IP packet that was encapsulated in an inbound IPsec packet may not be an object that is specified by an ACL to be protected. For example, a forged packet is not an object to be protected. If you enable ACL checking of de-encapsulated IPsec packets, all packets failing the checking will be discarded, improving the network security.

To enable ACL checking of de-encapsulated IPsec packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable ACL checking of de-encapsulated IPsec packets.	**ipsec decrypt check**	Optional. Enabled by default.

Configuring the IPsec anti-replay function

This feature is supported only in FIPS mode.

The IPsec anti-replay function protects networks against anti-replay attacks by using a sliding window mechanism called anti-replay window. This function checks the sequence number of each received IPsec packet against the current IPsec packet sequence number range of the sliding window. If the sequence number is not in the current sequence number range, the packet is considered a replayed packet and is discarded.

IPsec packet de-encapsulation involves complicated calculation. De-encapsulation of replayed packets not only makes no sense, but also consumes large amounts of resources and degrades performance, resulting in DoS. IPsec anti-replay checking, when enabled, is performed before the de-encapsulation process, reducing resource waste.

In some cases, however, the sequence numbers of some normal service data packets may be out of the current sequence number range, and the IPsec anti-replay function may drop them as well, affecting the normal communications. If this happens, disable IPsec anti-replay checking or adjust the size of the anti-replay window as required.

To configure IPsec anti-replay checking:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable IPsec anti-replay checking.	**ipsec anti-replay check**	Optional. Enabled by default.
3. Set the size of the IPsec anti-replay window.	**ipsec anti-replay window** *width*	Optional. 32 by default.

△ **CAUTION:**

- IPsec anti-replay checking is enabled by default. Do not disable it unless it needs to be disabled.
- A wider anti-replay window results in higher resource cost and more system performance degradation, which is against the original intention of the IPsec anti-replay function. Specify an anti-replay window size that is as small as possible.

NOTE:

IPsec anti-replay checking does not affect manually created IPsec SAs. According to the IPsec protocol, only IPsec SAs negotiated by IKE support anti-replay checking.

Configuring packet information pre-extraction

This feature is supported only in FIPS mode.

If you apply both an IPsec policy and QoS policy to an interface, by default, the interface first uses IPsec and then QoS to process IP packets, and QoS classifies packets by the headers of IPsec-encapsulated packets. If you want QoS to classify packets by the headers of the original IP packets, enable the packet information pre-extraction feature.

For more information about QoS policy and classification, see *ACL and QoS Configuration Guide.*

To configure packet information pre-extraction:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter IPsec policy view.	**ipsec policy** *policy-name seq-number* [**isakmp** | **manual**]	Configure either command.
3. Enable packet information pre-extraction.	**qos pre-classify**	Disabled by default.

Displaying and maintaining IPsec

To do…	Use the command…	Remarks
Display IPsec policy information	**display ipsec policy** [**brief** | **name** *policy-name* [*seq-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display IPsec proposal information	**display ipsec proposal** [*proposal-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display IPsec SA information	**display ipsec sa** [**brief** | **policy** *policy-name* [*seq-number*] | **remote** *ip-address*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display IPsec session information	**display ipsec session** [**tunnel-id** *integer*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view Only supported in FIPS mode.
Display IPsec packet statistics	**display ipsec statistics** [**tunnel-id** *integer*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

To do…	Use the command…	Remarks
Display IPsec tunnel information	**display ipsec tunnel** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Clear SAs	**reset ipsec sa** [**parameters** *dest-address protocol spi* | **policy** *policy-name* [*seq-number*] | **remote** *ip-address*]	Available in user view
Clear IPsec sessions	**reset ipsec session** [**tunnel-id** *integer*]	Available in user view Only supported in FIPS mode.
Clear IPsec statistics	**reset ipsec statistics**	Available in user view

IKE-based IPsec tunnel for IPv4 packets configuration example

Network requirements

As shown in Figure 2, configure an IPsec tunnel between Switch A and Switch B to protect data flows between Switch A and Switch B. Configure the tunnel to use the security protocol ESP, the encryption algorithm AES-CBC-128, and the authentication algorithm HMAC-SHA1-96.

Figure 2 Network diagram

Configuration procedure

1. Configure Switch A:

Assign an IP address to VLAN-interface 1.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 2.2.2.1 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

Define an ACL to identify data flows from Switch A to Switch B.

```
[SwitchA] acl number 3101
[SwitchA-acl-adv-3101] rule 0 permit ip source 2.2.2.1 0 destination 2.2.3.1 0
[SwitchA-acl-adv-3101] rule 5 permit ip source 2.2.3.1 0 destination 2.2.2.1 0
[SwitchA-acl-adv-3101] quit
```

Create an IPsec proposal named **tran1**.

```
[SwitchA] ipsec proposal tran1
```

Specify the encapsulation mode as **tunnel**.

```
[SwitchA-ipsec-proposal-tran1] encapsulation-mode tunnel
```

Specify the security protocol as **ESP**.

```
[SwitchA-ipsec-proposal-tran1] transform esp
```

Specify the algorithms for the proposal.

```
[SwitchA-ipsec-proposal-tran1] esp encryption-algorithm aes 128
[SwitchA-ipsec-proposal-tran1] esp authentication-algorithm sha1
[SwitchA-ipsec-proposal-tran1] quit
```

Configure the IKE peer.

```
[SwitchA] ike peer peer
[SwitchA-ike-peer-peer] pre-shared-key Ab12<><>
[SwitchA-ike-peer-peer] remote-address 2.2.3.1
[SwitchA-ike-peer-peer] quit
```

Create an IPsec policy that uses IKE for IPsec SA negotiation.

```
[SwitchA] ipsec policy map1 10 isakmp
```

Apply the IPsec proposal.

```
[SwitchA-ipsec-policy-isakmp-map1-10] proposal tran1
```

Apply the ACL.

```
[SwitchA-ipsec-policy-isakmp-map1-10] security acl 3101
```

Apply the IKE peer.

```
[SwitchA-ipsec-policy-isakmp-map1-10] ike-peer peer
[SwitchA-ipsec-policy-isakmp-map1-10] quit
```

Apply the IPsec policy group to VLAN-interface 1.

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ipsec policy map1
```

2. Configure Switch B:

Assign an IP address to VLAN-interface 1.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 2.2.3.1 255.255.255.0
[SwitchB-Vlan-interface1] quit
```

Define an ACL to identify data flows from Switch B to Switch A.

```
[SwitchB] acl number 3101
[SwitchB-acl-adv-3101] rule 0 permit ip source 2.2.3.1 0 destination 2.2.2.1 0
[SwitchB-acl-adv-3101] rule 5 permit ip source 2.2.2.1 0 destination 2.2.3.1 0
[SwitchB-acl-adv-3101] quit
```

Create an IPsec proposal named **tran1**.

```
[SwitchB] ipsec proposal tran1
```

Specify the encapsulation mode as **tunnel**.

```
[SwitchB-ipsec-proposal-tran1] encapsulation-mode tunnel
```

Specify the security protocol as **ESP**.

```
[SwitchB-ipsec-proposal-tran1] transform esp
```

Specify the algorithms for the proposal.

```
[SwitchB-ipsec-proposal-tran1] esp encryption-algorithm aes 128
[SwitchB-ipsec-proposal-tran1] esp authentication-algorithm sha1
[SwitchB-ipsec-proposal-tran1] quit
```

Configure the IKE peer.

```
[SwitchB] ike peer peer
[SwitchB-ike-peer-peer] pre-shared-key Ab12<><>
[SwitchB-ike-peer-peer] remote-address 2.2.2.1
[SwitchB-ike-peer-peer] quit
```

Create an IPsec policy that uses IKE for IPsec SA negotiation.

```
[SwitchB] ipsec policy use1 10 isakmp
```

Apply the ACL.

```
[SwitchB-ipsec-policy-isakmp-use1-10] security acl 3101
```

Apply the IPsec proposal.

```
[SwitchB-ipsec-policy-isakmp-use1-10] proposal tran1
```

Apply the IKE peer.

```
[SwitchB-ipsec-policy-isakmp-use1-10] ike-peer peer
[SwitchB-ipsec-policy-isakmp-use1-10] quit
```

Apply the IPsec policy group to VLAN-interface 1.

```
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ipsec policy use1
```

3. Verifying the configuration

After the previous configuration, send traffic from Switch B to Switch A. Switch A starts IKE negotiation with Switch B when receiving the first packet. If IKE negotiation is successful and SAs are set up, the traffic between the two switches will be IPsec protected.

Command reference

Modified command: ah authentication-algorithm

Old syntax

ah authentication-algorithm { **md5** | **sha1** }

undo ah authentication-algorithm

New syntax

In non-FIPS mode:

ah authentication-algorithm { **md5** | **sha1** }

undo ah authentication-algorithm

In FIPS mode:

ah authentication-algorithm sha1

undo ah authentication-algorithm

Views

IPsec proposal view

Default command level

2: System level

Parameters

md5: Uses MD5 algorithm. This keyword is not available for FIPS mode.

sha1: Uses SHA1.

Change description

After modification: In FIPS mode, MD5 algorithm is not supported. By default, AH uses SHA1 algorithm.

New command: connection-name

Use **connection-name** to configure an IPsec connection name. This name functions only as a description of the IPsec policy.

Use **undo connection-name** to restore the default.

Syntax

connection-name *name*

undo connection-name

Default

No IPsec connection name is configured.

Views

IPsec policy view

Default command level

2: System level

Parameters

name: IPsec connection name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

This command is supported only in FIPS mode.

Example

Set IPsec connection name to **aaa**.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 1 isakmp
[Sysname-ipsec-policy-isakmp-policy1-1] connection-name aaa
```

Modified command: display ipsec sa

Old syntax

display ipsec sa [**brief** | **policy** *policy-name* [*seq-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

New syntax

display ipsec sa [**brief** | **policy** *policy-name* [*seq-number*] | **remote** *ip-address*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

brief: Displays brief information about all IPsec SAs.

policy: Displays detailed information about IPsec SAs created by using a specified IPsec policy.

policy-name: Name of the IPsec policy, a string 1 to 15 characters.

seq-number: Sequence number of the IPsec policy, in the range 1 to 65535.

remote *ip-address*: Displays detailed information about the IPsec SA with a specified remote address. This option is supported only in FIPS mode.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Change description

After modification: This command displays information about the IPsec SA with a specified remote address.

New command: display ipsec session

Use **display ipsec session** to display information about IPsec sessions.

Syntax

display ipsec session [**tunnel-id** *integer*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

integer: ID of the IPsec tunnel, in the range 1 to 2000000000.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Usage guidelines

This command is supported only in FIPS mode.

If you do not specify any parameters, the command displays information about all IPsec sessions.

IPsec can find matched tunnels directly by session, reducing the intermediate matching procedures and improving the forwarding efficiency. A session is identified by the quintuplet of protocol, source IP address, source port, destination IP address, and destination port.

Examples

Display information about all IPsec sessions.

```
<Sysname> display ipsec session
    ------------------------------------------------------------
    total sessions : 2
    ------------------------------------------------------------
    tunnel-id : 3
    session idle time/total duration (sec) : 36/300

    session flow :      (8 times matched)
        Sour Addr : 15.15.15.1             Sour Port:    0  Protocol : 1
        Dest Addr : 15.15.15.2             Dest Port:    0  Protocol : 1

    ------------------------------------------------------------
```

```
tunnel-id : 4
session idle duration/total duration (sec) : 7/300

session flow :      (3 times matched)
    Sour Addr : 12.12.12.1            Sour Port:    0  Protocol : 1
    Dest Addr : 13.13.13.1            Dest Port:    0  Protocol : 1
```

Display information about the session with an IPsec tunnel ID of 5.

```
<Sysname> display ipsec session tunnel-id 5
    ------------------------------------------------------------
    total sessions : 1
    ------------------------------------------------------------
    tunnel-id : 5
    session idle time/total duration (sec) : 30/300

    session flow :      (4 times matched)
        Sour Addr : 12.12.12.2            Sour Port:    0  Protocol : 1
        Dest Addr : 13.13.13.2            Dest Port:    0  Protocol : 1
```

Table 1 Command output

Field	Description
total sessions	Total number of IPsec sessions.
tunnel-id	IPsec tunnel ID, same as the connection-id of the IPsec SA.
session idle time	Idle duration of the IPsec session in seconds.
total duration	Lifetime of the IPsec session in seconds, defaulted to 300 seconds.
session flow	Flow information of the IPsec session.
times matched	Total number of packets matching the IPsec session.
Sour Addr	Source IP address of the IPsec session.
Dest Addr	Destination IP address of the IPsec session.
Sour Port	Source port number of the IPsec session.
Dest Port	Destination port number of the IPsec session.
Protocol	Protocol number of the IPsec protected data flow, for example, 1 for ICMP.

Related commands

reset ipsec session

Modified command: esp authentication-algorithm

Old syntax

esp authentication-algorithm { **md5** | **sha1** }

undo esp authentication-algorithm

New syntax

In non-FIPS mode:

esp authentication-algorithm { **md5** | **sha1** }

undo esp authentication-algorithm

In FIPS mode:

esp authentication-algorithm sha1

undo esp authentication-algorithm

Views

IPsec proposal view

Default command level

2: System level

Parameters

md5: Uses the MD5 algorithm, which uses a 128-bit key. The FIPS mode does not support MD5.

sha1: Uses the SHA1 algorithm, which uses a 160-bit key.

Change description

After modification: In FIPS mode, the MD5 algorithm is not supported. By default, ESP uses SHA1 authentication algorithm.

Modified command: esp encryption-algorithm

Old syntax

esp encryption-algorithm { **3des | aes** [*key-length*] **| des** }

undo esp encryption-algorithm

New syntax

In non-FIPS mode:

esp encryption-algorithm { **3des | aes** [*key-length*] **| des** }

undo esp encryption-algorithm

In FIPS mode:

esp encryption-algorithm aes [*key-length*]

undo esp encryption-algorithm

Views

IPsec proposal view

Default command level

2: System level

Parameters

3des: Uses triple DES (3DES) in cipher block chaining (CBC) mode as the encryption algorithm. The 3DES algorithm uses a 168-bit key for encryption. The FIPS mode does not support this algorithm.

aes: Uses the Advanced Encryption Standard (AES) in CBC mode as the encryption algorithm. The AES algorithm uses a 128- bit, 192-bit, or 256-bit key for encryption.

key-length: Key length for the AES algorithm, which can be 128, 192, and 256 and defaults to 128. This argument is for AES only.

des: Uses the Data Encryption Standard (DES) in CBC mode as the encryption algorithm. The DES algorithm uses a 56-bit key for encryption. This keyword is not available for FIPS mode.

Change description

After modification: In FIPS mode, the 3DES and DES algorithms are not supported. By default, ESP uses AES-128 encryption algorithm.

New command: ike-peer (IPsec policy view)

Use **ike-peer** to reference an IKE peer in an IPsec policy configured through IKE negotiation.

Use **undo ike peer** to remove the reference.

Syntax

ike-peer *peer-name*

undo ike-peer *peer-name*

Views

IPsec policy view

Default command level

2: System level

Parameters

peer-name: IKE peer name, a string of 1 to 32 characters.

Usage guidelines

This command is supported only in FIPS mode.

This command applies to only IKE negotiation mode.

Examples

Configure a reference to an IKE peer in an IPsec policy.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 10 isakmp
[Sysname-ipsec-policy-isakmp-policy1-10] ike-peer peer1
```

Related commands

ipsec policy

New command: ipsec anti-replay check

Use **ipsec anti-replay check** to enable IPsec anti-replay checking.

Use **undo ipsec anti-replay check** to disable IPsec anti-replay checking.

Syntax

ipsec anti-replay check

undo ipsec anti-replay check

Default

IPsec anti-replay checking is enabled.

Views

System view

Default command level

2: System level

Usage guidelines

This command is supported only in FIPS mode.

Examples

Enable IPsec anti-replay checking.

```
<Sysname> system-view
[Sysname] ipsec anti-replay check
```

New command: ipsec anti-replay window

Use **ipsec anti-replay window** to set the size of the anti-replay window.

Use **undo ipsec anti-replay window** to restore the default.

Syntax

ipsec anti-replay window *width*

undo ipsec anti-replay window

Default

The size of the anti-replay window is 32.

Views

System view

Default command level

2: System level

Parameters

width: Size of the anti-replay window. It can be 32, 64, 128, 256, 512, or 1024.

Usage guidelines

This command is supported only in FIPS mode.

Your configuration affects only IPsec SAs negotiated later.

Examples

Set the size of the anti-replay window to 64.

```
<Sysname> system-view
[Sysname] ipsec anti-replay window 64
```

New command: ipsec decrypt check

Use **ipsec decrypt check** to enable ACL checking of de-encapsulated IPsec packets.

Use **undo ipsec decrypt check** to disable ACL checking of de-encapsulated IPsec packets.

Syntax

ipsec decrypt check

undo ipsec decrypt check

Default

ACL checking of de-encapsulated IPsec packets is enabled.

Views

System view

Default command level

2: System level

Usage guidelines

This command is supported only in FIPS mode.

Examples

Enable ACL checking of de-encapsulated IPsec packets.

```
<Sysname> system-view
[Sysname] ipsec decrypt check
```

New command: ipsec policy (interface view)

Use **ipsec policy** to apply an IPsec policy group to an interface.

Use **undo ipsec policy** to remove the application.

Syntax

ipsec policy *policy-name*

undo ipsec policy [*policy-name*]

Views

Interface view

Default command level

2: System level

Parameters

policy-name: Name of the existing IPsec policy group to be applied to the interface, a string of 1 to 15 characters.

Usage guidelines

This command is supported only in FIPS mode.

IPsec policies can be applied only to VLAN interfaces and Layer 3 Ethernet interfaces on the switch.

Only one IPsec policy group can be applied to an interface. To apply another IPsec policy group to the interface, remove the original application first. An IPsec policy can be applied to only one interface.

With an IPsec policy group applied to an interface, the system uses each IPsec policy in the group to protect certain data flows.

For each packet to be sent out an IPsec protected interface, the system checks the IPsec policies of the IPsec policy group in the ascending order of sequence numbers. If it finds an IPsec policy whose ACL matches the packet, it uses the IPsec policy to protect the packet. If it finds no ACL of the IPsec policies matches the packet, it does not provide IPsec protection for the packet and sends the packet out directly.

Examples

Apply IPsec policy group **pg1** to interface VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ipsec policy pg1
```

Related commands

ipsec policy (system view)

Modified command: ipsec policy (system view)

Old syntax

ipsec policy *policy-name seq-number* [**manual**]

undo ipsec policy *policy-name* [*seq-number*]

New syntax

ipsec policy *policy-name seq-number* [**isakmp** | **manual**]

undo ipsec policy *policy-name* [*seq-number*]

Views

System view

Default command level

2: System level

Parameters

policy-name: Name for the IPsec policy, a case-insensitive string of 1 to 15 characters, including letters and digits. No minus sign (-) can be included.

seq-number: Sequence number for the IPsec policy, in the range of 1 to 65535.

isakmp: Sets up SAs through IKE negotiation. This keyword is supported only in FIPS mode.

manual: Sets up SAs manually.

Change description

After modification: This command can create an IPsec policy through IKE negotiation and enter its view.

Modified command: ipsec proposal

Syntax

ipsec proposal *proposal-name*

undo ipsec proposal *proposal-name*

Views

System view

Default command level

2: System level

Parameters

proposal-name: Name for the proposal, a case-insensitive string of 1 to 32 characters .

Change description

After modification: In FIPS mode, this command can create a new IPsec proposal, with default protocol as ESP, encryption algorithm AES-128, and authentication algorithm SHA1.

New command: ipsec sa global-duration

Use **ipsec sa global-duration** to configure the global SA lifetime.

Use **undo ipsec sa global-duration** to restore the default.

Syntax

ipsec sa global-duration { **time-based** *seconds* | **traffic-based** *kilobytes* }

undo ipsec sa global-duration { **time-based** | **traffic-based** }

Default

The time-based global SA lifetime is 3,600 seconds, and the traffic-based global SA lifetime is 1843200 kilobytes.

Views

System view

Default command level

2: System level

Parameters

seconds: Time-based global SA lifetime in seconds, in the range 180 to 604800.

kilobytes: Traffic-based global SA lifetime in kilobytes, in the range 2560 to 4294967295.

Usage guidelines

This command is supported only in FIPS mode.

When negotiating to set up an SA, IKE prefers the lifetime of the IPsec policy that it uses. If the IPsec policy is not configured with its own lifetime, IKE uses the global SA lifetime.

When negotiating to set up an SA, IKE prefers the shorter one of the local lifetime and that proposed by the remote.

You can configure both a time-based and a traffic-based global SA lifetime. An SA is aged out when it has existed for the specified time period or has processed the specified volume of traffic.

The SA lifetime applies to only IKE negotiated SAs. It is not effective for manually configured SAs.

For CC evaluation in FIPS mode, if IPsec uses IKE automatic negotiation, when IPsec SAs reach the traffic-based lifetime, IPsec notifies IKE to re-perform phase 1 and phase 2 negotiations.

Examples

Set the time-based global SA lifetime to 7200 seconds (2 hours).

```
<Sysname> system-view
[Sysname] ipsec sa global-duration time-based 7200
```

Set the traffic-based global SA lifetime to 10240 kilobytes (10 Mbytes).

```
[Sysname] ipsec sa global-duration traffic-based 10240
```

Related commands

sa duration

New command: ipsec session idle-time

Use **ipsec session idle-time** to set the idle timeout for IPsec sessions.

Use **undo ipsec session idle-time** to restore the default.

Syntax

ipsec session idle-time *seconds*

undo ipsec session idle-time

Default

The IPsec session idle timeout is 300 seconds.

Views

System view

Default command level

2: System level

Parameters

Seconds: IPsec session idle timeout in seconds, in the range of 60 to 3,600.

Usage guidelines

This command is supported only in FIPS mode.

Examples

Set the IPsec session idle timeout to 600 seconds.

```
<Sysname> system-view
[Sysname] ipsec session idle-time 600
```

New command: pfs

Use **pfs** to enable and configure the perfect forward secrecy (PFS) feature so that the system uses the feature when employing the IPsec policy to initiate a negotiation.

Use **undo pfs** to remove the configuration.

Syntax

pfs { **dh-group2 | dh-group5 | dh-group14** }

undo pfs

Default

The PFS feature is not used for negotiation

Views

IPsec policy view

Default command level

2: System level

Parameters

dh-group2: Uses 1024-bit Diffie-Hellman group.

dh-group5: Uses 1536-bit Diffie-Hellman group.

dh-group14: Uses 2048-bit Diffie-Hellman group.

Usage guidelines

This command is supported only in FIPS mode.

In terms of security and necessary calculation time, the following four groups are in the descending order: 2048-bit Diffie-Hellman group (**dh-group14**), 1536-bit Diffie-Hellman group (**dh-group5**), and 1024-bit Diffie-Hellman group (**dh-group2**).

This command allows IPsec to perform an additional key exchange process during the negotiation phase 2, providing an additional level of security.

The local Diffie-Hellman group must be the same as that of the peer.

Examples

Enable and configure PFS for IPsec policy **policy1**.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 200 isakmp
[Sysname-ipsec-policy-isakmp-policy1-200] pfs dh-group2
```

Related commands

ipsec policy (system view)

New command: policy enable

Use **policy enable** to enable the IPsec policy.

Use **undo policy enable** to disable the IPsec policy.

Syntax

policy enable

undo policy enable

Default

The IPsec policy is enabled.

Views

IPsec policy view

Default command level

2: System level

Usage guidelines

This command is supported only in FIPS mode.

If the IPsec policy is not enabled for the IKE peer, the peer cannot take part in the IKE negotiation.

Examples

Enable the IPsec policy with the name policy1 and sequence number 100.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 isakmp
[Sysname-ipsec-policy-isakmp-policy1-100] policy enable
```

Related commands

ipsec policy (system view)

Modified command: proposal (IPsec policy view)

Old syntax

proposal *proposal-name*

undo proposal [*proposal-name*]

New syntax

proposal *proposal-name*&<1-6>

undo proposal [*proposal-name*]

Views

IPsec policy view

Default command level

2: System level

Parameters

proposal-name&<1-6>: Name of the IPsec proposal, a string of 1 to 32 characters. &<1-6> means that you can specify the *proposal-name* argument for up to six times.

Change description

Before modification: Because parameters of the security policy are only manually configured, only one security proposal can be referenced.

After modification: Because parameters of the security policy are automatically negotiated through IKE, up to six security proposals can be referenced, and IKE searches for a fully matched IPsec proposal during negotiation.

New command: qos pre-classify

Use **qos pre-classify** to enable packet information pre-extraction.

Use **undo qos pre-classify** to restore the default.

Syntax

qos pre-classify

undo qos pre-classify

Default

Packet information pre-extraction is disabled.

Views

IPsec policy view

Default command level

2: System level

Usage guidelines

This command is supported only in FIPS mode.

With the packet information pre-extraction feature enabled, QoS classifies a packet based on the header of the original IP packet—the header of the IP packet that has not been encapsulated by IPsec.

Examples

Enable packet information pre-extraction.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 isakmp
[Sysname-ipsec-policy-isakmp-policy1-100] qos pre-classify
```

Related commands

ipsec policy (system view)

Modified command: reset ipsec sa

Use **reset ipsec sa** to clear IPsec SAs.

Old syntax

reset ipsec sa [**policy** *policy-name* [*seq-number*]]

New syntax

reset ipsec sa [**parameters** *dest-address protocol spi* **|** **policy** *policy-name* [*seq-number*] **|** **remote** *ip-address*]

Views

User view

Default command level

2: System level

Parameters

parameters: Specifies IPsec SAs that use the specified destination IP address, security protocol, and SPI. This keyword is supported only in FIPS mode.

dest-address: Destination address, in dotted decimal notation.

protocol: Security protocol, which can be keyword **ah** or **esp**, case insensitive.

spi: Security parameter index, in the range 256 to 4294967295.

policy: Specifies IPsec SAs that use an IPsec policy.

policy-name: Name of the IPsec policy , a case-insensitive string of 1 to 15 characters, including letters and digits.

seq-number: Sequence number of the IPsec policy, in the range 1 to 65535. If no *seq-number* is specified, all the policies in the IPsec policy group named *policy-name* are specified.

remote: Specifies SAs to or from a remote address, in dotted decimal notation. This keyword is supported only in FIPS mode.

Usage guidelines

Immediately after a manually set up SA is cleared, the system automatically sets up a new SA based on the parameters of the IPsec policy. After IKE negotiated SAs are cleared, the system sets up new SAs only when IKE negotiation is triggered by interesting packets.

IPsec SAs appear in pairs. If you specify the **parameters** keyword to clear an IPsec SA, the IPsec SA in the other direction is also automatically cleared.

If you do not specify any parameter, the command clears all IPsec SAs.

Change description

Before modification: This command clears only IPsec SAs that are manually created.

After modification: This command clears IPsec SAs that are manually created or created through IKE negotiation.

New command: reset ipsec session

Use **reset ipsec session** to clear the sessions of a specified IPsec tunnel or all IPsec tunnels.

Syntax

reset ipsec session [**tunnel-id** *integer*]

Views

User view

Default command level

2: System level

Parameters

integer: ID of the IPsec tunnel, in the range 1 to 2000000000.

Usage guidelines

This command is supported only in FIPS mode.

Examples

Clear all IPsec sessions.

```
<Sysname> reset ipsec session
```

Clear the sessions of IPsec tunnel 5.

```
<Sysname> reset ipsec session tunnel-id 5
```

Related commands

display ipsec session

New command: sa duration

Use **sa duration** to set an SA lifetime for the IPsec policy.

Use **undo sa duration** to restore the default.

Syntax

sa duration { **time-based** *seconds* **| traffic-based** *kilobytes* }

undo sa duration { **time-based | traffic-based** }

Default

The SA lifetime of an IPsec policy equals the current global SA lifetime.

The time-based global SA lifetime is 3600 seconds, and traffic-based SA lifetime is 1843200 kilobytes.

Views

IPsec policy view

Default command level

2: System level

Parameters

seconds: Time-based SA lifetime in seconds, in the range 180 to 604800.

kilobytes: Traffic-based SA lifetime in kilobytes, in the range 2560 to 4294967295.

Usage guidelines

This command is supported only in FIPS mode.

When negotiating to set up an SA, IKE prefers the lifetime settings of the IPsec policy that it uses. If the IPsec policy or IPsec proposal is not configured with its own lifetime settings, IKE uses the global SA lifetime settings, which are configured with the **ipsec sa global-duration** command.

When negotiating to set up an SA, IKE prefers the shorter ones of the local lifetime settings and those proposed by the remote.

The SA lifetime applies to only IKE negotiated SAs. It is not effective for manually configured SAs.

For CC evaluation in FIPS mode, if IPsec uses IKE automatic negotiation, when IPsec SAs reach the traffic-based lifetime, the system notifies IKE to re-perform phase 1 and phase 2 negotiations.

Related commands: **ipsec sa global-duration**, **ipsec policy (system view)**.

Examples

Set the SA lifetime for IPsec **policy1** to 7200 seconds (two hours).

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 isakmp
[Sysname-ipsec-policy-isakmp-policy1-100] sa duration time-based 7200
```

Set the SA lifetime for IPsec policy **policy1** to 20480 kilobytes (20 Mbytes).

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 isakmp
[Sysname-ipsec-policy-isakmp-policy1-100] sa duration traffic-based 20480
```

Modified command: sa string-key

Syntax

sa string-key { **inbound | outbound** } { **ah | esp** } [**cipher | simple**] *string-key*

undo sa string-key { **inbound | outbound** } { **ah | esp** }

Views

IPsec policy view

Default command level

2: System level

Parameters

inbound: Specifies the inbound SA through which IPsec processes the received packets.

outbound: Specifies the outbound SA through which IPsec processes the packets to be sent.

ah: Uses AH.

esp: Uses ESP.

cipher: Sets a ciphertext key.

simple: Sets a plaintext key.

string-key: Specifies the key string. This argument is case sensitive. If **cipher** is specified, it must be a ciphertext string of 1 to 373 characters. If **simple** is specified, it must be a string of 1 to 255 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string. For different algorithms, enter strings of any length in the specified range. Using this key string, the system automatically generates keys meeting the algorithm requirements. When the protocol is ESP, the system generates the keys for both the authentication algorithm and encryption algorithm.

Change description

After modification: This command is not supported in FIPS mode.

New command: security acl

Use **security acl** to specify the ACL for the IPsec policy to reference.

Use **undo security acl** to remove the configuration.

Syntax

security acl *acl-number*

undo security acl

Default

An IPsec policy references no ACL.

Views

IPsec policy view

Default command level

2: System level

Parameters

acl-number: Number of the ACL for the IPsec policy to reference, in the range 3000 to 3999.

Usage guidelines

This command is supported only in FIPS mode.

With an IKE-dependent IPsec policy configured, data flows can be protected in standard mode. In standard mode, one tunnel protects one data flow. The data flow permitted by each ACL rule is protected by one tunnel that is established separately for it.

When you specify an ACL for an IPsec policy, follow these guidelines:

- You must create a mirror image ACL rule at the remote end for each ACL rule created at the local end. Otherwise, IPsec may protect traffic in only one direction.
- The ACL cannot be deployed to an aggregate interface or a tunnel interface.
- You cannot specify multiple ACLs for one IPsec policy or one ACL for multiple IPsec policies. To configure ACL rules you want to deploy for an IPsec policy, you must configure all of them in one ACL and specify the ACL for the IPsec policy.
- You can specify only one ACL for an IPsec policy. To deploy multiple ACL rules, configure the ACL rules in one ACL, and then reference the ACL in an IPsec policy.
- ACLs referenced by IPsec cannot be used by other services.

Examples

Configure IPsec policy policy1 to reference ACL 3001.

```
<Sysname> system-view
[Sysname] acl number 3001
[Sysname-acl-adv-3001] rule permit tcp source 10.1.1.0 0.0.0.255 destination 10.1.2.0
0.0.0.255
[Sysname-acl-adv-3001] quit
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] security acl 3001
```

Related commands

ipsec policy (system view)

Modified command: transform

Syntax

transform { **ah** | **ah-esp** | **esp** }

undo transform

Views

IPsec proposal view

Default command level

2: System level

Parameters

ah: Uses the AH protocol.

ah-esp: Uses ESP first and then AH.

esp: Uses the ESP protocol.

Change description

After modification: In FIPS mode,,

- If AH is used, the default authentication algorithm is SHA1.
- If ESP is used, the default encryption and authentication algorithms are AES-128 and SHA1, respectively.
- If both AH and ESP are used, AH uses the SHA1 authentication algorithm by default, and ESP uses the AES-128 encryption algorithm and the SHA1 authentication algorithm by default.

New command: tunnel local

Use **tunnel local** to configure the local address of an IPsec tunnel.

Use **undo tunnel local** to remove the configuration.

Syntax

tunnel local *ip-address*

undo tunnel local

Default

No local address is configured for an IPsec tunnel.

Views

IPsec policy view

Default command level

2: System level

Parameters

ip-address: Local address for the IPsec tunnel.

Usage guidelines

This command is supported only in FIPS mode.

The local address, if not configured, will be the address of the interface to which the IPsec policy is applied.

Examples

Set the local address of the IPsec tunnel to the address of Loopback 0, 10.0.0.1.

```
<Sysname> system-view
[Sysname] interface loopback 0
[Sysname-LoopBack0] ip address 10.0.0.1 32
[Sysname-LoopBack0] quit
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] tunnel local 10.0.0.1
```

Related commands

ipsec policy (system view)

New command: tunnel remote

Use **tunnel remote** to configure the remote address of an IPsec tunnel.

Use **undo tunnel remote** to remove the configuration.

Syntax

tunnel remote *ip-address*

undo tunnel remote [*ip-address*]

Default

No remote address is configured for the IPsec tunnel.

Views

IPsec policy view

Default command level

2: System level

Parameters

ip-address: Remote address for the IPsec tunnel.

Usage guidelines

This command is supported only in FIPS mode.

If you configure the remote address repeatedly, the last one takes effect.

An IPsec tunnel is established between the local and remote ends. The remote IP address of the local end must be the same as that of the local IP address of the remote end.

Examples

Set the remote address of the IPsec tunnel to 10.1.1.2.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 10 manual
[Sysname-ipsec-policy-policy1-10] tunnel remote 10.1.1.2
```

Related commands

ipsec policy (system view)

New feature: IKE

NOTE:

This chapter is applicable to only the switches in FIPS mode.

IKE overview

Built on a framework defined by the Internet Security Association and Key Management Protocol (ISAKMP), Internet Key Exchange (IKE) provides automatic key negotiation and SA establishment services for IPsec, simplifying the application, management, configuration and maintenance of IPsec dramatically.

Instead of transmitting keys directly across a network, IKE peers transmit keying materials between them, and calculate shared keys respectively. Even if a third party captures all exchanged data for calculating the keys, it cannot calculate the keys.

IKE security mechanism

IKE has a series of self-protection mechanisms and supports secure identity authentication, key distribution, and IPsec SA establishment on insecure networks.

Data authentication

Data authentication involves two concepts:

- **Identity authentication**—Mutual identity authentication between peers. Two authentication methods are available: pre-shared key authentication and PKI-based digital signature authentication (RSA signature).
- **Identity protection**—Encrypts the identity information with the generated keys before sending the information.

DH

The Diffie-Hellman (DH) algorithm is a public key algorithm. With this algorithm, two peers can exchange keying material and then use the material to calculate the shared keys. Due to the decryption complexity, a third party cannot decrypt the keys even after intercepting all keying materials.

PFS

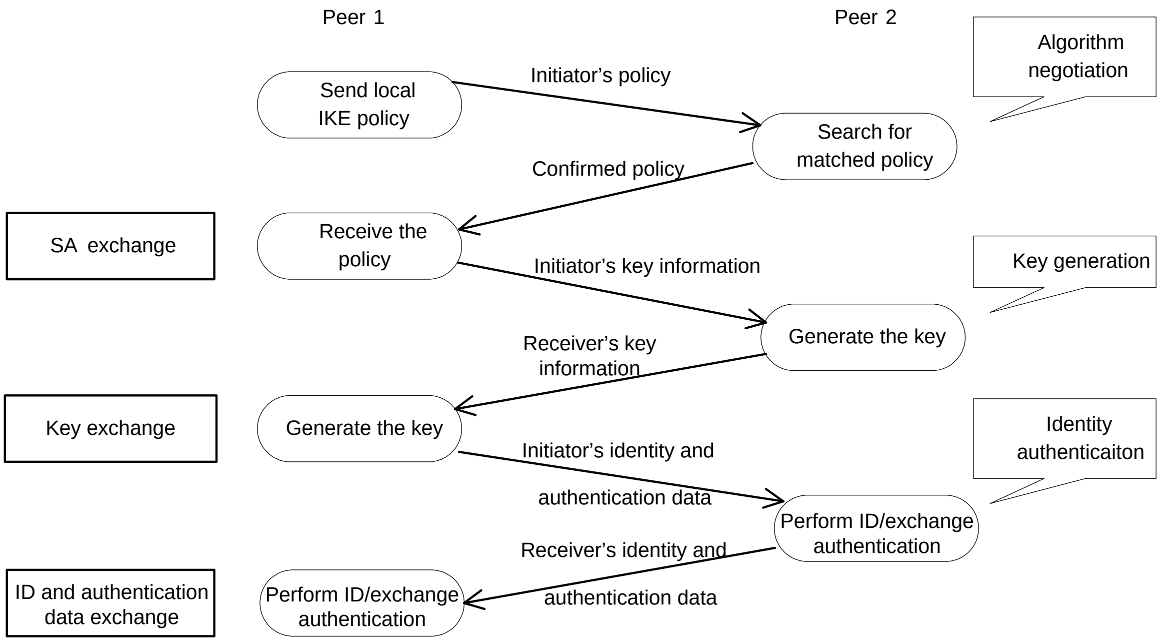
The Perfect Forward Secrecy (PFS) feature is a security feature based on the DH algorithm. By making sure keys have no derivative relations, it guarantees a broken key brings no threats to other keys. For IPsec, PFS is implemented by adding an additional key exchange at IKE negotiation phase 2.

IKE operation

IKE negotiates keys and establishes SAs for IPsec in two phases:

1. **Phase 1**—The two peers establish an ISAKMP SA, a secure, authenticated channel for communication.
2. **Phase 2**—Using the ISAKMP SA established in phase 1, the two peers negotiate to establish IPsec SAs.

Figure 3 IKE exchange process in main mode



As shown in Figure 3, the main mode of IKE negotiation in phase 1 involves three pairs of messages:

- SA exchange, used for negotiating the security policy.
- Key exchange, used for exchanging the Diffie-Hellman public value and other values like the random number. Key data is generated in this stage.
- ID and authentication data exchange, used for identity authentication and authentication of data exchanged in phase 1.

IKE functions

IKE provides the following functions for IPsec:

- Automatically negotiates IPsec parameters such as the keys.

- Performs DH exchange when establishing an SA, making sure that each SA has a key independent of other keys.
- Automatically negotiates SAs when the sequence number in the AH or ESP header overflows, making sure that IPsec provides the anti-replay service normally by using the sequence number.
- Provides end-to-end dynamic authentication.
- Identity authentication and management of peers influence IPsec deployment. A large-scale IPsec deployment needs the support of certificate authorities (CAs) or other institutes which manage identity data centrally.

Relationship between IKE and IPsec

Figure 4 Relationship between IKE and IPsec

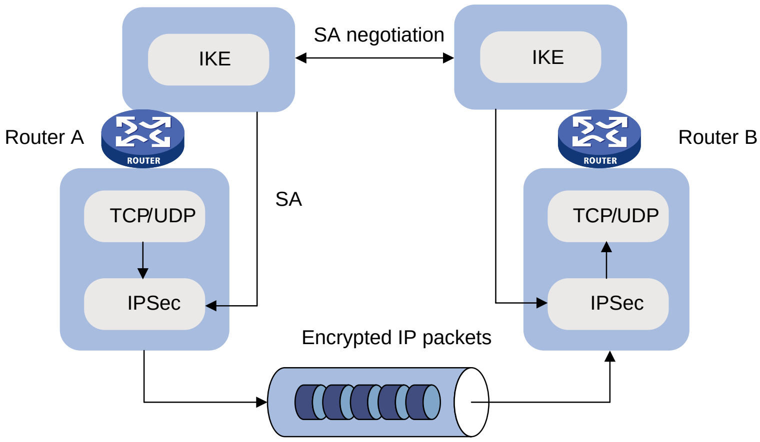


Figure 4 illustrates the relationship between IKE and IPsec:

- IKE is an application layer protocol using UDP and functions as the signaling protocol of IPsec.
- IKE negotiates SAs for IPsec and delivers negotiated parameters and generated keys to IPsec.
- IPsec uses the SAs set up through IKE negotiation for encryption and authentication of IP packets.

Protocols and standards

These protocols and standards are relevant to IKE:

- RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*
- RFC 2409, *The Internet Key Exchange (IKE)*
- RFC 2412, *The OAKLEY Key Determination Protocol*

IKE configuration task list

Prior to IKE configuration, you must determine the following parameters:

- The strength of the algorithms for IKE negotiation (the security protection level), including the identity authentication method, encryption algorithm, authentication algorithm, and DH group. Different algorithms provide different levels of protection. A stronger algorithm means more resistant to decryption of protected data but requires more resources. Generally, the longer the key, the stronger the algorithm.
- The pre-shared key or the PKI domain the certificate belongs to. For more information about PKI configuration, see the chapter "PKI configuration."

To configure IKE:

Task	Remarks
Configuring a name for the local security gateway	Optional.
Configuring an IKE proposal	Optional. Required if you want to specify an IKE proposal for an IKE peer to reference.
Configuring an IKE peer	Required.
Setting keepalive timers	Optional.
Setting the NAT keepalive timer	Optional.
Configuring a DPD detector	Optional.
Disabling next payload field checking	Optional.

Configuring a name for the local security gateway

If the IKE negotiation peer uses the security gateway name as its ID to initiate IKE negotiation (the **id-type name** or **id-type user-fqdn** command is configured on the initiator), configure the **ike local-name** command in system view or the **local-name** command in IKE peer view on the local device. If you configure both commands, the name configured in IKE peer view is used.

To configure a name for the local security gateway:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure a name for the local security gateway.	**ike local-name** *name*	Optional. By default, the device name is used as the name of the local security gateway.

Configuring an IKE proposal

An IKE proposal defines a set of attributes describing how IKE negotiation should take place. You may create multiple IKE proposals with different preferences. The preference of an IKE proposal is represented by its sequence number, and the lower the sequence number, the higher the preference.

Two peers must have at least one matching IKE proposal for successful IKE negotiation. During IKE negotiation, the initiator sends its IKE proposals to the peer, and the peer searches its own IKE proposals for a match. The search starts from the one with the lowest sequence number and proceeds in the ascending order of sequence number until a match is found or all the IKE proposals are found mismatching. The matching IKE proposals will be used to establish the secure tunnel.

Two matching IKE proposals have the same encryption algorithm, authentication method, authentication algorithm, and DH group. The SA lifetime will take the smaller one of the settings on the two sides.

By default, there is an IKE proposal, which has the lowest preference and uses the default encryption algorithm, authentication method, authentication algorithm, DH group, and ISAKMP SA lifetime.

To configure an IKE proposal:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Create an IKE proposal and enter its view.	**ike proposal** *proposal-number*	N/A
3.	Specify an encryption algorithm for the IKE proposal.	**encryption-algorithm aes-cbc** [*key-length*]	Optional. The default is AES-CBC-128.
4.	Specify an authentication method for the IKE proposal.	**authentication-method** { **pre-share** | **rsa-signature** }	Optional. Pre-shared key by default.
5.	Specify an authentication algorithm for the IKE proposal.	**authentication-algorithm sha**	Optional. SHA1 by default.
6.	Specify a DH group for key negotiation in phase 1.	**dh** { **group2** | **group5** | **group14** }	Optional. **group2** (the 1024-bit DH group) by default.
7.	Set the ISAKMP SA lifetime for the IKE proposal.	**sa duration** *seconds*	Optional. 86400 seconds by default.

NOTE:

Before an ISAKMP SA expires, IKE negotiates a new SA to replace it. DH calculation in IKE negotiation takes time, especially on low-end devices. To prevent SA updates from influencing normal communication, set the lifetime greater than 10 minutes.

Configuring an IKE peer

For an IPsec policy that uses IKE, you must configure an IKE peer by performing the following tasks:

- Specify the IKE negotiation mode (main mode) for the local end to use in IKE negotiation phase 1. When acting as the IKE negotiation responder, the local end uses the IKE negotiation mode of the remote end.
- Specify the IKE proposals for the local end to use when acting as the IKE negotiation initiator. When acting as the responder, the local end uses the IKE proposals configured in system view for negotiation.
- Configure a pre-shared key for pre-shared key authentication or a PKI domain for digital signature authentication.
- Specify the ID type for the local end to use in IKE negotiation phase 1. With pre-shared key authentication, the ID type must be IP address for main mode IKE negotiation.
- Specify the name or IP address of the local security gateway. You perform this task only when you want to specify a special address, for example, a loopback interface address, as the local security gateway address.
- Specify the name or IP address of the remote security gateway. For the local end to initiate IKE negotiation, you must specify the name or IP address of the remote security gateway on the local end so the local end can find the remote end.
- Enable NAT traversal. If there is NAT gateway on the path for tunneling, you must configure NAT traversal at the two ends of the IPsec tunnel, because one end may use a public address while the other end uses a private address.
- Specify the dead peer detection (DPD) detector for the IKE peer.

To configure an IKE peer:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create an IKE peer and enter IKE peer view.	**ike peer** *peer-name*	N/A
3. Specify the IKE negotiation mode for phase 1.	**exchange-mode main**	Optional. The default is **main**.
4. Specify the IKE proposals for the IKE peer to reference.	**proposal** *proposal-number*&<1-6>	Optional. By default, an IKE peer references no IKE proposals, and, when initiating IKE negotiation, it uses the IKE proposals configured in system view.
5. Configure the pre-shared key for pre-shared key authentication.	**pre-shared-key** [**cipher** | **simple**] *key*	Configure either command according to the authentication method for the IKE proposal.
6. Configure the PKI domain for digital signature authentication.	**certificate domain** *domain-name*	
7. Select the ID type for IKE negotiation phase 1.	**id-type** { **ip** | **name** | **user-fqdn** }	Optional. **ip** by default.
8. Configure the names of the two ends.	• Specify a name for the local security gateway: **local-name** *name* • Configure the name of the remote security gateway: **remote-name** *name*	Optional. By default, no name is configured for the local security gateway in IKE peer view, and the security gateway name configured by using the **ike local-name** command is used. The remote gateway name configured with **remote-name** command on the local gateway must be identical to the local name configured with the **local-name** command on the peer.
9. Configure the IP addresses of the two ends.	• Specify an IP address for the local gateway: **local-address** *ip-address* • Configure the IP addresses of the remote gateway: **remote-address** { *hostname* [**dynamic**] | *low-ip-address* [*high-ip-address*] }	Optional. By default, it is the primary IP address of the interface referencing the security policy. The remote IP address configured with the **remote-address** command on the local gateway must be identical to the local IP address configured with the **local-address** command on the peer.
10. Enable the NAT traversal function for IPsec/IKE.	**nat traversal**	Optional. Required when a NAT gateway is present in the VPN tunnel constructed by IPsec/IKE. Disabled by default.

Step	Command	Remarks
11. Apply a DPD detector to the IKE peer.	**dpd** *dpd-name*	Optional. No DPD detector is applied to an IKE peer by default. For more information about DPD configuration, see "Configuring a DPD detector."

NOTE:

After modifying the configuration of an IPsec IKE peer, execute the **reset ipsec sa** and **reset ike sa** commands to clear existing IPsec and IKE SAs. Otherwise, SA re-negotiation will fail.

Setting keepalive timers

IKE maintains the link status of an ISAKMP SA by keepalive packets. Generally, if the peer is configured with the keepalive timeout, you must configure the keepalive packet transmission interval on the local end. If the peer receives no keepalive packet during the timeout interval, the ISAKMP SA will be tagged with the TIMEOUT tag (if it does not have the tag), or be deleted along with the IPsec SAs it negotiated (when it has the tag already).

To set the keepalive timers:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the ISAKMP SA keepalive interval.	**ike sa keepalive-timer interval** *seconds*	No keepalive packet is sent by default.
3. Set the ISAKMP SA keepalive timeout.	**ike sa keepalive-timer timeout** *seconds*	No keepalive packet is sent by default.

NOTE:

The keepalive timeout configured at the local end must be longer than the keepalive interval configured at the remote end. Since it seldom occurs that more than three consecutive packets are lost on a network, the keepalive timeout can be configured to be three times of the keepalive interval.

Setting the NAT keepalive timer

If IPsec traffic needs to pass through NAT security gateways, you must configure the NAT traversal function. If no packet travels across an IPsec tunnel in a certain period of time, the NAT mapping may get aged and be deleted, disabling the tunnel beyond the NAT gateway from transmitting data to the intended end. To prevent NAT mappings from being aged, an ISAKMP SA behind the NAT security gateway sends NAT keepalive packets to its peer at a certain interval to keep the NAT session alive.

To set the NAT keepalive timer:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the NAT keepalive interval.	**ike sa nat-keepalive-timer interval** *seconds*	20 seconds by default.

Configuring a DPD detector

Dead peer detection (DPD) irregularly detects dead IKE peers. It works as follows:

1. When the local end sends an IPsec packet, it checks the time the last IPsec packet was received from the peer.
2. If the time interval exceeds the DPD interval, it sends a DPD hello to the peer.
3. If the local end receives no DPD acknowledgement within the DPD packet retransmission interval, it retransmits the DPD hello.
4. If the local end still receives no DPD acknowledgement after having made the maximum number of retransmission attempts (two by default), it considers the peer already dead, and clears the IKE SA and the IPsec SAs based on the IKE SA.

DPD enables an IKE entity to check the liveliness of its peer only when necessary. It generates less traffic than the keepalive mechanism, which exchanges messages periodically.

To configure a DPD detector:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a DPD detector and enter its view.	**ike dpd** *dpd-name*	N/A
3. Set the DPD interval.	**interval-time** *interval-time*	Optional. 10 seconds by default.
4. Set the DPD packet retransmission interval.	**time-out** *time-out*	Optional. 5 seconds by default.

Disabling next payload field checking

The Next payload field is in the generic payload header of the last payload of the IKE negotiation message (the message comprises multiple payloads). According to the protocol, this field must be 0 if the payload is the last payload of the packet. However, it may be set to other values on some brands of devices. For interoperability, disable the checking of this field.

To disable Next payload field checking:

Step	Command	Remark
1. Enter system view.	**system-view**	N/A
2. Disable Next payload field checking.	**ike next-payload check disabled**	Enabled by default.

Displaying and maintaining IKE

Task	Command	Remarks
Display IKE DPD information	**display ike dpd** [*dpd-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display IKE peer information	**display ike peer** [*peer-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.

Task	Command	Remarks
Display IKE SA information	**display ike sa** [**verbose** [**connection-id** *connection-id* | **remote-address** *remote-address*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display IKE proposal information	**display ike proposal** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Clear SAs established by IKE	**reset ike sa** [*connection-id*]	Available in user view.

IKE configuration example

Network requirements

As shown in Figure 5, configure an IPsec tunnel that uses IKE negotiation between gateways Switch A and Switch B to secure the communication between the two switches.

For Switch A, configure an IKE proposal that uses the sequence number 10 and the authentication algorithm SHA1. Configure Switch B to use the default IKE proposal.

Configure the two routers to use the pre-shared key authentication method.

Figure 5 Network diagram

Configuration procedure

1. Make sure Switch A and Switch B can reach each other.
2. Configure Switch A:

Assign an IP address to VLAN-interface 1.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-vlan-interface1] ip address 1.1.1.1 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

Configure ACL 3101 to identify traffic from Switch A to Switch B..

```
[SwitchA] acl number 3101
[SwitchA-acl-adv-3101] rule 0 permit ip source 1.1.1.1 0 destination 2.2.2.2 0
[SwitchA-acl-adv-3101] rule 1 permit ip source 2.2.2.2 0 destination 1.1.1.1 0
[SwitchA-acl-adv-3101] quit
```

Create IPsec proposal **tran1**.

```
[SwitchA] ipsec proposal tran1
```

Set the packet encapsulation mode to tunnel.

```
[SwitchA-ipsec-proposal-tran1] encapsulation-mode tunnel
```

Use security protocol ESP.

```
[Switch-ipsec-proposal-tran1] transform esp
```

Specify encryption and authentication algorithms.

```
[SwitchA-ipsec-proposal-tran1] esp encryption-algorithm aes 128
[SwitchA-ipsec-proposal-tran1] esp authentication-algorithm sha1
```

```
[SwitchA-ipsec-proposal-tran1] quit
```

Create an IKE proposal numbered 10.

```
[SwitchA] ike proposal 10
```

Set the authentication algorithm to **SHA1**.

```
[SwitchA-ike-proposal-10] authentication-algorithm sha
```

Configure the authentication method as pre-shared key.

```
[SwitchA-ike-proposal-10] authentication-method pre-share
```

Set the ISAKMP SA lifetime to 5000 seconds.

```
[SwitchA-ike-proposal-10] sa duration 5000
[SwitchA-ike-proposal-10] quit
```

Create IKE peer **peer**.

```
[SwitchA] ike peer peer
```

Configure the IKE peer to reference IKE proposal 10.

```
[SwitchA-ike-peer-peer]proposal 10
```

Set the pre-shared key.

```
[SwitchA-ike-peer-peer] pre-shared-key Ab12<><>
```

Specify the IP address of the peer security gateway.

```
[SwitchA-ike-peer-peer] remote-address 2.2.2.2
[SwitchA-ike-peer-peer] quit
```

Create an IPsec policy that uses IKE negotiation.

```
[SwitchA] ipsec policy map1 10 isakmp
```

Reference IPsec proposal **tran1**.

```
[SwitchA-ipsec-policy-isakmp-map1-10] proposal tran1
```

Reference ACL 3101 to identify the protected traffic.

```
[SwitchA-ipsec-policy-isakmp-map1-10] security acl 3101
```

Reference IKE peer **peer**.

```
[SwitchA-ipsec-policy-isakmp-map1-10] ike-peer peer
[SwitchA-ipsec-policy-isakmp-map1-10] quit
```

Apply the IPsec policy to VLAN-interface 1.

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ipsec policy map1
```

3. Configure Switch B:

Assign an IP address to VLAN-interface 1.

```
<SwitchB> system-view
[SwitchB] interface Vlan-interface1
[SwitchB-Vlan-interface1] ip address 2.2.2.2 255.255.255.0
[SwitchB-Vlan-interface1] quit
```

Configure ACL 3101 to identify traffic from Switch B to Switch A.

```
[SwitchB] acl number 3101
[SwitchB-acl-adv-3101] rule 0 permit ip source 2.2.2.2 0 destination 1.1.1.0 0
[SwitchB-acl-adv-3101] rule 1 permit ip source 1.1.1.1 0 destination 2.2.2.2 0
[SwitchB-acl-adv-3101] quit
```

Create IPsec proposal **tran1**.

```
[SwitchB] ipsec proposal tran1
```

Set the packet encapsulation mode to tunnel.

```
[SwitchB-ipsec-proposal-tran1] encapsulation-mode tunnel
```

Use security protocol ESP.

```
[SwitchB-ipsec-proposal-tran1] transform esp
```

Specify encryption and authentication algorithms.

```
[SwitchB-ipsec-proposal-tran1] esp encryption-algorithm aes 128
[SwitchB-ipsec-proposal-tran1] esp authentication-algorithm sha1
[SwitchB-ipsec-proposal-tran1] quit
```

Create an IKE proposal numbered 10.

```
[SwitchB] ike proposal 10
```

Set the authentication algorithm to **SHA1**.

```
[SwitchB-ike-proposal-10] authentication-algorithm sha
```

Configure the authentication method as pre-shared key.

```
[SwitchB-ike-proposal-10] authentication-method pre-share
```

Set the ISAKMP SA lifetime to 5000 seconds.

```
[SwitchB-ike-proposal-10] sa duration 5000
[SwitchB-ike-proposal-10] quit
```

Create IKE peer **peer**.

```
[SwitchB] ike peer peer
```

Configure the IKE peer to reference IKE proposal 10.

```
[SwitchB-ike-peer-peer]proposal 10
```

Set the pre-shared key.

```
[SwitchB-ike-peer-peer] pre-shared-key Ab12<><>
```

Specify the IP address of the peer security gateway.

```
[SwitchB-ike-peer-peer] remote-address 1.1.1.1
[SwitchB-ike-peer-peer] quit
```

Create an IPsec policy that uses IKE negotiation.

```
[SwitchB] ipsec policy use1 10 isakmp
```

Reference IPsec proposal **tran1**.

```
[SwitchB-ipsec-policy-isakmp-use1-10] proposal tran1
```

Reference ACL 3101 to identify the protected traffic.

```
[SwitchB-ipsec-policy-isakmp-use1-10] security acl 3101
```

Reference IKE peer **peer**.

```
[SwitchB-ipsec-policy-isakmp-use1-10] ike-peer peer
[SwitchB-ipsec-policy-isakmp-use1-10] quit
```

Apply the IPsec policy to VLAN-interface 1.

```
[SwitchB-Vlan-interface1] ipsec policy use1
```

Verifying the configuration

After the above configuration, send traffic from Switch B to Switch A. Switch A starts IKE negotiation with Switch B when receiving the first packet. IKE proposal matching starts with the one having the highest priority. During the matching process, lifetime is not involved but it is determined by the IKE negotiation parties.

Troubleshooting IKE

When you configure parameters to establish an IPsec tunnel, enable IKE error debugging to locate configuration problems:

```
<Switch> debugging ike error
```

Invalid user ID

Symptom

Invalid user ID.

Analysis

In IPsec, user IDs are used to identify data flows and to set up different IPsec tunnels for different data flows. Now, the IP address and username are used as the user ID.

The following is the debugging information:

```
got NOTIFY of type INVALID_ID_INFORMATION
```

Or

```
drop message from A.B.C.D due to notification type INVALID_ID_INFORMATION
```

Solution

Check that the ACLs in the IPsec policies configured on the interfaces at both ends are compatible. Configure the ACLs to mirror each other. For more information about ACL mirroring, see the chapter "IPsec configuration."

Proposal mismatch

Symptom

The proposals mismatch.

Analysis

The following is the debugging information:

```
got NOTIFY of type NO_PROPOSAL_CHOSEN
```

Or

```
drop message from A.B.C.D due to notification type NO_PROPOSAL_CHOSEN
```

The two parties in the negotiation have no matched proposals.

Solution

For the negotiation in phase 1, look up the IKE proposals for a match. For the negotiation in phase 2, check whether the parameters of the IPsec policies applied on the interfaces are matched, and whether the referred IPsec proposals have a match in protocol, encryption and authentication algorithms.

Failing to establish an IPsec tunnel

Symptom

The expected IPsec tunnel cannot be established.

Analysis

Sometimes this may happen that an IPsec tunnel cannot be established or there is no way to communicate in the presence of an IPsec tunnel in an unstable network. According to examination results, however, ACLs of both parties are configured correctly, and proposals are also matched.

In this case, the problem is usually caused by the reboot of one router after the IPsec tunnel is established.

Solution

- Use the **display ike sa** command to check whether both parties have established an SA in phase 1.
- Use the **display ipsec sa policy** command to check whether the IPsec policy on the interface has established IPsec SA.
- If the two commands show that one party has an SA but the other does not, use the **reset ipsec sa** command to clear the IPsec SA that has no corresponding SA, use the **reset ike sa** command to clear the IKE SA that has no corresponding IKE SA, and trigger SA re-negotiation.

ACL configuration error

Symptom

ACL configuration error results in data flow blockage.

Analysis

When multiple devices create different IPsec tunnels early or late, a device may have multiple peers. If the device is not configured with ACL rule, the peers send packets to it to set up different IPsec tunnels in different protection granularity respectively. As the priorities of IPsec tunnels are determined by the order they are established, a device cannot interoperate with other peers in fine granularity when its outbound packets are first matched with an IPsec tunnel in coarse granularity.

Solution

When a device has multiple peers, configure ACLs on the device to distinguish different data flows and try to avoid configuring overlapping ACL rules for different peers. If it is unavoidable, the subrules in fine granularity should be configured with higher preferences.

Command reference

authentication-algorithm

Use **authentication-algorithm** to specify an authentication algorithm for an IKE proposal.

Use **undo authentication-algorithm** to restore the default.

Syntax

authentication-algorithm sha

undo authentication-algorithm

Default

An IKE proposal uses the SHA1 authentication algorithm.

Views

IKE proposal view

Default command level

2: System level

Parameters

sha: Uses HMAC-SHA1.

Examples

Set SHA1 as the authentication algorithm for IKE proposal 10.

```
<Sysname> system-view
[Sysname] ike proposal 10
[Sysname-ike-proposal-10] authentication-algorithm sha
```

Related commands

- **display ike proposal**
- **ike proposal**

authentication-method

Use **authentication-method** to specify an authentication method for an IKE proposal.

Use **undo authentication-method** to restore the default.

Syntax

authentication-method { **pre-share** | **rsa-signature** }

undo authentication-method

Default

An IKE proposal uses the pre-shared key authentication method.

Views

IKE proposal view

Default command level

2: System level

Parameters

pre-share: Uses the pre-shared key method.

rsa-signature: Uses the RSA digital signature method.

Examples

Specify that IKE proposal 10 uses the pre-shared key authentication method.

```
<Sysname> system-view
[Sysname] ike proposal 10
[Sysname-ike-proposal-10] authentication-method pre-share
```

Related commands

- **display ike proposal**
- **ike proposal**

certificate domain

Use **certificate domain** to configure the PKI domain of the certificate when IKE uses digital signature as the authentication mode.

Use **undo certificate domain** to remove the configuration.

Syntax

certificate domain *domain-name*

undo certificate domain

Views

IKE peer view

Default command level

2: System level

Parameters

domain-name: Name of the PKI domain, a string of 1 to 15 characters.

Examples

Configure the PKI domain as **abcde** for IKE negotiation.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] certificate domain abcde
```

Related commands

- **authentication-method**
- **pki domain**

dh

Use **dh** to specify the DH group to be used in key negotiation phase 1 for an IKE proposal.

Use **undo dh** to restore the default.

Syntax

dh { **group2** | **group5** | **group14** }

undo dh

Default

Group2, the 1024-bit Diffie-Hellman group, is used.

Views

IKE proposal view

Default command level

2: System level

Parameters

group2: Uses the 1024-bit Diffie-Hellman group for key negotiation in phase 1.

group5: Uses the 1536-bit Diffie-Hellman group for key negotiation in phase 1.

group14: Uses the 2048-bit Diffie-Hellman group for key negotiation in phase 1.

Examples

Specify 1536-bit Diffie-Hellman for IKE proposal 10.

```
<Sysname> system-view
[Sysname] ike proposal 10
[Sysname-ike-proposal-10] dh group5
```

Related commands

- **display ike proposal**
- **ike proposal**

display ike dpd

Use **display ike dpd** to display information about Dead Peer Detection (DPD) detectors.

Syntax

display ike dpd [*dpd-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

dpd-name: DPD name, a string of 1 to 32 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Usage guidelines

If you do not specify any parameters, the command displays information about all DPD detectors.

Examples

Display information about all DPD detectors.

```
<Sysname> display ike dpd

---------------------------
 IKE dpd: dpd1
   references: 1
   interval-time: 10
   time_out: 5
---------------------------
```

Table 2 Command output

Field	Description
references	Number of IKE peers that use the DPD detector.
Interval-time	DPD query trigging interval in seconds.
time_out	DPD packet retransmission interval in seconds.

Related commands

ike dpd

display ike peer

Use **display ike peer** to display information about IKE peers.

Syntax

display ike peer [*peer-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

peer-name: Name of the IKE peer, a string of 1 to 32 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Usage guidelines

If you do not specify any parameters, the command displays information about all IKE peers.

Examples

Display information about all IKE peers.

```
<Sysname> display ike peer

---------------------------
 IKE Peer: aaa
   exchange mode: main on phase 1
   peer id type: ip
   peer ip address: 0.0.0.0 ~ 255.255.255.255
   local ip address:
   peer name:
   nat traversal: disable
   dpd:
---------------------------
```

Table 3 Command output

Field	Description
exchange mode	IKE negotiation mode in phase 1.
pre-shared-key	Pre-shared key used in phase 1.
peer id type	ID type used in phase 1.
peer ip address	IP address of the remote security gateway.
local ip address	IP address of the local security gateway.
peer name	Name of the remote security gateway.

Field	Description
nat traversal	Whether NAT traversal is enabled.
dpd	Name of the peer DPD detector.

Related commands

ike peer

display ike proposal

Use **display ike proposal** to view the settings of all IKE proposals.

Syntax

display ike proposal [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Usage guidelines

This command displays the configuration information of all IKE proposals in the descending order of proposal priorities.

Examples

Display the settings of all IKE proposals.

```
<Sysname> display ike proposal
priority authentication authentication encryption Diffie-Hellman duration
              method       algorithm    algorithm     group       (seconds)
---------------------------------------------------------------------------
  11       PRE_SHARED     SHA         AES_CBC_128     MODP_1024      86400
  default  PRE_SHARED     SHA         AES_CBC_128     MODP_1024      86400
```

Table 4 Command output

Field	Description
priority	Priority of the IKE proposal.
authentication method	Authentication method used by the IKE proposal.
authentication algorithm	Authentication algorithm used by the IKE proposal.
encryption algorithm	Encryption algorithm used by the IKE proposal.
Diffie-Hellman group	DH group used in IKE negotiation phase 1.

Field	Description
duration (seconds)	ISAKMP SA lifetime of the IKE proposal in seconds.

Related commands

- **authentication-algorithm**
- **authentication-method**
- **dh**
- **encryption-algorithm**
- **ike proposal**
- **sa duration**

display ike sa

Use **display ike sa** to display information about the current IKE SAs.

Syntax

display ike sa [**verbose** [**connection-id** *connection-id* | **remote-address** *remote-address*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

verbose: Displays detailed information.

connection-id *connection-id*: Displays detailed information about IKE SAs by connection ID, in the range 1 to 2000000000.

remote: Displays detailed information about IKE SAs with a specified remote address.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Usage guidelines

If you do not specify any parameters or keywords, the command displays brief information about the current IKE SAs.

Examples

Display brief information about the current IKE SAs.

```
<Sysname> display ike sa
    total phase-1 SAs:  1
    connection-id  peer            flag        phase   doi
  ----------------------------------------------------------
      1            202.38.0.2      RD|ST        1      IPSEC
      2            202.38.0.2      RD|ST        2      IPSEC
```

```
flag meaning
RD--READY ST--STAYALIVE RL--REPLACED FD—FADING TO—TIMEOUT
```

Table 5 Command output

Field	Description
total phase-1 SAs	Total number of SAs for phase 1.
connection-id	Identifier of the ISAKMP SA.
peer	Remote IP address of the SA.
flag	Status of the SA: • **RD (READY)**—The SA has been established. • **ST (STAYALIVE)**—This end is the initiator of the tunnel negotiation. • **RL (REPLACED)**—The tunnel has been replaced by a new one and will be deleted later. • **FD (FADING)**—The soft lifetime is over but the tunnel is still in use. The tunnel will be deleted when the hard lifetime is over. • **TO (TIMEOUT)**—The SA has received no keepalive packets after the last keepalive timeout. If no keepalive packets are received before the next keepalive timeout, the SA will be deleted.
phase	The phase the SA belongs to: • **Phase 1**—The phase for establishing the ISAKMP SA. • **Phase 2**—The phase for negotiating the security service. IPsec SAs are established in this phase.
doi	Interpretation domain the SA belongs to.

Display detailed information about the current IKE SAs.

```
<Sysname> display ike sa verbose
    ---------------------------------------------
    connection id: 2
    vpn-instance: 1
transmitting entity: initiator
    ---------------------------------------------
    local ip: 4.4.4.4
    local id type: IPV4_ADDR
    local id: 4.4.4.4

    remote ip: 4.4.4.5
    remote id type: IPV4_ADDR
    remote id: 4.4.4.5

    authentication-method: PRE-SHARED-KEY
    authentication-algorithm: HASH-SHA1
    encryption-algorithm: AES-CBC

    life duration(sec): 86400
    remaining key duration(sec): 86379
    exchange-mode: MAIN
    diffie-hellman group: GROUP1
    nat traversal: NO
```

Display detailed information about the IKE SA with the connection ID of 2.

```
<Sysname> display ike sa verbose connection-id 2
    -----------------------------------------------
    connection id: 2
    vpn-instance: vpn1
transmitting entity: initiator
    -----------------------------------------------
    local ip: 4.4.4.4
    local id type: IPV4_ADDR
    local id: 4.4.4.4

    remote ip: 4.4.4.5
    remote id type: IPV4_ADDR
    remote id: 4.4.4.5

    authentication-method: PRE-SHARED-KEY
    authentication-algorithm: HASH-SHA1
    encryption-algorithm: AES-CBC

    life duration(sec): 86400
    remaining key duration(sec): 82480
    exchange-mode: MAIN
    diffie-hellman group: GROUP14
    nat traversal: NO
```

Display detailed information about the IKE SA with the remote address of 4.4.4.5.

```
<Sysname> display ike sa verbose remote-address 4.4.4.5
    -----------------------------------------------
    connection id: 2
    vpn-instance: vpn1
    transmitting entity: initiator
    -----------------------------------------------
    local ip: 4.4.4.4
    local id type: IPV4_ADDR
    local id: 4.4.4.4

    remote ip: 4.4.4.5
    remote id type: IPV4_ADDR
    remote id: 4.4.4.5

    authentication-method: PRE-SHARED-KEY
    authentication-algorithm: HASH-SHA1
    encryption-algorithm: DES-CBC

    life duration(sec): 86400
    remaining key duration(sec): 82236
    exchange-mode: MAIN
    diffie-hellman group: GROUP1
    nat traversal: NO
```

Table 6 Command output

Field	Description
connection id	Identifier of the ISAKMP SA.
vpn-instance	MPLS L3VPN that the protected data belongs to.
transmitting entity	Entity in the IKE negotiation.
local ip	IP address of the local gateway.
local id type	Identifier type of the local gateway.
local id	Identifier of the local gateway.
remote ip	IP address of the remote gateway.
remote id type	Identifier type of the remote gateway.
remote id	Identifier of the remote security gateway.
authentication-method	Authentication method used by the IKE proposal.
authentication-algorithm	Authentication algorithm used by the IKE proposal.
encryption-algorithm	Encryption algorithm used by the IKE proposal.
life duration(sec)	Lifetime of the ISAKMP SA in seconds.
remaining key duration(sec)	Remaining lifetime of the ISAKMP SA in seconds.
exchange-mode	IKE negotiation mode in phase 1.
diffie-hellman group	DH group used for key negotiation in IKE phase 1.
nat traversal	Whether NAT traversal is enabled.

Related commands

- **ike peer**
- **ike proposal**

dpd

Use **dpd** to apply a DPD detector to an IKE peer.

Use **undo dpd** to remove the application.

Syntax

dpd *dpd-name*

undo dpd

Default

No DPD detector is applied to an IKE peer.

Views

IKE peer view

Default command level

2: System level

Parameters

dpd-name: DPD detector name, a string of 1 to 32 characters.

Examples

Apply **dpd1** to IKE peer peer1.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] dpd dpd1
```

encryption-algorithm

Use **encryption-algorithm** to specify an encryption algorithm for an IKE proposal.

Use **undo encryption-algorithm** to restore the default.

Syntax

encryption-algorithm aes-cbc [*key-length*]

undo encryption-algorithm

Default

The encryption algorithm for an IKE proposal is AES-128.

Views

IKE proposal view

Default command level

2: System level

Parameters

aes-cbc: Uses the AES algorithm in CBC mode as the encryption algorithm. The AES algorithm uses 128-bit, 192-bit, or 256-bit keys for encryption.

key-length: Key length for the AES algorithm, which can be 128, 192 or 256 bits and is defaulted to 128 bits.

Examples

Use 128-bit AES in CBC mode as the encryption algorithm for IKE proposal 10.

```
<Sysname> system-view
[Sysname] ike proposal 10
[Sysname-ike-proposal-10] encryption-algorithm aes 128
```

Related commands

- **display ike proposal**
- **ike proposal**

exchange-mode

Use **exchange-mode** to select an IKE negotiation mode.

Use **undo exchange-mode** to restore the default.

Syntax

exchange-mode main

undo exchange-mode

Default

Main mode is used.

Views

IKE peer view

Default command level

2: System level

Parameters

main: Main mode.

Examples

Specify that IKE negotiation works in main mode.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] exchange-mode main
```

Related commands

id-type

id-type

Use **id-type** to select the type of the ID for IKE negotiation.

Use **undo id-type** to restore the default.

Syntax

id-type { **ip** | **name** | **user-fqdn** }

undo id-type

Default

The ID type is IP address.

Views

IKE peer view

Default command level

2: System level

Parameters

ip: Uses an IP address as the ID during IKE negotiation.

name: Uses a FQDN name as the ID during IKE negotiation.

user-fqdn: Uses a user FQDN name as the ID during IKE negotiation.

Usage guidelines

In main mode, only the ID type of IP address can be used in IKE negotiation and SA creation.

Examples

Use the ID type of name during IKE negotiation.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] id-type name
```

Related commands

- **exchange-mode**
- **ike local-name**
- **local-address**
- **local-name**
- **remote-address**
- **remote-name**

ike dpd

Use **ike dpd** to create a DPD detector and enter IKE DPD view.

Use **undo ike dpd** to remove a DPD detector.

Syntax

ike dpd *dpd-name*

undo ike dpd *dpd-name*

Views

System view

Default command level

2: System level

Parameters

dpd-name: Name for the dead peer detection (DPD) detector, a string of 1 to 32 characters.

Usage guidelines

Dead peer detection (DPD) irregularly detects dead IKE peers. It works as follows:

1. When the local end sends an IPsec packet, it checks the time the last IPsec packet was received from the peer.
2. If the time interval exceeds the DPD interval, it sends a DPD hello to the peer.
3. If the local end receives no DPD acknowledgement within the DPD packet retransmission interval, it retransmits the DPD hello.
4. If the local end still receives no DPD acknowledgement after having made the maximum number of retransmission attempts (two by default), it considers the peer already dead, and clears the IKE SA and the IPsec SAs based on the IKE SA.

DPD enables an IKE entity to check the liveliness of its peer only when necessary. It generates less traffic than the keepalive mechanism, which exchanges messages periodically.

Examples

Create a DPD detector named **dpd2**.

```
<Sysname> system-view
[Sysname] ike dpd dpd2
```

Related commands

- **display ike dpd**
- **interval-time**
- **time-out**

ike local-name

Use **ike local-name** to configure a name for the local security gateway.

Use **undo ike local-name** to restore the default.

Syntax

ike local-name *name*

undo ike local-name

Default

The device name is used as the name of the local security gateway.

Views

System view

Default command level

2: System level

Parameters

name: Name of the local security gateway for IKE negotiation, a case-sensitive string of 1 to 32 characters.

Usage guidelines

If you configure the **id-type name** or **id-type user-fqdn** command on the initiator, the IKE negotiation peer uses the security gateway name as its ID to initiate IKE negotiation, and you must configure the **ike local-name** command in system view or the **local-name** command in IKE peer view on the local device. If you configure both the **ike local-name** command and the **local-name** command, the name configured by the **local-name** command is used.

The IKE negotiation initiator sends its security gateway name as its ID to the peer, and the peer uses the security gateway name configured with the **remote-name** command to authenticate the initiator. Make sure the local gateway name matches the remote gateway name configured on the peer.

Examples

Configure the local security gateway name as **app**.

```
<Sysname> system-view
[Sysname] ike local-name app
```

Related commands

id-type

remote-name

ike next-payload check disabled

Use **ike next-payload check disabled** to disable the checking of the Next payload field in the last payload of an IKE message during IKE negotiation, gaining interoperation with products assigning the field a value other than zero.

Use **undo ike next-payload check disabled** to restore the default.

Syntax

ike next-payload check disabled

undo ike next-payload check disabled

Default

The Next payload field is checked.

Views

System view

Default command level

2: System level

Examples

Disable Next payload field checking for the last payload of an IKE message.

```
<Sysname> system-view
[Sysname] ike next-payload check disabled
```

ike peer (system view)

Use **ike peer** to create an IKE peer and enter IKE peer view.

Use **undo ike peer** to delete an IKE peer.

Syntax

ike peer *peer-name*

undo ike peer *peer-name*

Views

System view

Default command level

2: System level

Parameters

peer-name: IKE peer name, a string of 1 to 32 characters.

Examples

Create an IKE peer named peer1 and enter IKE peer view.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1]
```

ike proposal

Use **ike proposal** to create an IKE proposal and enter IKE proposal view.

Use **undo ike proposal** to delete an IKE proposal.

Syntax

ike proposal proposal-number

undo ike proposal *proposal-number*

Views

System view

Default command level

2: System level

Parameters

proposal-number: IKE proposal number, in the range 1 to 65535. The lower the number, the higher the priority of the IKE proposal. During IKE negotiation, a high priority IKE proposal is matched before a low priority IKE proposal.

Usage guidelines

The system provides a default IKE proposal, which has the lowest priority and uses these settings:

- Encryption algorithm AES-128.
- Authentication algorithm HMAC-SHA1.
- Authentication method Pre-shared key.
- DH group MODP_1024.
- SA lifetime 86400 seconds.

Examples

Create IKE proposal 10 and enter IKE proposal view.

```
<Sysname> system-view
[Sysname] ike proposal 10
[Sysname-ike-proposal-10]
```

Related commands

display ike proposal

ike sa keepalive-timer interval

Use **ike sa keepalive-timer interval** to set the ISAKMP SA keepalive interval.

Use **undo ike sa keepalive-timer interval** to disable the ISAKMP SA keepalive transmission function.

Syntax

ike sa keepalive-timer interval *seconds*

undo ike sa keepalive-timer interval

Default

No keepalive packet is sent.

Views

System view

Default command level

2: System level

Parameters

seconds: Transmission interval of ISAKMP SA keepalives in seconds, in the range 20 to 28,800.

Usage guidelines

The keepalive interval configured at the local end must be shorter than the keepalive timeout configured at the remote end.

Examples

Set the keepalive interval to 200 seconds.

```
<Sysname> system-view
[Sysname] ike sa keepalive-timer interval 200
```

Related commands

ike sa keepalive-timer timeout

ike sa keepalive-timer timeout

Use **ike sa keepalive-timer timeout** to set the ISAKMP SA keepalive timeout.

Use **undo ike sa keepalive-timer timeout** to disable the function.

Syntax

ike sa keepalive-timer timeout *seconds*

undo ike sa keepalive-timer timeout

Default

No keepalive packet is sent.

Views

System view

Default command level

2: System level

Parameters

seconds: ISAKMP SA keepalive timeout in seconds, in the range 20 to 28800.

Usage guidelines

The keepalive timeout configured at the local end must be longer than the keepalive interval configured at the remote end. Since it seldom occurs that more than three consecutive packets are lost on a network, the keepalive timeout can be configured to be three times of the keepalive interval.

Examples

Set the keepalive timeout to 20 seconds.

```
<Sysname> system-view
[Sysname] ike sa keepalive-timer timeout 20
```

Related commands

ike sa keepalive-timer interval

ike sa nat-keepalive-timer interval

Use **ike sa nat-keepalive-timer interval** to set the NAT keepalive interval.

Use **undo ike sa nat-keepalive-timer interval** to disable the function.

Syntax

ike sa nat-keepalive-timer interval *seconds*

undo ike sa nat-keepalive-timer interval

Default

The NAT keepalive interval is 20 seconds.

Views

System view

Default command level

2: System level

Parameters

seconds: NAT keepalive interval in seconds, in the range 5 to 300.

Examples

Set the NAT keepalive interval to 5 seconds.

```
<Sysname> system-view
[Sysname] ike sa nat-keepalive-timer interval 5
```

interval-time

Use **interval-time** to set the DPD query triggering interval for a DPD detector.

Use **undo interval-time** to restore the default.

Syntax

interval-time *interval-time*

undo interval-time

Default

The DPD interval is 10 seconds.

Views

IKE DPD view

Default command level

2: System level

Parameters

interval-time: Sets DPD interval in seconds, in the range of 1 to 300 seconds. When the local end sends an IPsec packet, it checks the time the last IPsec packet was received from the peer. If the time interval exceeds the DPD interval, it sends a DPD hello to the peer.

Examples

Set the DPD interval to 1 second for dpd2.

```
<Sysname> system-view
[Sysname] ike dpd dpd2
[Sysname-ike-dpd-dpd2] interval-time 1
```

local-address

Use **local-address** to configure the IP address of the local security gateway in IKE negotiation.

Use **undo local-address** to remove the configuration.

Syntax

local-address *ip-address*

undo local-address

Default

The primary address of the interface referencing the IPsec policy is used as the local security gateway IP address for IKE negotiation.

Views

IKE peer view

Default command level

2: System level

Parameters

ip-address: IP address of the local security gateway to be used in IKE negotiation.

Usage guidelines

Use this command if you want to specify a different address for the local security gateway.

Examples

Set the IP address of the local security gateway to 1.1.1.1.

```
<Sysname> system-view
[Sysname] ike peer xhy
[Sysname-ike-peer-xhy] local-address 1.1.1.1
```

local-name

Use **local-name** to configure a name for the local security gateway to be used in IKE negation.

Use **undo local-name** to restore the default.

Syntax

local-name *name*

undo local-name

Default

The device name is used as the name of the local security gateway view.

Views

IKE peer view

Default command level

2: System level

Parameters

name: Name for the local security gateway to be used in IKE negotiation, a case-sensitive string of 1 to 32 characters.

Usage guidelines

If you configure the **id-type name** or **id-type user-fqdn** command on the initiator, the IKE negotiation peer uses the security gateway name as its ID to initiate IKE negotiation, and you must configure the **ike local-name** command in system view or the **local-name** command in IKE peer view on the local device. If you configure both the **ike local-name** command and the **local-name** command, the name configured by the **local-name** command is used.

The IKE negotiation initiator sends its security gateway name as its ID to the peer, and the peer uses the security gateway name configured with the **remote-name** command to authenticate the initiator. Make sure the local gateway name matches the remote gateway name configured on the peer.

Examples

Set the name of the local security gateway to **localgw** in IKE peer view of peer1.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] local-name localgw
```

Relate commands

- **id-type**
- **remote-name**

nat traversal

Use **nat traversal** to enable the NAT traversal function of IKE/IPsec.

Use **undo nat traversal** to disable the NAT traversal function of IKE/IPsec.

Syntax

nat traversal

undo nat traversal

Default

The NAT traversal function is disabled.

Views

IKE peer view

Default command level

2: System level

Examples

Enable the NAT traversal function for IKE peer peer1.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] nat traversal
```

peer

Use **peer** to set the subnet type of the peer security gateway for IKE negotiation.

Use **undo peer** to restore the default.

Syntax

peer { **multi-subnet** | **single-subnet** }

undo peer

Default

The subnet is a single one.

Views

IKE peer view

Default command level

2: System level

Parameters

multi-subnet: Sets the subnet type to multiple.

single-subnet: Sets the subnet type to single.

Usage guidelines

Use this command to enable interoperability with a NetScreen device.

Examples

Set the subnet type of the peer security gateway to **multiple**.

```
<Sysname> system-view
[Sysname] ike peer xhy
[Sysname-ike-peer-xhy] peer multi-subnet
```

pre-shared-key

Use **pre-shared-key** to configure the pre-shared key to be used in IKE negotiation.

Use **undo pre-shared-key** to remove the configuration.

Syntax

pre-shared-key [**cipher** | **simple**] *key*

undo pre-shared-key

Views

IKE peer view

Default command level

2: System level

Parameters

key: Plaintext pre-shared key to be displayed in cipher text, a case-sensitive string of 8 to 128 characters.

cipher *key*: Specifies the ciphertext pre-shared key to be displayed in cipher text, a case-sensitive string of 8 to 201 characters.

simple *key*: Specifies the plaintext pre-shared key to be displayed in plain text, a case-sensitive string of 8 to 128 characters.

Examples

Set the pre-shared key used in IKE negotiation to AAbbcc1234%.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] pre-shared-key AAbbcc1234%
```

Related commands

authentication-method

proposal (IKE peer view)

Use **proposal** to specify the IKE proposals for the IKE peer to reference.

Use **undo proposal** to remove one or all IKE proposals referenced by the IKE peer.

Syntax

proposal *proposal-number*&<1-6>

undo proposal [*proposal-number*]

Default

An IKE peer references no IKE proposals and, when initiating IKE negotiation, it uses the IKE proposals configured in system view.

Views

IKE peer view

Default command level

2: System level

Parameters

proposal-number&<1-6>: Sequence number of the IKE proposal for the IKE peer to reference, in the range 1 to 65535. &<1-6> means that you can specify the *proposal-number* argument for up to six times. An IKE proposal with a smaller sequence number has a higher priority.

Usage guidelines

In the IKE negotiation phase 1, the local peer uses the IKE proposals specified for it, if any.

An IKE peer can reference up to six IKE proposals.

The responder uses the IKE proposals configured in system view for negotiation.

Examples

Configure IKE peer **peer1** to reference IKE proposal **10**.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] proposal 10
```

Related commands

- **ike proposal**
- **ike peer** (system view)

remote-address

Use **remote-address** to configure the IP address of the IPsec remote security gateway.

Use **undo remote-address** to remove the configuration.

Syntax

remote-address { *hostname* [**dynamic**] **|** *low-ip-address* [*high-ip-address*] }

undo remote-address

Views

IKE peer view

Default command level

2: System level

Parameters

hostname: Host name of the IPsec remote security gateway, a case-insensitive string of 1 to 255 characters. The host name uniquely identifies the remote IPsec peer and can be resolved to an IP address by the DNS server.

dynamic: Specifies to use dynamic address resolution for the IPsec remote peer name. If you do not provide this keyword, the local peer has the remote host name resolved only once after you configure the remote host name.

low-ip-address: IP address of the IPsec remote security gateway. It is the lowest address in the address range if you want to specify a range of addresses.

high-ip-address: Highest address in the address range if you want to specify a range of addresses.

Usage guidelines

The IP address configured with the **remote-address** command must match the local security gateway IP address that the remote security gateway uses for IKE negotiation, which is the IP address configured with the **local-address** command or, if the **local-address** command is not configured, the primary IP address of the interface to which the policy is applied.

The local peer can be the initiator of IKE negotiation if the remote address is a host IP address or a host name. The local end can only be the responder of IKE negotiation if the remote address is an address range that the local peer can respond to.

If the IP address of the remote address changes frequently, configure the host name of the remote gateway with the **dynamic** keyword so that the local peer can use the up-to-date remote IP address to initiate IKE negotiation.

Examples

Configure the IP address of the remote security gateway as 10.0.0.1.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] remote-address 10.0.0.1
```

Configure the host name of the remote gateway as **test.com**, and specify the local peer to dynamically update the remote IP address.

```
<Sysname> system-view
[Sysname] ike peer peer2
[Sysname-ike-peer-peer2] remote-address test.com dynamic
```

Related commands

- **id-type ip**
- **local-address**

remote-name

Use **remote-name** to configure the name of the remote gateway.

Use **undo remote-name** to remove the configuration.

Syntax

remote-name *name*

undo remote-name

Views

IKE peer view

Default command level

2: System level

Parameters

name: Name of the peer security gateway for IKE negotiation, a string of 1 to 32 characters.

Usage guidelines

If you configure the **id-type name** or **id-type user-fqdn** command on the initiator, the IKE negotiation initiator sends its security gateway name as its ID for IKE negotiation, and the peer uses the security gateway name configured with the **remote-name** command to authenticate the initiator. Make sure the local gateway name matches the remote gateway name configured on the peer.

Examples

Configure the remote security gateway name as **apple** for IKE peer peer1.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] remote-name apple
```

Related commands

- **id-type**
- **ike local-name**
- **local-name**

reset ike sa

Use **reset ike sa** to clear IKE SAs.

Syntax

reset ike sa [*connection-id*]

Views

User view

Default command level

2: System level

Parameters

connection-id: Connection ID of the IKE SA to be cleared, in the range 1 to 2000000000.

Usage guidelines

If you do not specify a connection ID, the command clears all ISAKMP SAs.

When you clear a local IPsec SA, its ISAKMP SA can transmit the Delete message to notify the remote end to delete the paired IPsec SA. If the ISAKMP SA has been cleared, the local end cannot notify the remote end to clear the paired IPsec SA, and you must manually clear the remote IPsec SA.

Examples

Clear an IPsec tunnel to 202.38.0.2.

```
<Sysname> display ike sa
    total phase-1 SAs:  1
    connection-id  peer            flag        phase   doi
  ----------------------------------------------------------
      1            202.38.0.2      RD|ST       1       IPSEC
      2            202.38.0.2      RD|ST       2       IPSEC
flag meaning
RD--READY ST--STAYALIVE RL--REPLACED FD—FADING TO--TIMEOUT
<Sysname> reset ike sa 2
<Sysname> display ike sa
    total phase-1 SAs:  1
    connection-id  peer            flag        phase   doi
  ----------------------------------------------------------
      1            202.38.0.2      RD|ST       1       IPSEC
flag meaning
RD--READY ST--STAYALIVE RL--REPLACED FD—FADING TO—TIMEOUT
```

Related commands

display ike sa

sa duration

Use **sa duration** to set the ISAKMP SA lifetime for an IKE proposal.

Use **undo sa duration** to restore the default.

Syntax

sa duration *seconds*

undo sa duration

Default

The ISAKMP SA lifetime is 86400 seconds.

Views

IKE proposal view

Default command level

2: System level

Parameters

Seconds: Specifies the ISAKMP SA lifetime in seconds, in the range 60 to 604800.

Usage guidelines

Before an SA expires, IKE negotiates a new SA. The new SA takes effect immediately after being set up, and the old one will be cleared automatically when it expires.

Examples

Specify the ISAKMP SA lifetime for IKE proposal 10 as 600 seconds (10 minutes).

```
<Sysname> system-view
[Sysname] ike proposal 10
[Sysname-ike-proposal-10] sa duration 600
```

Related commands

- **display ike proposal**
- **ike proposal**

time-out

Use **time-out** to set the DPD packet retransmission interval for a DPD detector.

Use **undo time-out** to restore the default.

Syntax

time-out *time-out*

undo time-out

Default

The DPD packet retransmission interval is 5 seconds.

Views

IKE DPD view

Default command level

2: System level

Parameters

time-out: DPD packet retransmission interval in seconds, in the range 1 to 60.

Examples

Set the DPD packet retransmission interval to 1 second for dpd2.

```
<Sysname> system-view
[Sysname] ike dpd dpd2
[Sysname-ike-dpd-dpd2] time-out 1
```

New feature: Verifying the correctness and integrity of the file

Verifying the correctness and integrity of the file

Task	Command	Remarks
Verify the correctness and integrity of the file.	**crypto-digest sha256 file** *file-url*	Available in user view.

Command reference

crypto-digest

Use **crypto-digest** to calculate the digest value of a specific file.

Syntax

crypto-digest sha256 file *file-url*

Views

User view

Default command level

2: System level

Parameters

sha256: Specifies the digest algorithm SHA-256.

file *file-url*: Specifies a filename.

Usage guidelines

The digest value of a file is used to verify the correctness and integrity of the file. For example, you can use this command to calculate the digest value of a software package on your switch and compare it with the digest value issued by HP for the software package. If the two values are identical, it means that the package on your switch is the correct one.

Examples

Use SHA-256 to calculate the digest value of the file **1.bin**.

```
<Sysname> crypto-digest sha256 1.bin
Computing digest...
```

```
SHA256 digest(1.bin)=7bcb92458222f91f9a09a807c4c4567efd4d5dc4e4abc06c2a741df7045433eb
```

Modified feature: Configuring a password for the local user

Feature change description

Supported password to be saved by hash encryption algorithm and displayed as hash value.

Command changes

Modified command: password (local user view)

Old syntax

password [{ **cipher** | **simple** } *password*]

New syntax

password [[**hash**] { **cipher** | **simple** } *password*]

Views

Local user view

Change description

Before modification:

- Both ciphertext and plaintext passwords are supported.
- A plaintext password is a string of 1 to 63 characters. A ciphertext password is a string of 1 to 117 characters.

After modification:

- Both ciphertext and plaintext passwords are supported. The password is saved by hash encryption algorithm and displayed as hash value.
- If you do not specify hash encryption algorithm, a plaintext password is a string of 1 to 63 characters and a ciphertext password is a string of 1 to 117 characters.
- If you specify hash encryption algorithm, a plaintext password is a string of 1 to 63 characters and a ciphertext password is a string of 1 to 110 characters.

Modified feature: Clearing all users from the password control blacklist

Feature change description

Changed the command to clear all users from the password control blacklist.

Command changes

Modified command: reset password-control blacklist

Old syntax

reset password-control blacklist [**user-name** *name*]

New syntax

reset password-control blacklist { **all | user-name** *name* }

Views

User view

Change description

Before modification: The **reset password-control blacklist** command without the **user-name** *name* option specified clears all users from the password control blacklist.

After modification: The **reset password-control blacklist all** command clears all users from the password control blacklist.

Modified feature: 802.1X critical VLAN

Feature change description

The events that trigger an 802.1X user to be removed from the 802.1X critical VLAN change in this release. Any of the following events reflects that a RADIUS authentication server is reachable:

- An authentication server is added.
- A response from a RADIUS authentication server is received.
- The RADIUS server probing function detects that a RADIUS authentication server is reachable.

Command changes

None.

Modified feature: MAC authentication critical VLAN

Feature change description

The events that trigger an user to be removed from the MAC authentication critical VLAN change in this release. Any of the following events reflects that a RADIUS authentication server is reachable:

- An authentication server is added.
- A response from a RADIUS authentication server is received.
- The RADIUS server probing function detects that a RADIUS authentication server is reachable.

Command changes

None.

Modified feature: Modifying CLI configuration commands executed in FIPS mode for CC evaluation

Feature change description

Changed CLI configuration command keywords and value ranges when the device is operating in FIPS mode.

Modified command: super password

Old syntax

super password [**level** *user-level*] { **cipher** | **simple** } *password*

undo super password [**level** *user-level*]

New syntax

In non-FIPS mode:

super password [**level** *user-level*] [**hash**] { **cipher** | **simple** } *password*

undo super password [**level** *user-level*]

In FIPS mode:

super password [**level** *user-level*] { **cipher** | **simple** } *password*

undo super password [**level** *user-level*]

Views

2: System level

Parameters

level *user-level*: User privilege level, which ranges from 1 to 3 and defaults to 3.

Hash: Specifies hash encryption algorithm for generating password. (This keyword is not available for FIPS mode.)

cipher: Sets a ciphertext password for user privilege level switching.

simple: Sets a plaintext password for user privilege level switching.

password: Password string, case sensitive. Change description

In both FIPS and non-FIPS modes, the password must contain uppercase and lowercase letters, digits, and special characters.

In non-FIPS mode:

- If you specify the **simple** keyword, the password is a plaintext string 1 to 16 characters.
- If you specify the **cipher** and **hash** keywords, the password is a ciphertext string of 1 to 110 characters.
- If you specify the **cipher** keyword only, the password is a ciphertext string of 1 to 53 characters.

In FIPS mode:

- If you specify the **simple** keyword, the password is a plaintext string of 8 to 16 characters.
- If you specify the **cipher** keyword, the password is a ciphertext string of 8 to 53 characters.

Change description

After modification:

- In non-FIPS mode

- The **hash** keyword was added to support hash encryption algorithm for generating passwords for user privilege level switching.
- The length of the ciphertext password was changed. A ciphertext password can be a string of 1 to 53 characters, or 1 to 110 characters with the **hash** keyword specified.

- In FIPS mode
    - The length of a plaintext password was changed to be a string of 8 to 16 characters.
    - The length of a ciphertext password was changed to be a string of 8 to 53 characters.

Modified feature: Modifying login management commands executed in FIPS mode for CC evaluation

Feature change description

- Changed related command keywords and value ranges when the device is operating in FIPS mode.
- Added restrictions to related commands when the device is operating in FIPS mode: The commands **lock**, **user privilege level**, and **set authentication password** are not supported in FIPS mode.

Command changes

Modified command: authentication-mode

Use **authentication-mode** to set the authentication mode for the user interface.

Use **undo authentication-mode** to restore the default.

Old syntax

authentication-mode { **none** | **password** | **scheme** }

undo authentication-mode

New syntax

In non-FIPS mode:

authentication-mode { **none** | **password** | **scheme** }

undo authentication-mode

In FIPS mode:

authentication-mode scheme

undo authentication-mode

Default

In non-FIPS mode, the default authentication mode for VTY user interfaces is **password**, and for AUX user interfaces is **none**.

In FIPS mode, the default authentication mode is **scheme**.

Views

User interface view

Default command level

3: Manage level

Parameters

none: Performs no authentication. This keyword is not available for FIPS mode.

password: Performs local password authentication. This keyword is not available for FIPS mode.

scheme: Performs AAA authentication.

Change description

After modification: In FIPS mode, only the authentication mode **scheme** is supported and the keywords **none** and **password** are deleted.

Modified command: protocol inbound

Use **protocol inbound** to enable the current user interface to support either Telnet, SSH, or all of them. The configuration takes effect next time you log in.

Use **undo protocol inbound** to restore the default.

Old syntax

protocol inbound { **all** | **ssh** | **telnet** }

undo protocol inbound

New syntax

In non-FIPS mode:

protocol inbound { **all** | **ssh** | **telnet** }

undo protocol inbound

In FIPS mode:

protocol inbound { **all** | **ssh** }

undo protocol inbound

Default

All the three protocols are supported.

Views

VTY interface view

Default command level

3: Manage level

Parameters

all: Specifies both Telnet and SSH in non-FIPS mode, and only SSH in FIPS mode.

ssh: Specifies SSH only.

telnet: Specifies Telnet only. This keyword is not available for FIPS mode.

Change description

After modification: In FIPS mode, Telnet is not supported.

Modified command: set authentication password

In non-FIPS mode:

Use **set authentication password** to set an authentication password.

Use **undo set authentication password** to remove the local authentication password.

Old syntax

set authentication password { **cipher | simple** } *password*

undo set authentication password

New syntax

set authentication password [**hash**] { **cipher | simple** } *password*

undo set authentication password

Default

No local authentication password is set.

Views

User interface view

Default command level

3: Manage level

Parameters

Hash: Specifies hash encryption algorithm for generating password. (This keyword is not available for FIPS mode.)

cipher: Sets a ciphertext password for authentication.

simple: Sets a plaintext password for authentication.

- If you specify the **simple** keyword, the password is a plaintext string 1 to 16 characters.
- If you specify the **cipher** and **hash** keywords, the password is a ciphertext string of 1 to 110 characters.
- If you specify the **cipher** keyword only, the password is a ciphertext string of 1 to 53 characters.

Usage guidelines

For secrecy, all passwords, including passwords configured in plain text, are saved in cipher text.

This command is not supported in FIPS mode.

Change description

After modification: In non-FIPS mode,

- The **hash** keyword was added to support hash encryption algorithm for generating passwords for user privilege level switching.
- The length of the ciphertext password was changed. A ciphertext password can be a string of 1 to 53 characters, or 1 to 110 characters with the **hash** keyword specified.

Modified Feature: Modifying software upgrade commands executed in FIPS mode for CC evaluation

Feature change description

Added verification to the signatures of the system software image, Boot ROM image, and path files when the device is operating in FIPS mode.

- The system verifies the signature of the system software image after you execute the commands **boot-loader** and **boot-loader update file**. If the verification succeeds, the commands take effect.
- The system verifies the signature of the Boot ROM image after you execute the command **bootrom**. If the verification succeeds, the command takes effect.

- The system verifies the signatures of the path files after you execute the commands **patch install** and **patch load**. If the verification succeeds, the commands take effect.

Command changes

None.

Modified Feature: Modifying configuration file management commands executed in FIPS mode for CC evaluation

Feature change description

The **backup startup-configuration** and **restore startup-configuration** commands are not supported when the device is operating in FIPS mode.

Command changes

N/A

Modified Feature: Modifying security commands executed in FIPS mode for CC evaluation

Feature change description

Changed related security command keywords and value ranges when the device is operating in FIPS mode.

Command changes

Modified command: key (HWTACACS scheme view)

Syntax

key { **accounting** | **authentication** | **authorization** } [**cipher** | **simple**] *key*

undo key { **accounting** | **authentication** | **authorization** }

Views

HWTACACS scheme view

Default command level

2: System level

Change description

Before modification: The *key* argument specifies the plaintext or ciphertext key string and must contain at least 1 character.

After modification: In FIPS mode, the *key* argument specifies the plaintext or ciphertext key string and must contain at least 8 characters.

Modified command: key (RADIUS scheme view)

Syntax

key { **accounting** | **authentication** } [**cipher** | **simple**] *key*

undo key { **accounting** | **authentication** }

Views

RADIUS scheme view

Default command level

2: System level

Change description

Before modification: The *key* argument specifies the plaintext or ciphertext key string and must contain at least 1 character.

After modification: In FIPS mode, the *key* argument specifies the plaintext or ciphertext key string and must contain at least 8 characters.

Modified command: password

Old syntax

password [[**hash**] { **cipher** | **simple** } *password*]

undo password

New syntax

In non-FIPS mode:

password [[**hash**] { **cipher** | **simple** } *password*]

undo password

In FIPS mode:

password

undo password

Views

Local user view

Default command level

2: System level

Change description

In FIPS mode, parameters [**hash**] { **cipher** | **simple** } *password* are deleted.

The FIPS mode must operate with the password control feature. You always set the password in interactive mode. To use the interactive mode, enable the password control feature by the **password-control enable** command, and then do not specify any option for this command. For more information about password control commands, see the chapter "Password control configuration commands."

When password control is enabled, the password attributes, such as the password length and complexity, are under the restriction of the password control, and the local user password will not be displayed.

Modified command: primary accounting (RADIUS scheme view)

Syntax

primary accounting { *ipv4-address* **| ipv6** *ipv6-address* } [*port-number* **| key** [**cipher | simple**] *key* **| vpn-instance** *vpn-instance-name*] *

undo primary accounting

Views

RADIUS scheme view

Default command level

2: System level

Change description

Before modification: The *key* argument specifies the plaintext or ciphertext key string and must contain at least 1 character.

After modification: In FIPS mode, the *key* argument specifies the plaintext or ciphertext key string and must contain at least 8 characters.

Modified command: primary authentication (RADIUS scheme view)

Syntax

primary authentication { *ipv4-address* **| ipv6** *ipv6-address* } [*port-number* **| key** [**cipher | simple**] *key* **| vpn-instance** *vpn-instance-name* **| probe username** *name* [**interval** *interval*]] *

undo primary authentication

Views

RADIUS scheme view

Default command level

2: System level

Change description

Before modification: The *key* argument specifies the plaintext or ciphertext key string and must contain at least 1 character.

After modification: In FIPS mode, the *key* argument specifies the plaintext or ciphertext key string and must contain at least 8 characters.

Modified command: secondary accounting (RADIUS scheme view)

Syntax

secondary accounting { *ipv4-address* **| ipv6** *ipv6-address* } [*port-number* **| key** [**cipher | simple**] *key* **| vpn-instance** *vpn-instance-name*] *

undo secondary accounting [*ipv4-address* **| ipv6** *ipv6-address*]

Views

RADIUS scheme view

Default command level

2: System level

Change description

Before modification: The *key* argument specifies the plaintext or ciphertext key string and must contain at least 1 character.

After modification: In FIPS mode, the *key* argument specifies the plaintext or ciphertext key string and must contain at least 8 characters.

Modified command: secondary authentication (RADIUS scheme view)

Syntax

secondary authentication { *ipv4-address* **| ipv6** *ipv6-address* } [*port-number* **| key** [**cipher | simple**] *key* **| vpn-instance** *vpn-instance-name***|** **probe username** *name* [**interval** *interval*]] *

undo secondary authentication [*ipv4-address* **| ipv6** *ipv6-address*]

Views

RADIUS scheme view

Default command level

2: System level

Change description

Before modification: The *key* argument specifies the plaintext or ciphertext key string and must contain at least 1 character.

After modification: In FIPS mode, the *key* argument specifies the plaintext or ciphertext key string and must contain at least 8 characters.

Modified command: password-control composition

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

Default command level

2: System level

Change description

Before modification:

- The value range for the *type-number* argument is 1 to 4.
- The default global password composition policy is as follows: the minimum number of password composition types is 1 and the minimum number of characters of a password composition type is 1.

After modification:

- In FIPS mode, the value of the *type-number* argument must be 4.
- In FIPS mode, the default global password composition policy is as follows: the minimum number of password composition types is 4 and the minimum number of characters of a password composition type is 1.

Modified command: password-control length

Syntax

password-control length *length*

undo password-control length

Views

System view, user group view, local user view

Default command level

2: System level

Change description

Before modification: The *length* argument specifies the minimum password length in the range of 4 to 32.

After modification: The value range for the *length* argument is 8 to 32.

Modified command: password-control super composition

Syntax

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

undo password-control super composition

Views

System view

Default command level

2: System level

Change description

Before modification:

- The value range for the *type-number* argument is 1 to 4.
- By default, the minimum number of composition types is 1 and the minimum number of characters of a composition type is 1 for super passwords.

After modification:

- In FIPS mode, the value of the *type-number* argument must be 4.
- By default, the minimum number of composition types is 4 and the minimum number of characters of a composition type is 1 for super passwords in FIPS mode.

Modified command: password-control super length

Syntax

password-control super length *length*

undo password-control super length

Views

System view

Default command level

2: System level

Change description

Before modification: The *length* argument specifies the minimum length of a super password, in the range of 4 to 16.

After modification: The value range for the *length* argument is 8 to 16.

Modified command: public-key local create

Syntax

public-key local create { **dsa** | **rsa** }

Views

System view

Default command level

2: System level

Change description

Before modification: The DSA or RSA key modulus length is in the range of 512 to 2048 bits, and the default is 1024 bits.

After modification: In FIPS mode, the DSA key modulus length is in the range of 1024 to 2048 bits, and defaults to 1024 bits; the RSA key modulus length is 2048 bits. If the type of key pair already exists, the system asks you whether you want to overwrite it.

Modified command: scp

Old syntax

scp [**ipv6**] *server* [*port-number*] { **get** | **put** } *source-file-path* [*destination-file-path*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

New syntax

In non-FIPS mode:

scp [**ipv6**] *server* [*port-number*] { **get** | **put** } *source-file-path* [*destination-file-path*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

In FIPS mode:

scp [**ipv6**] *server* [*port-number*] { **get** | **put** } *source-file-path* [*destination-file-path*] [**identity-key rsa** | **prefer-ctos-cipher** { **aes128** | **aes256** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** } | **prefer-kex dh-group14** | **prefer-stoc-cipher** { **aes128** | **aes256** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** }] *

Views

User view

Default command level

3: Manage level

Change description

After modification:

- In FIPS mode, the following parameters are added:

- **prefer-ctos-cipher aes256**: Specifies **aes256-cbc** as the preferred encryption algorithm from client to server.
- **prefer-stoc-cipher aes256**: Specifies **aes256-cbc** as the preferred encryption algorithm from server to client.

- In FIPS mode, the following parameters are deleted:
  - **identity-key dsa**: Specifies **dsa** as the algorithm for public key authentication.
  - **prefer-ctos-cipher 3des**: Specifies **3des-cbc** as the preferred encryption algorithm from client to server.
  - **prefer-ctos-cipher des**: Specifies **des-cbc** as the preferred encryption algorithm from client to server.
  - **prefer-ctos-hmac md5**: Specifies **hmac-md5** as the preferred HMAC algorithm from client to server.
  - **prefer-ctos-hmac md5-96**: Specifies **hmac-md5-96** as the preferred HMAC algorithm from client to server.
  - **prefer-kex dh-group-exchange**: Specifies **diffie-hellman-group-exchange-sha1** as the preferred key exchange algorithm.
  - **prefer-kex dh-group1**: Specifies **diffie-hellman-group1-sha1** as the preferred key exchange algorithm.
  - **prefer-stoc-cipher 3des**: Specifies **3des-cbc** as the preferred encryption algorithm from server to client.
  - **prefer-stoc-cipher des**: Specifies **des-cbc** as the preferred encryption algorithm from server to client.
  - **prefer-stoc-hmac md5**: Specifies **hmac-md5** as the preferred HMAC algorithm from server to client.
  - **prefer-stoc-hmac md5-96**: Specifies **hmac-md5-96** as the preferred HMAC algorithm from server to client.

Modified command: ssh user

Old syntax

ssh user *username* **service-type stelnet authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* }

ssh user *username* **service-type** { **all** | **scp** | **sftp** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* **work-directory** *directory-name* }

undo ssh user *username*

New syntax

In non-FIPS mode:

ssh user *username* **service-type stelnet authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* }

ssh user *username* **service-type** { **all** | **scp** | **sftp** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* **work-directory** *directory-name* }

undo ssh user *username*

In FIPS mode:

ssh user *username* **service-type stelnet authentication-type** { **password** | **password-publickey assign publickey** *keyname* }

ssh user *username* **service-type** { **all** | **scp** | **sftp** } **authentication-type** { **password** | **password-publickey assign publickey** *keyname* **work-directory** *directory-name* }

undo ssh user *username*

Views

System view

Default command level

3: Manage level

Change description

After modification: In FIPS mode, the any authentication method and public key authentication method are deleted.

Modified command: ssh2

Old syntax

ssh2 [**ipv6** *server*] [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa | rsa** } **| prefer-ctos-cipher** { **3des | aes128 | des** } **| prefer-ctos-hmac** { **md5 | md5-96 | sha1 | sha1-96** } **| prefer-kex** { **dh-group-exchange | dh-group1 | dh-group14** } **| prefer-stoc-cipher** { **3des | aes128 | des** } **| prefer-stoc-hmac** { **md5 | md5-96 | sha1 | sha1-96** }] *

New syntax

In non-FIPS mode:

ssh2 [**ipv6** *server*] [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa | rsa** } **| prefer-ctos-cipher** { **3des | aes128 | des** } **| prefer-ctos-hmac** { **md5 | md5-96 | sha1 | sha1-96** } **| prefer-kex** { **dh-group-exchange | dh-group1 | dh-group14** } **| prefer-stoc-cipher** { **3des | aes128 | des** } **| prefer-stoc-hmac** { **md5 | md5-96 | sha1 | sha1-96** }] *

In FIPS mode:

ssh2 [**ipv6**] *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key rsa | prefer-ctos-cipher** { **aes128 | aes256** } **| prefer-ctos-hmac** { **sha1 | sha1-96** } **| prefer-kex dh-group14 | prefer-stoc-cipher** { **aes128 | aes256** } **| prefer-stoc-hmac** { **sha1 | sha1-96** }] *

Views

User view

Default command level

0: Visit level

Change description

After modification:

- In FIPS mode, the following parameters are added:
  - **prefer-ctos-cipher aes256**: Specifies **aes256-cbc** as the preferred encryption algorithm from client to server.
  - **prefer-stoc-cipher aes256**: Specifies **aes256-cbc** as the preferred encryption algorithm from server to client.
- In FIPS mode, the following parameters are deleted:
  - **identity-key dsa**: Specifies **dsa** as the algorithm for public key authentication.
  - **prefer-ctos-cipher 3des**: Specifies **3des-cbc** as the preferred encryption algorithm from client to server.
  - **prefer-ctos-cipher des**: Specifies **des-cbc** as the preferred encryption algorithm from client to server.
  - **prefer-ctos-hmac md5**: Specifies **hmac-md5** as the preferred HMAC algorithm from client to server.
  - **prefer-ctos-hmac md5-96**: Specifies **hmac-md5-96** as the preferred HMAC algorithm from client to server.

- **prefer-kex dh-group-exchange**: Specifies **diffie-hellman-group-exchange-sha1** as the preferred key exchange algorithm.
- **prefer-kex dh-group1**: Specifies **diffie-hellman-group1-sha1** as the preferred key exchange algorithm.
- **prefer-stoc-cipher 3des**: Specifies **3des-cbc** as the preferred encryption algorithm from server to client.
- **prefer-stoc-cipher des**: Specifies **des-cbc** as the preferred encryption algorithm from server to client.
- **prefer-stoc-hmac md5**: Specifies **hmac-md5** as the preferred HMAC algorithm from server to client.
- **prefer-stoc-hmac md5-96**: Specifies **hmac-md5-96** as the preferred HMAC algorithm from server to client.

Modified command: sftp

Old syntax

sftp [**ipv6**] *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa | rsa** } **| prefer-ctos-cipher** { **3des | aes128 | des** } **| prefer-ctos-hmac** { **md5 | md5-96 | sha1 | sha1-96** } **| prefer-kex** { **dh-group-exchange | dh-group1 | dh-group14** } **| prefer-stoc-cipher** { **3des | aes128 | des** } **| prefer-stoc-hmac** { **md5 | md5-96 | sha1 | sha1-96** }] *

New syntax

In non-FIPS mode:

sftp [**ipv6**] *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa | rsa** } **| prefer-ctos-cipher** { **3des | aes128 | des** } **| prefer-ctos-hmac** { **md5 | md5-96 | sha1 | sha1-96** } **| prefer-kex** { **dh-group-exchange | dh-group1 | dh-group14** } **| prefer-stoc-cipher** { **3des | aes128 | des** } **| prefer-stoc-hmac** { **md5 | md5-96 | sha1 | sha1-96** }] *

In FIPS mode:

sftp [**ipv6**] *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key rsa | prefer-ctos-cipher** { **aes128 | aes256** } **| prefer-ctos-hmac** { **sha1 | sha1-96** } **| prefer-kex dh-group14 | prefer-stoc-cipher** { **aes128 | aes256** } **| prefer-stoc-hmac** { **sha1 | sha1-96** }] *

Views

User view

Default command level

3: Manage level

Change description

After modification:

- In FIPS mode, the following parameters are added:
  - **prefer-ctos-cipher aes256**: Specifies **aes256-cbc** as the preferred encryption algorithm from client to server.
  - **prefer-stoc-cipher aes256**: Specifies **aes256-cbc** as the preferred encryption algorithm from server to client.
- In FIPS mode, the following parameters are deleted:
  - **identity-key dsa**: Specifies **dsa** as the algorithm for public key authentication.
  - **prefer-ctos-cipher 3des**: Specifies **3des-cbc** as the preferred encryption algorithm from client to server.
  - **prefer-ctos-cipher des**: Specifies **des-cbc** as the preferred encryption algorithm from client to server.

- **prefer-ctos-hmac md5**: Specifies **hmac-md5** as the preferred HMAC algorithm from client to server.
- **prefer-ctos-hmac md5-96**: Specifies **hmac-md5-96** as the preferred HMAC algorithm from client to server.
- **prefer-kex dh-group-exchange**: Specifies **diffie-hellman-group-exchange-sha1** as the preferred key exchange algorithm.
- **prefer-kex dh-group1**: Specifies **diffie-hellman-group1-sha1** as the preferred key exchange algorithm.
- **prefer-stoc-cipher 3des**: Specifies **3des-cbc** as the preferred encryption algorithm from server to client.
- **prefer-stoc-cipher des**: Specifies **des-cbc** as the preferred encryption algorithm from server to client.
- **prefer-stoc-hmac md5**: Specifies **hmac-md5** as the preferred HMAC algorithm from server to client.
- **prefer-stoc-hmac md5-96**: Specifies **hmac-md5-96** as the preferred HMAC algorithm from server to client.

Modified command: ciphersuite

Old syntax

ciphersuite [**rsa_3des_ede_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_256_cbc_sha** | **rsa_des_cbc_sha** | **rsa_rc4_128_md5** | **rsa_rc4_128_sha**] *

New syntax

In non-FIPS mode:

ciphersuite [**rsa_3des_ede_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_256_cbc_sha** | **rsa_des_cbc_sha** | **rsa_rc4_128_md5** | **rsa_rc4_128_sha**] *

In FIPS mode:

ciphersuite [**dhe_rsa_aes_128_cbc_sha** | **dhe_rsa_aes_256_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_256_cbc_sha**] *

Views

SSL server policy view

Default command level

2: System level

Change description

After modification:

- In FIPS mode, the following parameters are added:
  - **dhe_rsa_aes_128_cbc_sha**: Specifies the key exchange algorithm of DH_RSA, the data encryption algorithm of 128-bit AES_CBC, and the MAC algorithm of SHA.
  - **dhe_rsa_aes_256_cbc_sha**: Specifies the key exchange algorithm of DH_RSA, the data encryption algorithm of 256-bit AES_CBC, and the MAC algorithm of SHA.
- In FIPS mode, the following parameters are deleted:
  - **rsa_3des_ede_cbc_sha**: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 3DES_EDE_CBC, and the MAC algorithm of SHA.
  - **rsa_des_cbc_sha**: Specifies the key exchange algorithm of RSA, the data encryption algorithm of DES_CBC, and the MAC algorithm of SHA.
  - **rsa_rc4_128_md5**: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of MD5.

- **rsa_rc4_128_sha**: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of SHA.

Modified command: prefer-cipher

Old syntax

prefer-cipher { **rsa_3des_ede_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_256_cbc_sha** | **rsa_des_cbc_sha** | **rsa_rc4_128_md5** | **rsa_rc4_128_sha** }

undo prefer-cipher

New syntax

In non-FIPS mode:

prefer-cipher { **rsa_3des_ede_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_256_cbc_sha** | **rsa_des_cbc_sha** | **rsa_rc4_128_md5** | **rsa_rc4_128_sha** }

undo prefer-cipher

In FIPS mode:

prefer-cipher { **dhe_rsa_aes_128_cbc_sha** | **dhe_rsa_aes_256_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_256_cbc_sha** }

undo prefer-cipher

Views

SSL client policy view

Default command level

2: System level

Change description

After modification:

- In FIPS mode, the following parameters are added:
  - **dhe_rsa_aes_128_cbc_sha**: Specifies the key exchange algorithm of DH_RSA, the data encryption algorithm of 128-bit AES_CBC, and the MAC algorithm of SHA.
  - **dhe_rsa_aes_256_cbc_sha**: Specifies the key exchange algorithm of DH_RSA, the data encryption algorithm of 256-bit AES_CBC, and the MAC algorithm of SHA.
- In FIPS mode, the following parameters are deleted:
  - **rsa_3des_ede_cbc_sha**: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 3DES_EDE_CBC, and the MAC algorithm of SHA.
  - **rsa_des_cbc_sha**: Specifies the key exchange algorithm of RSA, the data encryption algorithm of DES_CBC, and the MAC algorithm of SHA.
  - **rsa_rc4_128_md5**: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of MD5.
  - **rsa_rc4_128_sha**: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of SHA.

Modified command: certificate request mode

Syntax

certificate request mode { **auto** [**key-length** *key-length* | **password** { **cipher** | **simple** } *password*] * | **manual** }

undo certificate request mode

Views

PKI domain view

Default command level

2: System level

Change description

Before modification: The *key-length* argument specifies the RSA key length in the range of 512 to 2048 bits, and the default is 1024 bits.

After modification: In FIPS mode, the value of the *key-length* argument must be 2048 bits.

Modified feature: Modifying SNMP commands executed in FIPS mode for CC evaluation

Feature change description

Changed related SNMP command keywords and value ranges when the device is operating in FIPS mode.

Command changes

Modified command: display snmp-agent community

Syntax

display snmp-agent community [**read** | **write**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Change description

This command is not supported in FIPS mode.

Modified command: snmp-agent community

Syntax

snmp-agent community { **read** | **write** } *community-name* [**acl** *acl-number* | **mib-view** *view-name*] *

undo snmp-agent community { **read** | **write** } *community-name*

Views

System view

Change description

This command is not supported in FIPS mode.

Modified command: snmp-agent group

Syntax

snmp-agent group { **v1** | **v2c** } *group-name* [**read-view** *view-name*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** *acl-number*]

undo snmp-agent group { **v1** | **v2c** } *group-name*

Views

System view

Change description

This command is not supported in FIPS mode.

Modified command: snmp-agent usm-user { v1 | v2c }

Syntax

snmp-agent group { **v1** | **v2c** } *group-name* [**read-view** *view-name*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** *acl-number*]

undo snmp-agent group { **v1** | **v2c** } *group-name*

Views

System view

Change description

This command is not supported in FIPS mode.

Modified command: snmp-agent calculate-password

Old syntax

snmp-agent calculate-password *plain-password* **mode** { **3desmd5** | **3dessha** | **md5** | **sha** } { **local-engineid** | **specified-engineid** *engineid* }

New syntax

In non-FIPS mode:

snmp-agent calculate-password *plain-password* **mode** { **3desmd5** | **3dessha** | **md5** | **sha** } { **local-engineid** | **specified-engineid** *engineid* }

In FIPS mode:

snmp-agent calculate-password *plain-password* **mode sha** { **local-engineid** | **specified-engineid** *engineid* }

Views

System view

Change description

After modification: In FIPS mode, the keywords **3desmd5**, **3dessha,** and **md5** are deleted.

Modified command: snmp-agent sys-info

Old syntax

snmp-agent sys-info { **contact** *sys-contact* | **location** *sys-location* | **version** { **all** | { **v1** | **v2c** | **v3** }***** } }

undo snmp-agent sys-info { **contact** | **location** | **version** { **all** | { **v1** | **v2c** | **v3** }* } }

New syntax

In non-FIPS mode:

snmp-agent sys-info { **contact** *sys-contact* | **location** *sys-location* | **version** { **all** | { **v1** | **v2c** | **v3** }* } }

undo snmp-agent sys-info { **contact** | **location** | **version** { **all** | { **v1** | **v2c** | **v3** }* } }

In FIPS mode:

snmp-agent sys-info { **contact** *sys-contact* | **location** *sys-location* | **version v3** }

undo snmp-agent sys-info { **contact** | **location** | **version v3** }

Views

System view

Change description

After modification: In FIPS mode, the keywords **all**, **v1,** and **v2c** are deleted.

Modified command: snmp-agent target-host

Old syntax

snmp-agent target-host trap address udp-domain { *ip-address* | **ipv6** *ipv6-address* } [**udp-port** *port-number*] [**dscp** *dscp-value*] [**vpn-instance** *vpn-instance-name*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]

undo snmp-agent target-host trap address udp-domain { *ip-address* | **ipv6** *ipv6-address* } **params securityname** *security-string* [**vpn-instance** *vpn-instance-name*]

New syntax

In non-FIPS mode:

snmp-agent target-host trap address udp-domain { *ip-address* | **ipv6** *ipv6-address* } [**udp-port** *port-number*] [**dscp** *dscp-value*] [**vpn-instance** *vpn-instance-name*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]

undo snmp-agent target-host trap address udp-domain { *ip-address* | **ipv6** *ipv6-address* } **params securityname** *security-string* [**vpn-instance** *vpn-instance-name*]

In FIPS mode:

snmp-agent target-host trap address udp-domain { *ip-address* | **ipv6** *ipv6-address* } [**udp-port** *port-number*] [**dscp** *dscp-value*] [**vpn-instance** *vpn-instance-name*] **params securityname** *security-string* **v3** [**authentication** | **privacy**]

undo snmp-agent target-host trap address udp-domain { *ip-address* | **ipv6** *ipv6-address* } **params securityname** *security-string* [**vpn-instance** *vpn-instance-name*]

Views

System view

Change description

After modification: In FIPS mode, the keywords **v1** and **v2c** are deleted.

Modified command: snmp-agent usm-user v3

Old syntax

snmp-agent usm-user v3 *user-name group-name* [**cipher**] [**authentication-mode** { **md5 | sha** } *auth-password* [**privacy-mode** { **3des | aes128 | des56** } *priv-password*]] [**acl** *acl-number* **| acl ipv6** *ipv6-acl-number*] *

undo snmp-agent usm-user v3 *user-name group-name* { **local | engineid** *engineid-string* }

New syntax

In non-FIPS mode:

snmp-agent usm-user v3 *user-name group-name* [**cipher**] [**authentication-mode** { **md5 | sha** } *auth-password* [**privacy-mode** { **3des | aes128 | des56** } *priv-password*]] [**acl** *acl-number* **| acl ipv6** *ipv6-acl-number*] *

undo snmp-agent usm-user v3 *user-name group-name* { **local | engineid** *engineid-string* }

In FIPS mode:

snmp-agent usm-user v3 *user-name group-name* [**cipher**] [**authentication-mode sha** *auth-password* [**privacy-mode aes128** *priv-password*]] [**acl** *acl-number* **| acl ipv6** *ipv6-acl-number*] *

undo snmp-agent usm-user v3 *user-name group-name* { **local | engineid** *engineid-string* }

Views

System view

Change description

After modification: In FIPS mode, the keywords **md5**, **3des,** and **des56** are deleted.

A5500EI-CMW520-R2215

This release has the following changes:

- New feature: Changing the brand name
- New feature: Configuring the maximum number of Selected ports allowed for an aggregation group
- New feature: Bulk configuring interfaces
- New feature: Configuring LLDP to advertise a specific voice VLAN
- Modified feature: Displaying the remaining power of the IRF fabric
- Modified feature: NTP
- Modified feature: Setting the IRF link down report delay

New feature: Changing the brand name

Changing the brand name

Some HP, H3C, and 3Com switches (see Table 16) can form an IRF fabric, and their MPUs are interchangeable.

If different brand MPUs are used on your switch or IRF fabric, change the MPU names to be the same to prevent an active/standby MPU switchover or master re-election from causing network management problems, including device information (vendor name, device model, and device panels) changes and re-collection of information about MPUs and other hardware components.

Table 16 HP, H3C, and 3Com switch model mappings

HP switch model	H3C switch model	3COM switch model
HP 5500-24G EI Switch with 2 Interface Slots (JD377A)	S5500-28C-EI	Switch 4800G 24-Port
HP 5500-48G EI Switch with 2 Interface Slots (JD375A)	S5500-52C-EI	Switch 4800G 48-Port
HP 5500-24G-SFP EI Switch with 2 Interface Slots (JD374A)	S5500-28F-EI	Switch 4800G 24-Port SFP
HP 5500-24G-PoE+ EI Switch with 2 Interface Slots(JG241A)	S5500-28C-PWR-EI	Switch 4800G PWR 24-Port
HP 5500-48G-PoE+ EI Switch with 2 Interface Slots (JG240A)	S5500-52C-PWR-EI	Switch 4800G PWR 48-Port

Configuration preparation

Before you change the brand name for an HP, H3C, or 3Com switch, prepare the proper Boot ROM and system software image file according to the switch model mappings as listed in Table 16. The following describes the procedure for changing the brand name of an H3C or 3Com switch to HP. The procedure is the same for changing the brand names among HP, H3C, and 3Com switches.

1. Load the proper HP Boot ROM to the flash memory of the H3C or 3Com switch and use the HP Boot ROM to upgrade the Boot ROM of the switch.
2. Load the proper HP system software image file to the flash memory of the H3C or 3Com switch, specify the file as the main system software image file, and reboot the switch.

3. Execute the **brand** command and reboot the switch.

NOTE:

For HP 5500 EI use the **bootrom update** command to upgrade the Boot ROM.

Configuration guidelines

- After you change the brand name of a 3Com switch to HP or H3C, the default baudrate of the console port changes from 19200 to 9600.
- The port numbering rule for 3Com switches is different from that for HP and H3C switches. After you change the brand name for a 3Com switch, the port numbers become inconsistent with the silkscreen marks. Configure the port (if necessary) according to the numbering rules for the models in Table 16.
- The default settings for some features on 3Com switches are different from those on HP and H3C switches. After you change the brand name for a switch, the default settings for those features become the default settings of the target brand.

Configuration procedure

You can use the **display brand** command to display the brand names of the member switches. If any consistent brand names exist in the IRF fabric, change them to the same.

To change brand name for a member switch:

Step	Command
1. Change the brand name for a member switch.	**brand** { **hp** | **h3c**| **3com** } [**slot** *slot-number*]
2. Reboot the member switch.	**reboot slot** *slot-number*

After you change the brand name for a member switch, the switch can use the later software versions for the new brand.

NOTE:

The default settings vary with different brands. Changing the brand name might affect the running configuration. After you change the brand name of a member switch, verify the configuration and re-configure the switch if necessary.

Command reference

brand

Syntax

brand { **hp** | **h3c** | **3com** } [**slot** *slot-number*]

View

User view

Default level

2: System level

Parameters

slot *slot-number*: Specifies an IRF member switch. If this option is not specified, the command applies to all member switches in the IRF fabric.

Description

Use **brand** to change the brand name for an IRF member switch.

After you perform this command, use the **display brand** command to verify the new brand name and then reboot the member switch to make your change take effect.

Examples

Display brand information.

```
<H3C>display brand
Current BRANDs:
 Slot 1: HP.
 Slot 3: H3C.
New BRANDs:
 Slot 1: HP.
 Slot 3: H3C.
<H3C>
```

Change the brand name of member switch 3 to HP.

```
<HP>brand hp slot 3
Configuration will take effect after next reboot.
 Do you want to continue? [Y/N]:y
 Configuration is successful.
```

Display brand information.

```
<H3C>display brand
Current BRANDs:
 Slot 1: HP.
 Slot 3: H3C.
New BRANDs:
 Slot 1: HP.
 Slot 3: HP.
<H3C>
The output shows that the brand name has been changed. After a reboot, member switch 3 becomes an HP member switch.
```

display brand

Syntax

display brand [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

User view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display brand** to display the brand name of a member switch.

Examples

Display the brand name of the current member switch.

```
<H3C>display brand
Current BRANDs:
 Slot 1: HP.
 Slot 3: H3C.
New BRANDs:
 Slot 1: HP.
 Slot 3: H3C.
<H3C>
```

New feature: Configuring the maximum number of Selected ports allowed for an aggregation group

By default, the maximum number of Selected ports allowed in an aggregation group depends on the hardware capabilities of the member ports. After you manually configure the maximum number of Selected ports in an aggregation group, the maximum number of Selected ports allowed in the aggregation group is the lower value of the two upper limits.

You can configure redundancy between two ports using the following guideline: Assign two ports to an aggregation group, and configure the maximum number of Selected ports allowed in the aggregation group as 1. In this way, only one Selected port is allowed in the aggregation group at any point in time, while the Unselected port serves as a backup port.

Configuration guidelines

Follow these guidelines when you configure the port threshold settings:

- If you set a minimum threshold for a static aggregation group, also make the same setting for its peer aggregation group to guarantee correct aggregation.
- Make sure the two link aggregation ends have the same maximum numbers of selected ports.

Make sure you understand the following impacts of the port threshold settings:

- Configuring the maximum number of Selected ports in an aggregation group may cause some of the selected member ports in the aggregation group to become unselected.

Configuration procedure

To configure the maximum number of Selected ports allowed for an aggregation group:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Enter aggregate interface view.	• Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number* • Enter Layer 3 aggregate interface view: **interface route-aggregation** *interface-number*	Use either command.
3. Configure the maximum number of Selected ports allowed for the aggregation group.	**link-aggregation selected-port maximum** *number*	By default, the maximum number of Selected ports allowed in an aggregation group depends on only the hardware capabilities of the member ports.

Command reference

link-aggregation selected-port maximum

Syntax

link-aggregation selected-port maximum *number*

undo link-aggregation selected-port maximum

View

Layer 2 aggregate interface view, Layer 3 aggregate interface view

Default level

2: System level

Parameters

number: Specifies the maximum number of Selected ports allowed in an aggregation group. This argument ranges from 1 to 8.

Description

Use **link-aggregation selected-port maximum** to configure the maximum number of Selected ports allowed in the aggregation group.

Use **undo link-aggregation selected-port maximum** to restore the default setting.

By default, the maximum number of Selected ports allowed in an aggregation group is limited only by the hardware capabilities of the member ports.

Executing this command may cause some of the member ports in the aggregation group to become unselected.

The maximum numbers of Selected ports for the local and peer aggregation groups must be consistent.

Examples

Configure the maximum number of Selected ports as 3 in the aggregation group corresponding to Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation selected-port maximum 3
```

New feature: Bulk configuring interfaces

You can enter interface range view to bulk configure multiple interfaces with the same feature instead of configuring them one by one. For example, you can perform the **shutdown** command in interface range view to shut down a range of interfaces.

Failure of applying a command on one member interface does not affect the application of the command on the other member interfaces. If applying a command on one member interface fails, the system displays an error message and continues with the next member interface.

Configuration guidelines

When you bulk configure interfaces in interface range view, follow these restrictions and guidelines:

- In interface range view, only the commands supported by the first interface are available.
- Do not assign an aggregate interface and any of its member interfaces to an interface range at the same time. Some commands, after being executed on both an aggregate interface and its member interfaces, can break up the aggregation.
- No limit is set on the maximum number of interfaces in an interface range. The more interfaces in an interface range, the longer the command execution time.

Configuration procedure

To bulk configure interfaces:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface range view.	Approach 1: **interface range** *interface-list* Approach 2: **interface range name** *name* [**interface** *interface-list*]	Use either approach. In approach 2, you assign a name to an interface range and can specify this name rather than the interface range to enter the interface range view.
3. Display commands available for the first interface in the interface range.	**Enter ?** at the interface range prompt.	Optional.
4. Perform available commands to configure the interfaces.	**Available commands vary by interface.**	N/A
5. Verify the configuration.	**display this**	Optional.

Command reference

interface range

Syntax

interface range *interface-list*

View

System view

Default level

2: System level

Parameters

interface-list: Interface list in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-5>. The *interface-type interface-number* argument specifies an interface by its type and number. &<1-5> indicates that you can specify up to five interfaces or interface lists. When you specify the **to** keyword in *interface-type interface-number1* **to** *interface-type interface-number2*, the interfaces before and after the **to** keyword must be on the same interface card or subcard, and the interface number before **to** must be no greater than the one after **to**.

Description

Use **interface range** to create an interface range and enter interface range view.

You can use this command to enter interface range view to bulk configure multiple interfaces with the same feature instead of configuring them one by one. For example, you can perform the **shutdown** command in interface range view to shut down a range of interfaces.

In interface range view, only the commands supported by the first interface are available. To view the commands supported by the first interface in the interface range, enter the interface range view and enter **?** at the command line interface prompt.

To verify the configuration of the first interface in the interface range, execute the **display this** command in interface range view.

Failure of applying a command on one member interface does not affect the application of the command on the other member interfaces. If applying a command on one member interface fails, the system displays an error message and continues with the next member interface.

Examples

Shut down interfaces GigabitEthernet 1/0/1 through GigabitEthernet 1/0/24, VLAN interface 2,

```
<Sysname> system-view
[Sysname] interface range gigabitethernet1/0/1 to gigabitethernet1/0/24 vlan-interface 2
[Sysname-if-range] shutdown
```

interface range name

Syntax

interface range name *name* [**interface** *interface-list*]

undo interface range name *name*

View

System view

Default level

2: System level

Parameters

name: Interface range name, a case-sensitive string of 1 to 32 characters.

interface-list: Interface list in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-5>. The *interface-type interface-number* argument specifies an interface by its type and number. &<1-5> indicates that you can specify up to five interfaces or interface lists. When you specify the **to** keyword in *interface-type interface-number1* **to** *interface-type interface-number2*, the interfaces before and after the **to** keyword must be on the same interface card or subcard, and the interface number before **to** must be no greater than the one after **to**.

Description

Use the **interface range name** *name* **interface** *interface-list* command to create an interface range, configure a name for the interface range, add interfaces to the interface range, and enter the interface range view.

Use the **interface range name** command without the **interface** keyword to enter the view of an interface range with the specified name.

Use **undo interface range name** to delete the interface range with the specified name.

You can use this command to assign a name to an interface range and can specify this name rather than the interface range to enter the interface range view.

You can use the **display current-configuration | include interface range** command to view the member interfaces of an interface range.

In interface range view, only the commands supported by the first interface are available. To view the commands supported by the first interface in the interface range, enter the interface range view and enter **?** at the command line interface prompt.

To verify the configuration of the first interface in the interface range, execute the **display this** command in interface range view.

Failure of applying a command on one member interface does not affect the application of the command on the other member interfaces. If applying a command on one member interface fails, the system displays an error message and continues with the next member interface.

When you bulk configure interfaces, follow these guidelines:

- Do not assign an aggregate interface and any of its member interfaces to an interface range at the same time. Some commands, after being executed on both an aggregate interface and its member interfaces, can break up the aggregation.
- No limit is set on the maximum number of interfaces in an interface range. The more interfaces in an interface range, the longer the command execution time.

Examples

Add GigabitEthernet 1/0/1 to GigabitEthernet 1/0/12 to interface range named **myEthPort**, and enter the interface range view.

```
<Sysname> system-view
[Sysname] interface range name myEthPort interface GigabitEthernet1/0/1 to
GigabitEthernet1/0/12
[Sysname-if-range-myEthPort]
```

Enter the view of interface range named **myEthPort**.

```
<Sysname> system-view
[Sysname] interface range name myEthPort
[Sysname-if-range-myEthPort]
```

New feature: Configuring LLDP to advertise a specific voice VLAN

Voice VLAN advertisement through LLDP is available only for LLDP-enabled IP phones. If CDP-compatibility is enabled, this feature is also available for CDP-enabled IP phones. For more information about LLDP, CDP compatibility, and voice VLANs, see *Layer 2—LAN Switching Configuration Guide*.

Configuration guidelines

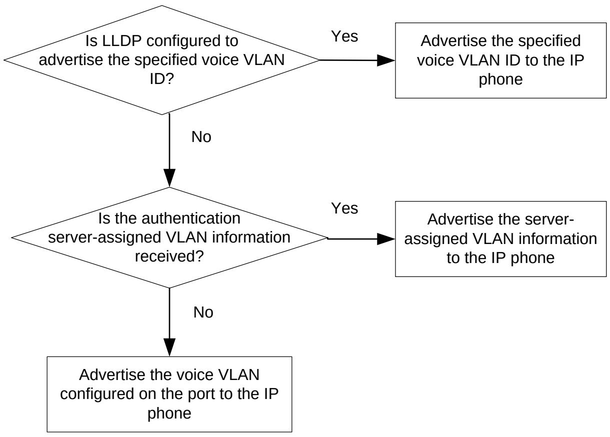
Use this feature in one of the following scenarios:

- Decrease the voice VLAN processing delay in an IRF fabric.

  By default, if the voice VLAN feature is configured on an LLDP-enabled port, LLDP advertises this voice VLAN to the IP hone connected to the port. When a packet arrives on the port, the switch compares the source MAC address against its voice device OUI list. If a match is found, the switch learns the MAC address in the voice VLAN, and promotes the forwarding priority for the packet. Because this process is completed in software, in an IRF fabric, MAC address learning and synchronization of the learned MAC address entry to all member devices introduces an undesirable delay. Directly specifying the voice VLAN to be advertised by LLDP enables the IRF fabric to learn and synchronize MAC address entries faster in hardware.
- Avoid configuring the voice VLAN function on a port.

Figure 1 shows the procedure of voice VLAN advertisement through LLDP.

Figure 1 Voice VLAN advertisement through LLDP



With the received voice VLAN information, the IP phone automatically completes the voice VLAN configuration, including the voice VLAN ID, tagging status, and priority. This voice VLAN can be the voice VLAN directly specified for LLDP advertisement, the voice VLAN configured on the port, or the voice VLAN assigned by a server, depending on your configuration.

To identify the voice VLAN advertised by LLDP, execute the **display lldp local-information** command, and examine the MED information fields in the command output.

Configuration procedure

To configure LLDP to advertise a specific voice VLAN:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view or port group view.	• Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* • Enter port group view: **port-group manual** *port-group-name*	Use one of the commands.
3. Configure LLDP to advertise a specific voice VLAN.	**lldp voice-vlan** *vlan-id*	By default, LLDP advertises the voice VLAN configured on the port.

Dynamically advertising server-assigned VLANs through LLDP

Dynamic advertisement of server-assigned VLANs through LLDP must work with 802.1X or MAC authentication, and is available only for LLDP-enabled IP phones. If 802.1X authentication is used, make sure the IP phones also support 802.1X authentication.

To implement this function for an IP phone, perform the following configuration tasks:

- Enable LLDP globally and on the port connected to the IP phone.
- Configure 802.1X or MAC authentication to make sure the IP phone can pass security authentication. For more information about 802.1X authentication, MAC authentication, and VLAN assignment by servers, see *Security Configuration Guide*.
- Configure VLAN authorization for the IP phone on the authentication server.

After the IP phone passes authentication, LLDP advertises the server-assigned VLAN in the Network Policy TLV to the IP phone. The IP phone will send its traffic tagged with the assigned VLAN.

Command reference

lldp voice-vlan

Syntax

lldp voice-vlan *vlan-id*

undo lldp voice-vlan

View

Layer 2 Ethernet interface view, port group view

Default level

2: System level

Parameters

vlan-id: Specifies a voice VLAN by its ID, which ranges from 1 to 4094.

Description

Use **lldp voice-vlan** *vlan-id* to configure a port to advertise a specific voice VLAN ID to the connected IP phone through LLDP. If CDP compatibility is enabled, LLDP also includes the specified voice VLAN ID in the CDP packets sent to the IP phone.

Use **undo lldp voice-vlan** to restore the default.

By default, if a voice VLAN is configured on an LLDP-enabled port, LLDP advertises this voice VLAN to the IP phone connected to the port.

Examples

Configure port GigabitEthernet 1/0/1 to advertise voice VLAN 4094.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp voice-vlan 4094
```

Modified feature: Displaying the remaining power of the IRF fabric

Feature change description

Before modification: The system displays only the remaining power of the master device.

After modification: The system displays the remaining power of each IRF member device.

Command changes

Modified command: display poe interface

Syntax

display poe interface [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Change description

Before modification: The **PSE** field is not displayed. The system displays only the remaining power of the master device.

After modification: The **PSE** field is displayed. The system displays the remaining power of each IRF member device.

Examples

Display the power supplying state of all PoE interfaces.

```
<Sysname> display poe interface
 Interface  Status   Priority  CurPower  Operating    IEEE   Detection
                              (W)        Status       Class  Status
 PSE : 4
 GE1/0/1      enabled  high     3.6      on           0      delivering-power
 GE1/0/2      enabled  low      0.0      off          0      searching
 GE1/0/3      enabled  low      0.0      off          0      searching
 GE1/0/4      enabled  low      0.0      off          0      searching
 GE1/0/5      enabled  low      0.0      off          0      searching
 GE1/0/6      enabled  low      0.0      off          0      searching
 GE1/0/7      enabled  low      0.0      off          0      searching
 GE1/0/8      enabled  low      0.0      off          0      searching
 ……
 GE1/0/23     enabled  low      0.0      off          0      searching
 GE1/0/24     enabled  low      0.0      off          0      searching

  ---  1 port(s) on,    3.6 (W) consumed,   367.4 (W) remaining ---

 PSE : 7
 GE2/0/1      enabled  high     7.6      on           0      delivering-power
 GE2/0/2      enabled  low      0.0      off          0      searching
 GE2/0/3      enabled  low      0.0      off          0      searching
 GE2/0/4      enabled  low      0.0      off          0      searching
```

```
 GE2/0/5      enabled  low      0.0      off          0      searching
 GE2/0/6      enabled  low      0.0      off          0      searching
 GE2/0/7      enabled  low      0.0      off          0      searching
 GE2/0/8      enabled  low      0.0      off          0      searching
 ……
 GE2/0/23     enabled  low      0.0      off          0      searching
 GE2/0/24     enabled  low      0.0      off          0      searching

  ---  1 port(s) on,    7.6 (W) consumed,   362.4 (W) remaining ---
```

Modified command: display poe interface power

Syntax

display poe interface power [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Change description

Before modification: The **PSE** field is not displayed. The system displays only the remaining power of the master device.

After modification: The **PSE** field is displayed. The system displays the remaining power of each IRF member device.

Examples

Display power information for all PoE interfaces.

```
<Sysname> display poe interface power
 Interface    CurPower  PeakPower   MaxPower  PD Description
               (W)       (W)         (W)
 PSE : 4
 GE1/0/1     0.0       0.0         15.4
 GE1/0/2     0.0       0.0         15.4
 GE1/0/3     0.0       0.0         15.4
 GE1/0/4     0.0       0.0         15.4
 GE1/0/5     0.0       0.0         15.4
 GE1/0/6     0.0       0.0         15.4
 GE1/0/7     0.0       0.0         15.4
 GE1/0/8     0.0       0.0         15.4
 ……
 GE1/0/23    0.0       0.0         15.4
 GE1/0/24    0.0       0.0         15.4
   ---  0 port(s) on,    0.0 (W) consumed,   370.0 (W) remaining ---

 PSE : 7
 GE2/0/1     0.0       0.0         15.4
 GE2/0/2     0.0       0.0         15.4
 GE2/0/3     0.0       0.0         15.4
 GE2/0/4     0.0       0.0         15.4
 GE2/0/5     0.0       0.0         15.4
 GE2/0/6     0.0       0.0         15.4
```

```
GE2/0/7     0.0       0.0         15.4
GE2/0/8     0.0       0.0         15.4
……
GE2/0/23    0.0       0.0         15.4
GE2/0/24    0.0       0.0         15.4
  ---  0 port(s) on,    0.0 (W) consumed,   370.0 (W) remaining ---
```

Modified feature: NTP

Feature change description

Added NTP version 4.

Command changes

Modified command: ntp-service broadcast-server

Syntax

ntp-service broadcast-server [**authentication-keyid** *keyid* **| version** *number*] *

View

Layer 3 Ethernet port view, VLAN interface view

Change description

Before modification: The **version** *number* option is in the range of 1 to 3.

After modification: The **version** *number* option is in the range of 1 to 4.

Modified command: ntp-service multicast-server

Syntax

ntp-service multicast-server [*ip-address*] [**authentication-keyid** *keyid* **| ttl** *ttl-number* **| version** *number*] *

View

Layer 3 Ethernet port view, VLAN interface view

Change description

Before modification: The **version** *number* option is in the range of 1 to 3.

After modification: The **version** *number* option is in the range of 1 to 4.

Modified command: ntp-service unicast-peer

Syntax

ntp-service unicast-peer [**vpn-instance** *vpn-instance-name*] { *ip-address* | *peer-name* } [**authentication-keyid** *keyid* **| priority | source-interface** *interface-type interface-number* **| version** *number*] *

View

System view

Change description

Before modification: The **version** *number* option is in the range of 1 to 3.

After modification: The **version** *number* option is in the range of 1 to 4.

Modified command: ntp-service unicast-server

Syntax

ntp-service unicast-server [**vpn-instance** *vpn-instance-name*] { *ip-address* | *server-name* } [**authentication-keyid** *keyid* | **priority** | **source-interface** *interface-type interface-number* | **version** *number*] *

View

System view

Change description

Before modification: The **version** *number* option is in the range of 1 to 3.

After modification: The **version** *number* option is in the range of 1 to 4.

Modified feature: Setting the IRF link down report delay

Feature change description

Changed the value range and the default value of the IRF link down report delay.

Command changes

Modified command: irf link-delay

Old syntax

irf link-delay *interval*

New syntax

irf link-delay *interval*

View

System view

Change description

Before modification: The value range (in milliseconds) for the *interval* argument is 200 to 2000. By default, IRF link down events are immediately reported to the upper layer.

After modification: The value range (in milliseconds) for the *interval* argument is 0 to 30000. By default, IRF link down events are reported 4 seconds later after their occurrence.

A5500EI-CMW520-F2212

This release has the following changes:

- New feature: Setting the DSCP value for multiple types of protocol packets
- New feature: Portal authentication in IPv6 networks
- Modified feature: Password configuration and display
- Modified feature: Task ID for IPv6 socket display
- Removed feature: Local user password display

New feature: Setting the DSCP value for multiple types of protocol packets

A field in an IPv4 or IPv6 header contains 8 bits and is used to identify the service type of an IP packet. In an IPv4 packet, this field is called “Type of Service (ToS).” In an IPv6 packet, this field is called “Traffic class.” According to RFC 2474, the ToS field is redefined as the differentiated services (DS) field, where a DSCP value is represented by the first six bits (0 to 5) and is in the range 0 to 63. The remaining two bits (6 and 7) are reserved. When a packet is being transmitted, the network devices can identify its DSCP value, and determines the transmission priority of the packet according to the DSCP value.

This release allows you to set the DSCP value for multiple types of protocol packets, including VRRP, RADIUS, SSH, HTTP, Telnet, FTP, TFTP, IGMP, MLD, PIM, IPv6 PIM, NTP, NQA, SNMP, ICMP, IGMP Snooping, MLD Snooping, DHCP, DNS, IPv6 DNS, DHCPv6, RIP, OSPF, BGP, and IPv6 BGP.

When you configure the DSCP value for some types of protocol packets, you should specify the ToS field value rather than the DSCP value. Because the DSCP field is the first 6 bits of the ToS field, each four continuous ToS field values, starting from 0, correspond to one DSCP value. An easier way to convert the DSCP value to the ToS value is to multiply the expected DSCP value by four to get the ToS field value.

Setting the DSCP value for BGP protocol packets

To set the DSCP value for BGP protocol packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter BGP view.	• Enter BGP view: **bgp** *as-number* • Enter BGP-VPN instance view: **a. bgp** as-number **b. ipv4-family vpn-instance** vpn-instance-name	Use either approach.
3. Set the DSCP value for BGP protocol packets sent to the specified BGP peer or BGP peer group.	**peer** { *group-name* | *ip-address* } **dscp** *dscp-value*	Optional. By default, the DSCP value in BGP protocol packets is 48.

Setting the DSCP value for DHCPv6 protocol packets

To set the DSCP value for DHCPv6 protocol packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the DSCP value for DHCPv6 protocol packets sent by the DHCPv6 servers and DHCPv6 relay agents.	**ipv6 dhcp dscp** *dscp-value*	Optional. By default, the DSCP value in DHCPv6 protocol packets sent by the DHCPv6 servers and DHCPv6 relay agents is 56.
3. Set the DSCP value for DHCPv6 protocol packets sent by the DHCPv6 clients.	**ipv6 dhcp client dscp** *dscp-value*	Optional. By default, the DSCP value in DHCPv6 protocol packets sent by the DHCPv6 clients is 56.

Setting the DSCP value for DHCP protocol packets

To set the DSCP value for DHCP protocol packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the DSCP value for DHCP protocol packets sent by the DHCP servers and DHCP relay agents.	**dhcp dscp** *dscp-value*	Optional. By default, the DSCP value in DHCP protocol packets sent by the DHCP servers and DHCP relay agents is 56.
3. Set the DSCP value for DHCP protocol packets sent by the DHCP clients.	**dhcp client dscp** *dscp-value*	Optional. By default, the DSCP value in DHCP protocol packets sent by the DHCP clients is 56.

Setting the DSCP value for DNS protocol packets

To set the DSCP value for DNS protocol packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the DSCP value for DNS protocol packets transmitted.	**dns dscp** *dscp-value*	Optional. By default, the DSCP value in DNS protocol packets transmitted is 0.

Setting the DSCP value for FTP and TFTP protocol packets

To set the DSCP value for FTP and TFTP protocol packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the DSCP value for protocol packets sent by the IPv4 FTP clients.	**ftp client dscp** *dscp-value*	Optional. By default, the DSCP value in protocol packets sent by the IPv4 FTP clients is 0.
3. Set the DSCP value for protocol packets sent by the IPv6 FTP clients.	**ftp client ipv6 dscp** *dscp-value*	Optional. By default, the DSCP value in protocol packets sent by the IPv6 FTP clients is 0.
4. Set the DSCP value for protocol packets sent by the IPv4 FTP servers.	**ftp server dscp** *dscp-value*	Optional. By default, the DSCP value in protocol packets sent by the IPv4 FTP servers is 0.
5. Set the DSCP value for protocol packets sent by the IPv4 TFTP clients.	**tftp client dscp** *dscp-value*	Optional. By default, the DSCP value in protocol packets sent by the IPv4 TFTP clients is 0.
6. Set the DSCP value for protocol packets sent by the IPv6 TFTP clients.	**tftp client ipv6 dscp** *dscp-value*	Optional. By default, the DSCP value in protocol packets sent by the IPv6 TFTP clients is 0.

Setting the DSCP value for HTTP protocol packets

To set the DSCP value for HTTP protocol packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the DSCP value for IPv4 HTTP protocol packets transmitted.	**ip http dscp** *dscp-value*	Optional. By default, the DSCP value in IPv4 HTTP protocol packets transmitted is 16.
3. Set the DSCP value for IPv6 HTTP protocol packets transmitted.	**ipv6 http dscp** *dscp-value*	Optional. By default, the DSCP value in IPv6 HTTP protocol packets transmitted is 0.

Setting the DSCP value for IGMP protocol packets sent by IGMP snooping

This configuration allows you to set the DSCP value for IGMP protocol packets sent by IGMP snooping.

To set the DSCP value for IGMP protocol packets transmitted:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Enter IGMP-snooping view.	**igmp-snooping**	N/A
3. Set the DSCP value for IGMP protocol packets transmitted.	**dscp** *dscp-value*	Required. By default, the DSCP value in IGMP protocol packets transmitted is 48.

Setting the DSCP value for IGMP protocol packets

To set the DSCP value for IGMP protocol packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter public network IGMP view or VPN instance IGMP view.	**igmp** [**vpn-instance** *vpn-instance-name*]	N/A
3. Set the DSCP value for IGMP protocol packets.	**dscp** *dscp-value*	Optional. By default, the DSCP value in IGMP protocol packets is 48.

Setting the DSCP value for IPv6 BGP protocol packets

To set the DSCP value for IPv6 BGP protocol packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter BGP view.	**bgp** as-number	Required.
3. Enter IPv6 address family view.	**ipv6-family**	N/A
4. Set the DSCP value for IPv6 BGP protocol packets sent to the specified IPv6 BGP peer or IPv6 BGP peer group.	**peer** { *ipv6-group-name* | *ipv6-address* } **dscp** *dscp-value*	Optional. By default, the DSCP value in IPv6 BGP protocol packets is 48.

Setting the DSCP value for IPv6 DNS protocol packets

To set the DSCP value for IPv6 DNS protocol packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the DSCP value for IPv6 DNS protocol packets transmitted.	**dns ipv6 dscp** *dscp-value*	Optional. By default, the DSCP value in IPv6 DNS protocol packets transmitted is 0.

Setting the DSCP value for IPv6 PIM protocol packets

To set the DSCP value for IPv6 PIM protocol packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter IPv6 PIM view.	**pim ipv6**	N/A
3. Set the DSCP value for IPv6 PIM protocol packets.	**dscp** *dscp-value*	Optional. By default, the DSCP value in IPv6 PIM protocol packets is 48.

Setting the DSCP value for MLD protocol packets sent by MLD snooping

This configuration allows you to set the DSCP value for MLD protocol packets sent by MLD snooping.

To set the DSCP value for MLD protocol packets transmitted:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter MLD-snooping view.	**mld-snooping**	N/A
3. Set the DSCP value for MLD protocol packets transmitted.	**dscp** *dscp-value*	Required. By default, the DSCP value in MLD protocol packets transmitted is 48.

Setting the DSCP value for MLD protocol packets

To set the DSCP value for MLD protocol packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter MLD view.	**mld**	N/A
3. Set the DSCP value for MLD protocol packets.	**dscp** *dscp-value*	Optional. By default, the DSCP value in MLD protocol packets is 48.

Setting the ToS value for packets sent by the TCP listening service on the NQA server

To set the ToS value for packets sent by the TCP listening service on the NQA server:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Set the ToS value for packets sent by the TCP listening service on the NQA server.	**nqa server tcp-connect tos** *tos*	Optional. By default, the ToS value in the packets sent by the TCP listening service on the NQA server is 0.

Setting the ToS value for packets sent by the UDP listening service on the NQA server

To set the ToS value for packets sent by the UDP listening service on the NQA server:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the ToS value for packets sent by the UDP listening service on the NQA server.	**nqa server udp-echo tos** *tos*	Optional. By default, the ToS value in the packets sent by the UDP listening service on the NQA server is 0.

Setting the ToS value for NQA probe packets

To set the ToS value for NQA probe packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter NQA operation view.	**nqa entry** *admin-name operation-tag*	N/A
3. Specify the DHCP type and enter its view.	**type dhcp**	Required.
4. Set the ToS value for NQA probe packets.	**tos** *value*	Optional. By default, the ToS value in NQA probe packets is 0.

Setting the DSCP value for NTP protocol packets

To set the DSCP value for NTP protocol packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the DSCP value for NTP protocol packets.	**ntp-service dscp** *dscp-value*	Optional. By default, the DSCP value in NTP protocol packets is 16.

Setting the DSCP value for OSPF protocol packets

To set the DSCP value for OSPF protocol packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable an OSPF process.	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	Required. By default, no OSPF process is enabled.
3. Set the DSCP value for OSPF protocol packets.	**dscp** *dscp-value*	Optional. By default, the DSCP value in OSPF protocol packets is 48.

Setting the DSCP value for PIM protocol packets

To set the DSCP value for PIM protocol packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter public network IGMP view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	N/A
3. Set the DSCP value for PIM protocol packets.	**dscp** *dscp-value*	Optional. By default, the DSCP value in PIM protocol packets is 48.

Setting the DSCP value for RADIUS protocol packets

To set the DSCP value for RADIUS protocol packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the DSCP value for IPv4 RADIUS protocol packets.	**radius dscp** *dscp-value*	Optional. By default, the DSCP value in IPv4 RADIUS protocol packets is 0.
3. Set the DSCP value for IPv6 RADIUS protocol packets.	**radius ipv6 dscp** *dscp-value*	Optional. By default, the DSCP value in IPv6 RADIUS protocol packets is 0.

Setting the DSCP value for RIP protocol packets

To set the DSCP value for RIP protocol packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a RIP process and enter RIP view.	**rip** [*process-id*] [**vpn-instance** *vpn-instance-name*]	Required. By default, no RIP process runs.

Step	Command	Remarks
3. Set the DSCP value for RIP protocol packets.	**dscp** *dscp-value*	Optional. By default, the DSCP value in RIP protocol packets is 48.

Setting the DSCP value for SNMP trap packets

To set the DSCP value for SNMP trap packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the DSCP value for SNMP trap packets.	**snmp-agent target-host trap address udp-domain** { *ip-address* | **ipv6** *ipv6-address* } [**udp-port** *port-number*] [**dscp** *dscp-value*] [**vpn-instance** *vpn-instance-name*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]	Optional. By default, the DSCP value in SNMP trap packets is 0.

Setting the DSCP value for SNMP response packets

To set the DSCP value for SNMP response packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the DSCP value for SNMP response packets.	**snmp-agent packet response dscp** *dscp-value*	Optional. By default, the DSCP value in SNMP response packets is 0.

Setting the DSCP value for SSH protocol packets

To set the DSCP value for SSH protocol packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the DSCP value for protocol packets sent by the IPv4 SSH servers.	**ssh server dscp** *dscp-value*	Optional. By default, the DSCP value in protocol packets sent by the IPv4 SSH servers is 16.
3. Set the DSCP value for protocol packets sent by the IPv6 SSH servers.	**ssh server ipv6 dscp** *dscp-value*	Optional. By default, the DSCP value in protocol packets sent by the IPv6 SSH servers is 0.

Step	Command	Remarks
4. Set the DSCP value for protocol packets sent by the IPv4 SSH clients.	**ssh client dscp** *dscp-value*	Optional. By default, the DSCP value in protocol packets sent by the IPv4 SSH clients is 16.
5. Set the DSCP value for protocol packets sent by the IPv6 SSH clients.	**ssh client ipv6 dscp** *dscp-value*	Optional. By default, the DSCP value in protocol packets sent by the IPv6 SSH clients is 0.
6. Set the DSCP value for protocol packets sent by the IPv4 SFTP clients.	**sftp client dscp** *dscp-value*	Optional. By default, the DSCP value in protocol packets sent by the IPv4 SFTP clients is 16.
7. Set the DSCP value for protocol packets sent by the IPv6 SFTP clients.	**sftp client ipv6 dscp** *dscp-value*	Optional. By default, the DSCP value in protocol packets sent by the IPv6 SFTP clients is 8.

Setting the DSCP value for Telnet protocol packets

To set the DSCP value for Telnet protocol packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the DSCP value for protocol packets sent by the IPv4 Telnet clients.	**telnet client dscp** *dscp-value*	Optional. By default, the DSCP value in protocol packets sent by the IPv4 Telnet clients is 16.
3. Set the DSCP value for protocol packets sent by the IPv6 Telnet clients.	**telnet client ipv6 dscp** *dscp-value*	Optional. By default, the DSCP value in protocol packets sent by the IPv6 Telnet clients is 0.
4. Set the DSCP value for protocol packets sent by the IPv4 Telnet servers.	**telnet server dscp** *dscp-value*	Optional. By default, the DSCP value in protocol packets sent by the IPv4 Telnet servers is 48.
5. Set the DSCP value for protocol packets sent by the IPv6 Telnet servers.	**telnet server ipv6 dscp** *dscp-value*	Optional. By default, the DSCP value in protocol packets sent by the IPv6 Telnet servers is 0.

Setting the DSCP value for VRRP protocol packets

To set the DSCP value for VRRP protocol packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Set the DSCP value for IPv4 VRRP protocol packets.	**vrrp dscp** *dscp-value*	Optional. By default, the DSCP value in IPv4 VRRP protocol packets is 48.
3. Set the DSCP value for IPv6 VRRP protocol packets.	**vrrp ipv6 dscp** *dscp-value*	Optional. By default, the DSCP value in IPv6 VRRP protocol packets is 56.

Setting the DSCP value for the protocol packets sent to the log host

To set the DSCP value for the protocol packets sent to the log host:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the DSCP value for the protocol packets sent to the log host.	**info-center loghost** [**vpn-instance** *vpn-instance-name*] { *host-ipv4-address* | **ipv6** *host-ipv6-address* } [**port** *port-number*] [**dscp** *dscp-value*] [**channel** { *channel-number* | *channel-name* } | **facility** *local-number*] *	Optional. By default, the DSCP value in the protocol packets sent to the log host is 0.

New commands

dhcp client dscp

Syntax

dhcp client dscp *dscp-value*

undo dhcp client dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the DHCP protocol packets transmitted, which ranges from 0 to 63.

Description

Use the **dhcp client dscp** command to set the DSCP value for DHCP protocol packets sent by the DHCP clients.

Use the **undo dhcp client dscp** command to restore the default.

By default, the DSCP value in DHCP protocol packets sent by the DHCP clients is 56.

Examples

Set the DSCP value to 30 for DHCP protocol packets sent by the DHCP clients.

```
<Sysname> system-view
[Sysname] dhcp client dscp 30
```

dhcp dscp

Syntax

dhcp dscp *dscp-value*

undo dhcp dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the DHCP protocol packets transmitted, which ranges from 0 to 63.

Description

Use the **dhcp dscp** command to set the DSCP value for DHCP protocol packets sent by the DHCP servers and DHCP relay agents.

Use the **undo dhcp dscp** command to restore the default.

By default, the DSCP value in DHCP protocol packets sent by the DHCP servers and DHCP relay agents is 56.

Examples

Set the DSCP value to 30 for DHCP protocol packets transmitted.

```
<Sysname> system-view
[Sysname] dhcp dscp 30
```

dns dscp

Syntax

dns dscp *dscp-value*

undo dns dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the DNS protocol packets transmitted, which ranges from 0 to 63.

Description

Use the **dns dscp** command to set the DSCP value for DNS protocol packets transmitted.

Use the **undo dns dscp** command to restore the default.

By default, the DSCP value in DNS protocol packets transmitted is 0.

Examples

Set the DSCP value to 30 for DNS protocol packets transmitted.

```
<Sysname> system-view
[Sysname] dns dscp 30
```

dns ipv6 dscp

Syntax

dns ipv6 dscp *dscp-value*

undo dns ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the IPv6 DNS protocol packets transmitted, which ranges from 0 to 63.

Description

Use the **dns ipv6 dscp** command to set the DSCP value for IPv6 DNS protocol packets transmitted.

Use the **undo dns ipv6 dscp** command to restore the default.

By default, the DSCP value in IPv6 DNS protocol packets transmitted is 0.

Examples

Set the DSCP value to 30 for IPv6 DNS protocol packets transmitted.

```
<Sysname> system-view
[Sysname] dns ipv6 dscp 30
```

dscp (IGMP view)

Syntax

dscp *dscp-value*

undo dscp

View

Public network IGMP view, VPN instance IGMP view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **dscp** command to set the DSCP value for IGMP protocol packets.

Use the **undo dscp** command to restore the default.

By default, the DSCP value in IGMP protocol packets is 48.

Examples

Set the DSCP value to 63 for IGMP protocol packets in the public network.

```
<Sysname> system-view
[Sysname] igmp
```

```
[Sysname-igmp] dscp 63
```

Set the DSCP value to 63 for IGMP protocol packets in the VPN instance named **mvpn**.

```
<Sysname> system-view
[Sysname] igmp vpn-instance mvpn
[Sysname-igmp-mvpn] dscp 63
```

dscp (IGMP-Snooping view)

Syntax

dscp *dscp-value*

undo dscp

View

IGMP-snooping view

Default level

2: System level

Parameters

dscp-value: DSCP value in the IGMP protocol packets transmitted, which ranges from 0 to 63.

Description

Use the **dscp** command to set the DSCP value for IGMP protocol packets transmitted.

Use the **undo dscp** command to restore the default.

By default, the DSCP value in IGMP protocol packets transmitted is 48.

Examples

Set the DSCP value to 63 for IGMP protocol packets transmitted.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] dscp 63
```

dscp (IPv6 PIM view)

Syntax

dscp *dscp-value*

undo dscp

View

IPv6 PIM view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **dscp** command to set the DSCP value for IPv6 PIM protocol packets.

Use the **undo dscp** command to restore the default.

By default, the DSCP value in IPv6 PIM protocol packets is 48.

Examples

Set the DSCP value to 63 for IPv6 PIM protocol packets.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] dscp 63
```

dscp (MLD view)

Syntax

dscp *dscp-value*

undo dscp

View

MLD view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **dscp** command to set the DSCP value for MLD protocol packets.

Use the **undo dscp** command to restore the default.

By default, the DSCP value in MLD protocol packets is 48.

Examples

Set the DSCP value to 63 for MLD protocol packets.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] dscp 63
```

dscp (MLD-Snooping view)

Syntax

dscp *dscp-value*

undo dscp

View

MLD-snooping view

Default level

2: System level

Parameters

dscp-value: DSCP value in the MLD protocol packets transmitted, which ranges from 0 to 63.

Description

Use the **dscp** command to set the DSCP value for MLD protocol packets transmitted.

Use the **undo dscp** command to restore the default.

By default, the DSCP value in MLD protocol packets transmitted is 48.

Examples

Set the DSCP value to 63 for MLD protocol packets transmitted by MLD-snooping.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] dscp 63
```

dscp (OSPF view)

Syntax

dscp *dscp-value*

undo dscp

View

OSPF view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **dscp** command to set the DSCP value for OSPF protocol packets.

Use the **undo dscp** command to restore the default.

By default, the DSCP value in OSPF protocol packets is 48.

Examples

Set the DSCP value to 63 for OSPF protocol packets sent by OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf
[Sysname-ospf-1] dscp 63
```

dscp (PIM view)

Syntax

dscp *dscp-value*

undo dscp

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **dscp** command to set the DSCP value for PIM protocol packets.

Use the **undo dscp** command to restore the default.

By default, the DSCP value in PIM protocol packets is 48.

Examples

Set the DSCP value to 63 for PIM protocol packets in the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] dscp 63
```

Set the DSCP value to 63 for PIM protocol packets in the VPN instance named **mvpn**.

```
<Sysname> system-view
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] dscp 63
```

dscp (RIP view)

Syntax

dscp *dscp-value*

undo dscp

View

RIP view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **dscp** command to set the DSCP value for RIP protocol packets.

Use the **undo dscp** command to restore the default.

By default, the DSCP value in RIP protocol packets is 48.

Examples

Set the DSCP value to 63 for RIP protocol packets sent by RIP process 1.

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1] dscp 63
```

ftp client dscp

Syntax

ftp client dscp *dscp-value*

undo ftp client dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **ftp client dscp** command to set the DSCP value for FTP protocol packets sent by the FTP clients.

Use the **undo ftp client dscp** command to restore the default.

By default, the DSCP value in protocol packets sent by the FTP clients is 0.

Examples

Set the DSCP value to 30 for protocol packets sent by the FTP clients.

```
<Sysname> system-view
[Sysname] ftp client dscp 30
```

ftp client ipv6 dscp

Syntax

ftp client ipv6 dscp *dscp-value*

undo ftp client ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **ftp client ipv6 dscp** command to set the DSCP value for FTP protocol packets sent by the IPv6 FTP clients.

Use the **undo ftp client ipv6 dscp** command to restore the default.

By default, the DSCP value in protocol packets sent by the IPv6 FTP clients is 0.

Examples

Set the DSCP value to 30 for protocol packets sent by the IPv6 FTP clients.

```
<Sysname> system-view
[Sysname] ftp client ipv6 dscp 30
```

ftp server dscp

Syntax

ftp server dscp *dscp-value*

undo ftp server dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **ftp server dscp** command to set the DSCP value for FTP protocol packets sent by the FTP servers.

Use the **undo ftp server dscp** command to restore the default.

By default, the DSCP value in protocol packets sent by the FTP servers is 0.

Examples

Set the DSCP value to 30 for protocol packets sent by the FTP servers.

```
<Sysname> system-view
[Sysname] ftp server dscp 30
```

ip http dscp

Syntax

ip http dscp *dscp-value*

undo ip http dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **ip http dscp** command to set the DSCP value for HTTP protocol packets transmitted.

Use the **undo ip http dscp** command to restore the default.

By default, the DSCP value in HTTP protocol packets transmitted is 16.

Examples

Set the DSCP value to 30 for HTTP protocol packets transmitted.

```
<Sysname> system-view
[Sysname] ip http dscp 30
```

ipv6 dhcp client dscp

Syntax

ipv6 dhcp client dscp *dscp-value*

undo ipv6 dhcp client dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the DHCPv6 protocol packets transmitted, which ranges from 0 to 63.

Description

Use the **ipv6 dhcp client dscp** command to set the DSCP value for DHCPv6 protocol packets sent by the DHCPv6 clients.

Use the **undo ipv6 dhcp client dscp** command to restore the default.

By default, the DSCP value in DHCPv6 protocol packets sent by the DHCPv6 clients is 56.

Examples

Set the DSCP value to 30 for DHCPv6 protocol packets sent by the DHCPv6 clients.

```
<Sysname> system-view
[Sysname] ipv6 dhcp client dscp 30
```

ipv6 dhcp dscp

Syntax

ipv6 dhcp dscp *dscp-value*

undo ipv6 dhcp dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the DHCPv6 protocol packets transmitted, which ranges from 0 to 63.

Description

Use the **ipv6 dhcp dscp** command to set the DSCP value for DHCPv6 protocol packets sent by the DHCPv6 servers and DHCPv6 relay agents.

Use the **undo ipv6 dhcp dscp** command to restore the default.

By default, the DSCP value in DHCPv6 protocol packets sent by the DHCPv6 servers and DHCPv6 relay agents is 56.

Examples

Set the DSCP value to 30 for the DHCPv6 protocol packets sent by the DHCPv6 servers and DHCPv6 relay agents.

```
<Sysname> system-view
[Sysname] ipv6 dhcp dscp 30
```

ipv6 http dscp

Syntax

ipv6 http dscp *dscp-value*

undo ipv6 http dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **ipv6 http dscp** command to set the DSCP value for IPv6 HTTP protocol packets transmitted.

Use the **undo ipv6 http dscp** command to restore the default.

By default, the DSCP value in IPv6 HTTP protocol packets transmitted is 0.

Examples

Set the DSCP value to 30 for IPv6 HTTP protocol packets transmitted.

```
<Sysname> system-view
[Sysname] ipv6 http dscp 30
```

nqa server tcp-connect tos

Syntax

nqa server tcp-connect tos *tos*

undo nqa server tcp-connect tos

View

System view

Default level

2: System level

Parameters

tos: Type of Service (ToS) field value in the protocol packets sent by the TCP listening service on the NQA server. This argument ranges from 0 to 255.

Description

Use the **nqa server tcp-connect tos** command to set the ToS value for packets sent by the TCP listening service on the NQA server.

Use the **undo nqa server tcp-connect tos** command to restore the default.

By default, the ToS value in the packets sent by the TCP listening service on the NQA server is 0.

Examples

Set the ToS value to 30 for packets sent by the TCP listening service on the NQA server.

```
<Sysname> system-view
[Sysname] nqa server tcp-connect tos 30
```

nqa server udp-echo tos

Syntax

nqa server udp-echo tos *tos*

undo nqa server udp-echo tos

View

System view

Default level

2: System level

Parameters

tos: Type of Service (ToS) field value in the protocol packets sent by the UDP listening service on the NQA server. This argument ranges from 0 to 255.

Description

Use the **nqa server udp-echo tos** command to set the ToS value for packets sent by the UDP listening service on the NQA server.

Use the **undo nqa server udp-echo tos** command to restore the default.

By default, the ToS value in the packets sent by the UDP listening service on the NQA server is 0.

Examples

Set the ToS value to 30 for packets sent by the UDP listening service on the NQA server.

```
<Sysname> system-view
[Sysname] nqa server udp-echo tos 30
```

ntp-service dscp

Syntax

ntp-service dscp *dscp-value*

undo ntp-service dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **ntp-service dscp** command to set the DSCP value for NTP protocol packets.

Use the **undo ntp-service dscp** command to restore the default.

By default, the DSCP value in NTP protocol packets is 16.

Examples

Set the DSCP value to 30 for NTP protocol packets.

```
<Sysname> system-view
[Sysname] ntp-service dscp 30
```

peer dscp (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* **|** *ip-address* } **dscp** *dscp-value*

undo peer { *group-name* **|** *ip-address* } **dscp**

View

BGP view, BGP VPN instance view

Default level

2: System level

Parameters

group-name: Peer group name, a string of 1 to 47 characters.

ip-address: IP address of a peer.

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **peer dscp** command to set the DSCP value for BGP protocol packets sent to the specified BGP peer or BGP peer group.

Use the **undo peer dscp** command to cancel the configuration.

By default, the DSCP value in BGP protocol packets is 48.

Make sure that the specified BGP peer or BGP peer group already exists.

Examples

In BGP view, set the DSCP value to 63 for BGP protocol packets sent to the BGP peer group named **test**, which already exists.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test dscp 63
```

In BGP VPN instance view, set the DSCP value to 63 for BGP protocol packets sent to the BGP peer group named **test**, which already exists. (You must create VPN instance **vpn1** first)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer test dscp 63
```

peer dscp (IPv6 address family view)

Syntax

peer { *ipv6-group-name* **|** *ipv6-address* } **dscp** *dscp-value*

undo peer { *ipv6-group-name* **|** *ipv6-address* } **dscp**

View

IPv6 address family view

Default level

2: System level

Parameters

ipv6-group-name: Peer group name, a string of 1 to 47 characters.

Ipv6-address: IPv6 address of a peer.

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **peer dscp** command to set the DSCP value for IPv6 BGP protocol packets sent to the specified IPv6 peer or IPv6 peer group.

Use the **undo peer dscp** command to cancel the configuration.

By default, the DSCP value in IPv6 BGP protocol packets is 48.

Make sure that the specified IPv6 peer or IPv6 peer group already exists.

Examples

Set the DSCP value to 63 for IPv6 BGP protocol packets sent to the EBGP peer group named **test**.

```
<Sysname] system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test dscp 63
```

radius dscp

Syntax

radius dscp *dscp-value*

undo radius dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **radius dscp** command to set the DSCP value for IPv4 RADIUS protocol packets.

Use the **undo radius dscp** command to restore the default.

By default, the DSCP value in IPv4 RADIUS protocol packets is 0.

Examples

Set the DSCP value to 6 for IPv4 RADIUS protocol packets.

```
<Sysname> system-view
[Sysname] radius dscp 6
```

radius ipv6 dscp

Syntax

radius ipv6 dscp *dscp-value*

undo radius ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **radius ipv6 dscp** command to set the DSCP value for IPv6 RADIUS protocol packets.

Use the **undo radius ipv6 dscp** command to restore the default.

By default, the DSCP value in IPv6 RADIUS protocol packets is 0.

Examples

Set the DSCP value to 6 for IPv6 RADIUS protocol packets.

```
<Sysname> system-view
[Sysname] radius ipv6 dscp 6
```

sftp client dscp

Syntax

sftp client dscp *dscp-value*

undo sftp client dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **sftp client dscp** command to set the DSCP value for protocol packets sent by the IPv4 SFTP clients.

Use the **undo sftp client dscp** command to restore the default.

By default, the DSCP value in protocol packets sent by the IPv4 SFTP clients is 16.

Examples

Set the DSCP value to 30 for protocol packets sent by the IPv4 SFTP clients.

```
<Sysname> system-view
[Sysname] sftp client dscp 30
```

sftp client ipv6 dscp

Syntax

sftp client ipv6 dscp *dscp-value*

undo sftp client ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **sftp client ipv6 dscp** command to set the DSCP value for protocol packets sent by the IPv6 SFTP clients.

Use the **undo sftp client ipv6 dscp** command to restore the default.

By default, the DSCP value in protocol packets sent by the IPv6 SFTP clients is 8.

Examples

Set the DSCP value to 30 for protocol packets sent by the IPv6 SFTP clients.

```
<Sysname> system-view
[Sysname] sftp client ipv6 dscp 30
```

snmp-agent packet response dscp

Syntax

snmp-agent packet response dscp *dscp-value*

undo snmp-agent packet response dscp

View

System view

Default level

3: Manage level

Parameters

dscp-value: DSCP value in the SNMP response packets, which ranges from 0 to 63.

Description

Use the **snmp-agent packet response dscp** command to set the DSCP value for SNMP response packets.

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

By default, the DSCP value in SNMP response packets is 0.

Examples

Set the DSCP value to 45 for SNMP response packets.

```
<Sysname> system-view
[Sysname] snmp-agent packet response dscp 45
```

ssh client dscp

Syntax

ssh client dscp *dscp-value*

undo ssh client dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **ssh client dscp** command to set the DSCP value for protocol packets sent by the IPv4 SSH clients.

Use the **undo ssh client dscp** command to restore the default.

By default, the DSCP value in protocol packets sent by the IPv4 SSH clients is 16.

Examples

Set the DSCP value to 30 for protocol packets sent by the IPv4 SSH clients.

```
<Sysname> system-view
[Sysname] ssh client dscp 30
```

ssh client ipv6 dscp

Syntax

ssh client ipv6 dscp *dscp-value*

undo ssh client ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **ssh client ipv6 dscp** command to set the DSCP value for protocol packets sent by the IPv6 SSH clients.

Use the **undo ssh client ipv6 dscp** command to restore the default.

By default, the DSCP value in protocol packets sent by the IPv6 SSH clients is 0.

Examples

Set the DSCP value to 30 for protocol packets sent by the IPv6 SSH clients.

```
<Sysname> system-view
[Sysname] ssh client ipv6 dscp 30
```

ssh server dscp

Syntax

ssh server dscp *dscp-value*

undo ssh server dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **ssh server dscp** command to set the DSCP value for protocol packets sent by the IPv4 SSH servers.

Use the **undo ssh server dscp** command to restore the default.

By default, the DSCP value in protocol packets sent by the IPv4 SSH servers is 16.

Examples

Set the DSCP value to 30 for protocol packets sent by the IPv4 SSH servers.

```
<Sysname> system-view
[Sysname] ssh server dscp 30
```

ssh server ipv6 dscp

Syntax

ssh server ipv6 dscp *dscp-value*

undo ssh server ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **ssh server ipv6 dscp** command to set the DSCP value for protocol packets sent by the IPv6 SSH servers.

Use the **undo ssh server ipv6 dscp** command to restore the default.

By default, the DSCP value in protocol packets sent by the IPv6 SSH servers is 0.

Examples

Set the DSCP value to 30 for protocol packets sent by the IPv6 SSH servers.

```
<Sysname> system-view
[Sysname] ssh server ipv6 dscp 30
```

telnet client dscp

Syntax

telnet client dscp *dscp-value*

undo telnet client dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **telnet client dscp** command to set the DSCP value for protocol packets sent by the Telnet clients.

Use the **undo telnet client dscp** command to restore the default.

By default, the DSCP value in protocol packets sent by the Telnet clients is 16.

Examples

Set the DSCP value to 30 for protocol packets sent by the Telnet clients.

```
<Sysname> system-view
[Sysname] telnet client dscp 30
```

telnet client ipv6 dscp

Syntax

telnet client ipv6 dscp *dscp-value*

undo telnet client ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **telnet client ipv6 dscp** command to set the DSCP value for protocol packets sent by the IPv6 Telnet clients.

Use the **undo telnet client ipv6 dscp** command to restore the default.

By default, the DSCP value in protocol packets sent by the IPv6 Telnet clients is 0.

Examples

Set the DSCP value to 0 for protocol packets sent by the IPv6 Telnet clients.

```
<Sysname> system-view
[Sysname] telnet client ipv6 dscp 30
```

telnet server dscp

Syntax

telnet server dscp *dscp-value*

undo telnet server dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **telnet server dscp** command to set the DSCP value for protocol packets sent by the Telnet servers.

Use the **undo telnet server dscp** command to restore the default.

By default, the DSCP value in protocol packets sent by the Telnet servers is 48.

Examples

Set the DSCP value to 30 for protocol packets sent by the Telnet servers.

```
<Sysname> system-view
[Sysname] telnet server dscp 30
```

telnet server ipv6 dscp

Syntax

telnet server ipv6 dscp *dscp-value*

undo telnet server ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **telnet server ipv6 dscp** command to set the DSCP value for protocol packets sent by the IPv6 Telnet servers.

Use the **undo telnet server ipv6 dscp** command to restore the default.

By default, the DSCP value in protocol packets sent by the IPv6 Telnet servers is 0.

Examples

Set the DSCP value to 30 for protocol packets sent by the IPv6 Telnet servers.

```
<Sysname> system-view
[Sysname] telnet server ipv6 dscp 30
```

tftp client dscp

Syntax

tftp client dscp *dscp-value*

undo tftp client dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **tftp client dscp** command to set the DSCP value for protocol packets sent by the TFTP clients.

Use the **undo tftp client dscp** command to restore the default.

By default, the DSCP value in protocol packets sent by the TFTP clients is 0.

Examples

Set the DSCP value to 30 for protocol packets sent by the TFTP clients.

```
<Sysname> system-view
[Sysname] tftp client dscp 30
```

tftp client ipv6 dscp

Syntax

tftp client ipv6 dscp *dscp-value*

undo tftp client ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **tftp client ipv6 dscp** command to set the DSCP value for protocol packets sent by the IPv6 TFTP clients.

Use the **undo tftp client ipv6 dscp** command to restore the default.

By default, the DSCP value in protocol packets sent by the IPv6 TFTP clients is 0.

Examples

Set the DSCP value to 30 for protocol packets sent by the IPv6 TFTP clients.

```
<Sysname> system-view
[Sysname] tftp client ipv6 dscp 30
```

tos (DHCP operation type view)

Syntax

tos *value*

undo tos

View

DHCP operation type view

Default level

2: System level

Parameters

value: ToS value in the NQA probe packets, which ranges from 0 to 255.

Description

Use the **tos** command to set the ToS value for NQA probe packets.

Use the **undo tos** command to restore the default.

By default, the ToS value in NQA probe packets is 0.

Examples

Set the ToS value to 1 for NQA probe packets.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type dhcp
[Sysname-nqa-admin-test-dhcp] tos 1
```

vrrp dscp

Syntax

vrrp dscp *dscp-value*

undo vrrp dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **vrrp dscp** command to set the DSCP value for IPv4 VRRP protocol packets.

Use the **undo vrrp dscp** command to restore the default.

By default, the DSCP value in IPv4 VRRP protocol packets is 48.

Examples

Set the DSCP value to 30 for IPv4 VRRP protocol packets transmitted.

```
<Sysname> system-view
[Sysname] vrrp dscp 30
```

vrrp ipv6 dscp

Syntax

vrrp ipv6 dscp *dscp-value*

undo vrrp ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use the **vrrp ipv6 dscp** command to set the DSCP value for IPv6 VRRP protocol packets.

Use the **undo vrrp ipv6 dscp** command to restore the default.

By default, the DSCP value in IPv6 VRRP protocol packets is 56.

Examples

Set the DSCP value to 30 for IPv6 VRRP protocol packets transmitted.

```
<Sysname> system-view
[Sysname] vrrp ipv6 dscp 30
```

Modified commands

Modified command: info-center loghost

Old syntax

info-center loghost [**vpn-instance** *vpn-instance-name*] { *host-ipv4-address* **| ipv6** *host-ipv6-address* } [**port** *port-number*] [**channel** { *channel-number* **|** *channel-name* } **| facility** *local-number*] *

New syntax

info-center loghost [**vpn-instance** *vpn-instance-name*] { *host-ipv4-address* **| ipv6** *host-ipv6-address* } [**port** *port-number*] [**dscp** *dscp-value*] [**channel** { *channel-number* **|** *channel-name* } **| facility** *local-number*] *

Views

System view

Change description

The **dscp** *dscp-value* option is added.

dscp *dscp-value*: Sets the DSCP value in the packets sent to the log host, which ranges from 0 to 63 and defaults to 0.

Modified command: ping ipv6

Old syntax

ping ipv6 [**-a** *source-ipv6* **| -c** *count* **| -m** *interval* **| -s** *packet-size* **| -t** *timeout* **| -vpn-instance** *vpn-instance-name*] * *host* [**-i** *interface-type interface-number*]

New Syntax

ping ipv6 [**-a** *source-ipv6* **| -c** *count* **| -m** *interval* **| -s** *packet-size* **| -t** *timeout* **| -vpn-instance** *vpn-instance-name* **| -tos** *tos*] * *host* [**-i** *interface-type interface-number*]

Views

Any view

Change description

The **-tos** *tos* option is added.

-tos *tos*: Sets the Traffic Class field value in the ICMPv6 echo request. The *tos* argument ranges from 0 to 255 and defaults to 0.

Modified command: snmp-agent target-host

Old syntax

snmp-agent target-host trap address udp-domain { *ip-address* **| ipv6** *ipv6-address* } [**udp-port** *port-number*] [**vpn-instance** *vpn-instance-name*] **params securityname** *security-string* [**v1 | v2c | v3** [**authentication | privacy**]]

New Syntax

snmp-agent target-host trap address udp-domain { *ip-address* **| ipv6** *ipv6-address* } [**udp-port** *port-number*] [**dscp** *dscp-value*] [**vpn-instance** *vpn-instance-name*] **params securityname** *security-string* [**v1 | v2c | v3** [**authentication | privacy**]]

Views

System view

Change description

The **dscp** *dscp-value* option is added.

dscp *dscp-value*: Sets the DSCP value for the SNMP traps, which ranges from 0 to 63 and defaults to 0.

Modified command: tracert

Old syntax

tracert [**-a** *source-ip* **| -f** *first-ttl* **| -m** *max-ttl* **| -p** *port* **| -q** *packet-number* **| -vpn-instance** *vpn-instance-name* **| -w** *timeout*] * *host*

New Syntax

tracert [**-a** *source-ip* **| -f** *first-ttl* **| -m** *max-ttl* **| -p** *port* **| -q** *packet-number* **| -vpn-instance** *vpn-instance-name* **| -w** *timeout* **| -tos** *tos*] * *host*

Views

Any view

Change description

The **-tos** *tos* option is added.

-tos *tos*: Sets the ToS field value in the tracert request. The *tos* argument ranges from 0 to 255 and defaults to 0.

Modified command: tracert ipv6

Old syntax

tracert ipv6 [**-f** *first-ttl* **| -m** *max-ttl* **| -p** *port* **| -q** *packet-number* **| -vpn-instance** *vpn-instance-name* **| -w** *timeout*] * *host*

New Syntax

tracert ipv6 [**-f** *first-ttl* **| -m** *max-ttl* **| -p** *port* **| -q** *packet-number* **| -vpn-instance** *vpn-instance-name* **| -w** *timeout* **| -tos** *tos*] * *host*

Views

Any view

Change description

The **-tos** *tos* option is added.

-tos *tos*: Sets the Traffic Class field value in the tracert request. The *tos* argument ranges from 0 to 255 and defaults to 0.

New feature: Portal authentication in IPv6 networks

Configuring portal authentication for an IPv6 network

The following portal authentication features are supported in an IPv6 network:

Tasks at a glance
Specifying an IPv6 portal server for portal authentication
Configuring an IPv6 portal-free rule
Specifying a source IPv6 subnet for portal authentication
Specifying an authentication domain for IPv6 portal users
Specifying a source IPv6 address for outgoing IPv6 portal packets
Logging off an IPv6 portal user

Specifying an IPv6 portal server for portal authentication

To specify an IPv6 portal server for portal authentication:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Specify an IPv6 portal server.	**portal server** *server-name* **ipv6** *ipv6-address* [**key** [**cipher** | **simple**] *key-string* | **port** *port-id* | **url** *url-string*] *	By default, no IPv6 portal server is specified.

Configuring an IPv6 portal-free rule

To configure an IPv6 portal-free rule:

Step	Command
1. Enter system view.	**system-view**
2. Configure an IPv6 portal-free rule.	**portal free-rule** *rule-number* { **destination** { **any** | **ipv6** { *ipv6-address prefix-length* | **any** } } | **source** { **any** | [**interface** *interface-type interface-number* | **ipv6** { *ipv6-address prefix-length* | **any** } | **mac** *mac-address* | **vlan** *vlan-id*] * } } *

Specifying a source IPv6 subnet for portal authentication

To specify a source IPv6 subnet for portal authentication:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. (Optional) Specify a source IPv6 subnet.	**portal auth-network ipv6** *ipv6-network-address prefix-length*	By default, the source IPv6 subnet is ::/0, which means that users from any IPv6 subnet must pass portal authentication to access network resources.

Specifying an authentication domain for IPv6 portal users

To specify an authentication domain for IPv6 portal users:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Specify an authentication domain for IPv6 portal users on the interface.	**portal domain ipv6** *domain-name*	By default, no authentication domain is specified for IPv6 portal users.

Specifying a source IPv6 address for outgoing IPv6 portal packets

To specify a source IPv6 address for outgoing IPv6 portal packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Specify a source IPv6 address for outgoing IPv6 portal packets on the interface.	**portal nas-ip ipv6** *ipv6-address*	By default, no source IPv6 address is specified and the IPv6 address of the user logon interface is used as the source IPv6 address for outgoing IPv6 portal packets.

Logging off an IPv6 portal user

To log off an IPv6 portal user:

Step	Command
1. Enter system view.	**system-view**
2. Log off an IPv6 portal user.	**portal delete-user ipv6** *ipv6-address*

IPv6 portal authentication commands

portal auth-network ipv6

Use the **portal auth-network ipv6** command to configure a source IPv6 subnet for portal authentication on an interface. You can use this command to configure multiple source IPv6 subnets on an interface. Then, only HTTP packets from these IPv6 subnets can trigger portal authentication on the interface. If an unauthenticated user is not on any authentication source IPv6 subnet, the access device discards all the user's HTTP packets that do not match any portal-free rule.

Use the **undo portal auth-network ipv6** command to remove a specific source IPv6 subnet for portal authentication.

Syntax

portal auth-network ipv6 *ipv6-network-address prefix-length*

undo portal auth-network ipv6 *ipv6-network-address*

Default

The source IPv6 subnet for portal authentication is ::/0, meaning that users in all IPv6 subnets must pass portal authentication.

Views

Interface view

Default command level

2: System level

Parameters

ipv6 *ipv6-network-address*: Specifies an authentication source IPv6 subnet address.

prefix-length: IPv6 address prefix length, in the range of 0 to 128.

Examples

Configure a portal authentication source subnet of 2011::1/64 on interface VLAN-interface 2 to allow only users from subnet 2011::1/64 to trigger portal authentication.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname–Vlan-interface2] portal auth-network ipv6 2011::1 64
```

portal delete-user ipv6

Use the **portal delete-user** command to log off an IPv6 portal user.

Syntax

portal delete-user ipv6 *ipv6-address*

Views

System view

Default command level

2: System level

Parameters

ipv6 *ipv6-address*: Logs off the portal user with the specified IPv6 address.

Examples

Log off the portal user whose IPv6 address is 2011::1.

```
<Sysname> system-view
[Sysname] portal delete-user ipv6 2011::1
```

portal domain ipv6

Use the **portal domain ipv6** command to specify an authentication domain for IPv6 portal users on an interface. Then, the switch uses the authentication domain for authentication, authorization and accounting (AAA) of the IPv6 portal users on the interface.

Use the **undo portal domain** command to delete the authentication domain specified for IPv6 portal users.

Syntax

portal domain ipv6 *domain-name*

undo portal domain ipv6

Default

No authentication domain is specified for IPv6 portal users on an interface.

Views

Interface view

Default command level

2: System level

Parameters

ipv6: Specifies IPv6 portal users.

domain-name: Specifies an authentication domain name, a case-insensitive string of 1 to 24 characters. The domain specified by this argument must already exist.

Examples

Configure the authentication domain for IPv6 portal users on VLAN-interface 100 as **my-domain**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] portal domain ipv6 my-domain
```

portal free-rule ipv6

Use the **portal free-rule ipv6** command to configure an IPv6 portal-free rule and specify the source filtering criteria, destination filtering criteria, or both.

Use the **undo portal free-rule** command to remove a specific portal-free rule or all portal-free rules.

Syntax

portal free-rule *rule-number* { **destination** { **any** | **ipv6** { *ipv6-address prefix-length* | **any** } } | **source** { **any** | [**interface** *interface-type interface-number* | **ipv6** { *ipv6-address prefix-length* | **any** } | **mac** *mac-address* | **vlan** *vlan-id*] * } } *

undo portal free-rule { *rule-number* | **all** }

Views

System view

Default command level

2: System level

Parameters

rule-number: Number for the portal-free rule.

any: Imposes no limitation on the previous keyword.

ipv6 *ipv6-address*: Specifies an IPv6 address for the portal-free rule.

prefix-length: Specifies the prefix length of the IPv6 address, in the range of 0 to 128.

interface *interface-type interface-number*: Specifies a source interface.

mac *mac-address*: Specifies a source MAC address in the format H-H-H.

vlan *vlan-id*: Specifies a source VLAN ID.

all: Specifies all portal-free rules.

Usage guidelines

If you specify both a source IPv6 address and a source MAC address in a portal-free rule, the IPv6 address must be a host address with a 128-bit prefix. Otherwise, the specified MAC address does not take effect.

Examples

Configure a portal-free rule, allowing any packet whose source IPv6 address is 2011::1/64 to bypass portal authentication.

```
<Sysname> system-view
[Sysname] portal free-rule 15 source ipv6 2011::1 64 destination ipv6 any
```

portal nas-ip ipv6

Use the **portal nas-ip ipv6** command to configure an interface to use a specific source IPv6 address for outgoing IPv6 portal packets.

Use the **undo portal nas-ip ipv6** command to delete the specified source IPv6 address.

Syntax

portal nas-ip ipv6 *ipv6-address*

undo portal nas-ip ipv6

Default

No source IPv6 address is specified for outgoing IPv6 portal packets on an interface. The switch uses the IP address of the user logon interface as the source IPv6 address for outgoing IPv6 portal packets.

Views

Interface view

Default command level

2: System level

Parameters

ipv6 *ipv6-address*: Specifies a source IPv6 address for outgoing portal packets. This IPv6 address must be a local IPv6 address, but cannot be a multicast address, an all 0 address, or a link-local address.

Examples

Configure interface VLAN-interface 5 to use 2011::2 as the source IPv6 address for outgoing portal packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface 5
[Sysname-Vlan-interface5] portal nas-ip ipv6 2011::2
```

portal server ipv6

Use the **portal server** *server-name* **ipv6** command to configure an IPv6 portal server for portal authentication.

Use the **undo portal server** command to remove an portal server, restore the default destination port and default URL address, or delete the shared key.

Syntax

portal server *server-name* **ipv6** *ipv6-address* [**key** [**cipher** | **simple**] *key-string* **| port** *port-id* **| url** *url-string*] *

undo portal server *server-name* [**key** | **port** | **url**]

Default

No IPv6 portal server is configured for portal authentication.

Views

System view

Default command level

2: System level

Parameters

server-name: Configures a name for the specified portal server, a case-sensitive string of 1 to 32 characters.

ipv6 *ipv6-address*: Specifies a portal server by its IPv6 address.

key: Specifies a shared key for communication with the portal server. Portal packets exchanged between the access device and the portal server carry an authenticator, which is generated with the shared key. The receiver uses the authenticator to check the correctness of the received portal packets.

cipher: Sets a ciphertext shared key.

simple: Sets a plaintext shared key.

key-string: Specifies the shared key. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **simple** nor **cipher** is specified, you set a plaintext shared key.

port *port-id*: Specifies the destination port number used when the device sends an unsolicited message to the portal server, in the range of 1 to 65534. The default is 50100.

url *url-string*: Specifies the uniform resource locator (URL) to which HTTP packets are to be redirected. The default URL is in the http://*ip-address* format, where *ip-address* is the IP address of the portal server. You can also specify the domain name of the portal server, in which case you must use the **portal free-rule** command to configure the IP address of the DNS server as a portal authentication-free destination IP address.

Examples

Configure portal server **pts**, setting the IPv6 address to **2011::1**, the key to plaintext string **portal**, and the redirection URL to **http://2011::1/portal**.

```
<Sysname> system-view
[Sysname] portal server pts ipv6 2011::1 key simple portal url http://[2011::1]portal
```

Modified feature: Password configuration and display

Feature change description

Modified password setup and display for password-related security features.

NOTE:

To improve security, this release saves all plaintext and ciphertext passwords and keys in cipher text in the configuration file.

Command changes

Modified command: area-authentication-mode

Old syntax

area-authentication-mode { **md5** | **simple** } *password* [**ip** | **osi**]

New syntax

area-authentication-mode { **md5** | **simple** } [**cipher**] *password* [**ip** | **osi**]

Views

IS-IS view

Parameters

md5: MD5 authentication mode.

simple: Simple authentication mode.

cipher: Sets a password in cipher text. If this keyword is not specified, set a password in plain text.

password: Password, a case-sensitive string of 1 to 16 characters in plain text, or 33 to 53 characters in cipher text.

ip: Checks IP related fields in LSPs.

osi: Checks OSI related fields in LSPs.

NOTE:

Whether a password should use **ip** or **osi** is not affected by the actual network environment.

Change description

Before modification:

- For MD5 authentication, a ciphertext password must comprise 24 characters.
- For simple authentication, you must set a plaintext password.

After modification:

- For MD5 authentication, a ciphertext password comprises 33 to 53 characters.
- For simple authentication, you can use the **cipher** keyword to set a ciphertext password of 33 to 53 characters.

Modified command: bfd authentication-mode

Old syntax

bfd authentication-mode { **md5** *key-id key* **|** **sha1** *key-id key* **|** **simple** *key-id password* }

New syntax

bfd authentication-mode { **md5** *key-id* [**cipher**] *key* **|** **sha1** *key-id* [**cipher**] *key* **|** **simple** *key-id* [**cipher**] *password* }

View

Interface view

Parameters

md5: Specifies the message digest 5 (MD5) authentication mode.

sha1: Specifies the secure hash algorithm (SHA-1) authentication mode.

simple: Specifies the simple authentication mode.

key-id: Sets the authentication key ID, in the range of 1 to 255.

cipher: Sets a ciphertext authentication key or password. If this keyword is not specified, you set a plaintext authentication key or password.

key: Sets the MD5 or SHA-1 authentication key. This argument is case sensitive. It must be a plaintext string of 1 to 16 characters or a ciphertext string of 33 to 53 characters.

password: Sets the password for simple authentication. This argument is case sensitive. It must be a plaintext string of 1 to 16 characters or a ciphertext string of 33 to 53 characters.

Change description

The **cipher** keyword is added. With **cipher** specified, you can set a ciphertext authentication key or password of 33 to 53 characters for MD5 authentication, SHA-1 authentication, or simple authentication.

Modified command: bims-server

Old syntax

bims-server ip *ip-address* [**port** *port-number*] **sharekey** *key*

New syntax

bims-server ip *ip-address* [**port** *port-number*] **sharekey** [**cipher** **|** **simple**] *key*

View

DHCP address pool view

Parameters

ip *ip-address*: Specifies an IP address for the BIMS server.

port *port-number*: Specifies a port number for the BIMS server in the range of 1 to 65534.

cipher: Sets a ciphertext key.

simple: Sets a plaintext key.

key: Specifies the key string. This argument is case sensitive. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If **simple** is specified, it must be a string of 1 to 16 characters. If neither **simple** nor **cipher** is specified, you set a plaintext key.

Change description

Before modification: You can set only a plaintext shared key.

After modification: You can set a plaintext or a ciphertext shared key. A ciphertext shared key can comprise 53 characters at most.

Modified command: certificate request mode

Syntax

certificate request mode { **auto** [**key-length** *key-length* **| password** { **cipher | simple** } *password*] * **| manual** }

Views

PKI domain view

Parameters

auto: Requests a certificate in auto mode.

key-length: Length of the RSA keys in bits, in the range of 512 to 2048. It is 1024 bits by default.

cipher: Sets a ciphertext password for certificate revocation.

simple: Sets a plaintext password for certificate revocation.

password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 31 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 73 characters.

manual: Requests a certificate in manual mode.

Change description

Before modification: A ciphertext password comprises 31 characters at most.

After modification: A ciphertext password comprises 73 characters at most.

Modified command: cluster-local-user

Syntax

cluster-local-user *user-name* [**password** { **cipher | simple** } *password*]

Views

Cluster view

Parameters

user-name: Specifies the username for logging onto the cluster member devices through Web. It is a string of 1 to 55 characters.

password: Specifies the password for logging onto the cluster member devices through Web. If this keyword is not specified, you can log in without a password.

cipher: Specifies a ciphertext password.

simple: Specifies a plaintext password.

password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 63 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 117 characters.

Change description

Before modification:

- **cipher**: Sets a plaintext or ciphertext password. The password will be saved in cipher text in the configuration file.

- **cipher** *password*: Specifies the password string, which can be a plaintext string of 1 to 63 characters, or a 24-character or 88-character ciphertext string.

After modification:

- **cipher**: Sets a ciphertext password.
- **cipher** *password*: Specifies a ciphertext password of 1 to 117 characters.

Modified command: cluster-snmp-agent usm-user v3

Old syntax

cluster-snmp-agent usm-user v3 *user-name group-name* [**authentication-mode** { **md5 | sha** } *auth-password* [**privacy-mode des56** *priv-password*]]

New syntax

cluster-snmp-agent usm-user v3 *user-name group-name* [**authentication-mode** { **md5 | sha** } [**cipher | simple**] *auth-password* [**privacy-mode des56** [**cipher | simple**] *priv-password*]]

Views

Cluster view

Parameters

user-name: User name, a string of 1 to 32 characters.

group-name: Group name, a string of 1 to 32 characters.

authentication-mode: Specifies the security level to be authentication needed.

md5: Specifies the authentication protocol to be HMAC-MD5-96.

sha: Specifies the authentication protocol to be HMAC-SHA-96.

cipher*:* Specifies a ciphertext password.

simple*:* Specifies a plaintext password.

auth-password: Specifies the authentication password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **cipher** nor **simple** is specified, you set a plaintext string.

privacy-mode: Specifies the security level to be encrypted.

des56: Specifies the encryption protocol to be DES (data encryption standard).

priv-password: Specifies the privacy password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **cipher** nor **simple** is specified, you set a plaintext string.

Change description

Before modification:

- **cipher** and **simple** keywords are not supported. You can directly enter a plaintext or a ciphertext password.
- The authentication password (*auth-password*) and the privacy password (*priv-password*) can be a plaintext string of 1 to 16 characters, or a 24-character ciphertext string.

After modification:

- You can use the **cipher** keyword to set a ciphertext password or use the **simple** keyword to set a plaintext password. If neither **cipher** nor **simple** is specified, you set a plaintext password.
- A plaintext password comprises 1 to 16 characters. A ciphertext password comprises 1 to 53 characters.

Modified command: cwmp acs password

Old syntax

cwmp acs password *password*

New syntax

cwmp acs password [**cipher** | **simple**] *password*

View

CWMP view

Parameters

cipher*:* Specifies a ciphertext password.

simple*:* Specifies a plaintext password.

password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 255 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 373 characters. If neither **cipher** nor **simple** is specified, you set a plaintext password string.

Change description

Before modification: You cannot specify the password type (plaintext or ciphertext).

After modification: You can set a plaintext password or a ciphertext password. A ciphertext password comprises 1 to 373 characters.

Modified command: cwmp cpe password

Old syntax

cwmp cpe password *passowrd*

New syntax

cwmp cpe password [**cipher** | **simple**] *passowrd*

View

CWMP view

Parameters

cipher*:* Specifies a ciphertext password.

simple*:* Specifies a plaintext password.

password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 255 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 373 characters. If neither **cipher** nor **simple** is specified, you set a plaintext password string.

Change description

Before modification: You cannot specify the password type (plaintext or ciphertext).

After modification: You can set a plaintext password or a ciphertext password. A ciphertext password comprises 1 to 373 characters.

Modified command: dldp authentication-mode

Old syntax

dldp authentication-mode { **md5** *md5-password* **| none | simple** *simple-password* }

New syntax

dldp authentication-mode { **none |** { **md5 | simple** } *password* }

View

System view

Parameters

none: Specifies not to perform authentication.

md5: Specifies to perform MD5 authentication and sets the password in plain text or cipher text.

simple: Specifies to perform simple authentication and sets the password in plain text or cipher text.

password: Plain text password, a case-sensitive string of 1 to 16 characters; or a cipher text password, a case-sensitive string of 33 to 53 characters.

Change description

Before modification: You can set only a plaintext password for simple authentication, and a plaintext password or a 24-character ciphertext password for MD5 authentication.

After modification: You can set a plaintext password or a ciphertext password for both simple authentication and MD5 authentication. A ciphertext password comprises 33 to 53 characters.

Modified command: domain-authentication-mode

Old syntax

domain-authentication-mode { **md5 | simple** } *password* [**ip | osi**]

New syntax

domain-authentication-mode { **md5 | simple** } [**cipher**] *password* [**ip | osi**]

Views

IS-IS view

Parameters

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

cipher: Sets a password in cipher text. If this keyword is not specified, set a password in plain text.

password: Password, a case-sensitive string of 1 to 16 characters in plain text, or 33 to 53 characters in cipher text.

ip: Checks IP related fields in LSPs.

osi: Checks OSI related fields in LSPs.

> **NOTE:**
> Whether a password should use **ip** or **osi** is not affected by the actual network environment.

Change description

Before modification:

- For MD5 authentication, a ciphertext password must comprise 24 characters.
- For simple authentication, you must set a plaintext password.

After modification:

- For MD5 authentication, a ciphertext password comprises 33 to 53 characters.

- For simple authentication, you can use the **cipher** keyword to set a ciphertext password of 33 to 53 characters.

Modified command: ftp-server

Syntax

ftp-server *ip-address* [**user-name** *username* **password** { **cipher | simple** } *password*]

Views

Cluster view

Parameters

ip-address: Specifies the IP address of the FTP server.

username: Specifies the username for logging onto the FTP server, a string of 1 to 32 characters.

cipher: Specifies a ciphertext password.

simple: Specifies a plaintext password.

password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters.

Change description

Before modification:

- **cipher**: Sets a plaintext or ciphertext password. The password will be saved in cipher text in the configuration file.
- **cipher** *password*: Specifies the password string, which can be a plaintext string of 1 to 16 characters, or a 24-character ciphertext string.

After modification:

- **cipher**: Sets a ciphertext password.
- **cipher** *password*: Specifies a ciphertext password of 1 to 53 characters.

Modified command: isis authentication-mode

Old syntax

isis authentication-mode { **md5 | simple** } *password* [**level-1 | level-2**] [**ip | osi**]

New syntax

isis authentication-mode { **md5 | simple** } [**cipher**] *password* [**level-1 | level-2**] [**ip | osi**]

Views

Interface view

Parameters

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

cipher: Sets a password in cipher text. If this keyword is not specified, set a password in plain text.

password: Password, a case-sensitive string of 1 to 16 characters in plain text, or 33 to 53 characters in cipher text.

level-1: Configures the password for Level-1.

level-2: Configures the password for Level-2.

ip: Checks IP related fields in LSPs and SNPs.

osi: Checks OSI related fields in LSPs and SNPs.

> **NOTE:**
> Whether a password should use **ip** or **osi** is not affected by the actual network environment.

Change description

Before modification:

- For MD5 authentication, a ciphertext password must comprise 24 characters.
- For simple authentication, you must set a plaintext password.

After modification:

- For MD5 authentication, a ciphertext password comprises 33 to 53 characters.
- For simple authentication, you can use the **cipher** keyword to set a ciphertext password of 33 to 53 characters.

Modified command: key (HWTACACS scheme view)

Syntax

key { **accounting** | **authentication** | **authorization** } [**cipher** | **simple**] *key*

Views

HWTACACS scheme view

Parameters

accounting: Sets the shared key for secure HWTACACS accounting communication.

authentication: Sets the shared key for secure HWTACACS authentication communication.

authorization: Sets the shared key for secure HWTACACS authorization communication.

cipher: Sets a ciphertext shared key.

simple: Sets a plaintext shared key.

key: Specifies the shared key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 255 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 373 characters. If neither **cipher** nor **simple** is specified, you set a plaintext shared key string.

Change description

Before modification: A ciphertext password comprises 352 characters at most.

After modification: A ciphertext password comprises 373 characters at most.

Modified command: key (RADIUS scheme view)

Syntax

key { **accounting** | **authentication** } [**cipher** | **simple**] *key*

Views

RADIUS scheme view

Parameters

accounting: Sets the shared key for secure RADIUS accounting communication.

authentication: Sets the shared key for secure RADIUS authentication/authorization communication.

cipher: Sets a ciphertext shared key.

simple: Sets a plaintext shared key.

key: Specifies the shared key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 64 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 117 characters. If neither **cipher** nor **simple** is specified, you set a plaintext shared key string.

Change description

Before modification: A ciphertext shared key must be of 12, 24, 32, 44, 64, 76, 88, or 96 characters.

After modification: A ciphertext shared key comprises 117 characters at most.

Modified command: mac-authentication user-name-format

Syntax

mac-authentication user-name-format { **fixed** [**account** *name*] [**password** { **cipher | simple** } *password*] **| mac-address** [{ **with-hyphen | without-hyphen** } [**lowercase | uppercase**]] }

Views

System view

Parameters

fixed: Uses a shared account for all MAC authentication users.

account *name*: Specifies the username for the shared account. The name takes a case-insensitive string of 1 to 55 characters. If no username is specified, the default name **mac** applies.

password: Specifies the password for the shared user account:

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Specifies the password. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 63 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 117 characters.

mac-address: Uses MAC-based user accounts for MAC authentication users. If this option is specified, you must create one user account for each user, and use the MAC address of the user as both the username and password for the account. You can also specify the format of username and password:

- **with-hyphen**—Hyphenates the MAC address, for example xx-xx-xx-xx-xx-xx.
- **without-hyphen**—Excludes hyphens from the MAC address, for example, xxxxxxxxxxxx.
- **lowercase**—Enters letters in lower case.
- **uppercase**—Capitalizes letters.

Change description

Before modification: If **cipher** is specified, you can enter 1 to 63 characters in plain text, or 24 or 88 characters in cipher text, for the password. If you enter no more than 16 characters in plain text, the string is encrypted into a 24-character password. If you enter 16 to 63 characters in plain text, the string is encrypted into an 88-character password. The system treats a 24-character password as a ciphertext password, if it can decrypt the password. If not, the system treats the password as a plaintext password.

After modification: A ciphertext password comprises 117 characters at most.

Modified command: ntp-service authentication-keyid

Old syntax

ntp-service authentication-keyid *keyid* **authentication-mode md5** *value*

New syntax

ntp-service authentication-keyid *keyid* **authentication-mode md5** [**cipher | simple**] *value*

Views

System view

Parameters

keyid: Authentication key ID, which is in the range of 1 to 4294967295.

cipher: Sets a ciphertext key.

simple: Sets a plaintext key. This key will be saved in cipher text for secrecy.

value: Specifies the MD5 authentication key string. This argument is case sensitive. If **simple** is specified, it is a string of 1 to 32 characters. If **cipher** is specified, it is a string of 1 to 73 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string.

Change description

Before modification: You cannot specify the key type (plaintext or ciphertext).

After modification: You can set a plaintext or ciphertext key. A ciphertext key string comprises 1 to 73 characters.

Modified command: ospf authentication-mode

syntax

For MD5/HMAC-MD5 authentication:

ospf authentication-mode { **hmac-md5 | md5** } *key-id* [**cipher | plain**] *password*

For simple authentication:

ospf authentication-mode simple [**cipher | plain**] *password*

Views

Interface view

Parameters

hmac-md5: HMAC-MD5 authentication.

md5: MD5 authentication.

simple: Simple authentication.

key-id: Authentication key ID, in the range of 1 to 255.

cipher: Specifies a ciphertext password.

plain: Specifies a plaintext password.

If no **cipher** or **plain** is specified, the default password type for MD5/HMAC-MD5 authentication mode is **cipher**, and the default password type for simple authentication mode is **plain**.

password: Password.

- In simple authentication mode, a plaintext password is a case-sensitive string of 1 to 8 characters, and a ciphertext password is a case-sensitive string of 1 to 41 characters.

- In MD5/HMAC-MD5 authentication mode, a plaintext password is a case-sensitive string of 1 to 16 characters, and a ciphertext password is a case-sensitive string of 1 to 53 characters.

Change description

Before modification: If **cipher** is specified, you can enter a plaintext password or a 24-character ciphertext password.

After modification: If **cipher** is specified, you must enter a ciphertext password. For simple authentication, it must be a ciphertext string of 1 to 41 characters. For MD5/HMAC-MD5 authentication, it must be a ciphertext string of 1 to 53 characters.

Modified command: password (FTP operation type view)

Old syntax

password *password*

New syntax

password [**cipher** | **simple**] *password*

Views

FTP operation type view

Parameters

cipher: Sets a password in cipher text.

simple: Sets a password in plain text.

password: Specifies the password used to log in to the FTP server, a case-sensitive string of 1 to 32 characters in plain text, or 1 to 73 characters in cipher text. If the **cipher** or **simple** keyword is not specified, the password is in plain text.

Change description

Before modification: You cannot specify the password type (plaintext or ciphertext).

After modification: You can set a plaintext password or a ciphertext password. A ciphertext password comprises 1 to 73 characters.

Modified command: password (local user view)

Syntax

password [{ **cipher** | **simple** } *password*]

Views

Local user view

Parameters

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 63 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 117 characters. If neither **cipher** nor **simple** is specified, you set a plaintext password string in interactive mode.

Change description

Before modification: If **cipher** is specified, you can set a plaintext password, or a 24-character or 88-character ciphertext password. The system treats a 24-character password as a ciphertext password, if it can decrypt the password. If not, the system treats the password as a plaintext password.

After modification: A ciphertext password comprises 117 characters at most.

Modified command: password (RADIUS-server user view)

Syntax

password [**cipher** | **simple**] *password*

Views

RADIUS-server user view

Parameters

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 128 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 201 characters. If neither **cipher** nor **simple** is specified, you set a plaintext password string.

Change description

Before modification: A ciphertext password must be of 12, 24, 32, 44, 64, 76, 88, 96, 108, 120, 128, 140, 152, 160, 172, or 184 characters.

After modification: A ciphertext password comprises 201 characters at most.

Modified command: peer password (BGP view, BGP-VPN instance view)

Syntax

peer { *group-name* **|** *ipv6-address* } **password** { **cipher** **|** **simple** } *password*

Views

BGP view, BGP-VPN instance view

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Specifies the password string.

- If **simple** is specified, a plaintext password is a case-sensitive string of 1 to 80 characters.
- If **cipher** is specified, a plaintext password is a case-sensitive string of 1 to 80 characters, and a ciphertext password is a case-sensitive string of 33 to 137 characters.

Change description

Before modification: If **cipher** is specified, you can set a 24-character or 108-character ciphertext password.

After modification: A ciphertext password comprises 33 to 137 characters.

Modified command: peer password (IPv6 address family view)

Syntax

peer { *group-name* **|** *ipv6-address* } **password** { **cipher | simple** } *password*

Views

IPv6 address family view

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Specifies the password string.

- If **simple** is specified, a plaintext password is a case-sensitive string of 1 to 80 characters.
- If **cipher** is specified, a plaintext password is a case-sensitive string of 1 to 80 characters, and a ciphertext password is a case-sensitive string of 33 to 137 characters.

Change description

Before modification: If **cipher** is specified, you can set a 24-character or 88-character ciphertext password.

After modification: A ciphertext password comprises 33 to 137 characters.

Modified command: peer password (MSDP view)

Syntax

peer *peer-address* **password** { **cipher | simple** } *password*

Views

Public network MSDP view, VPN instance MSDP view

Parameters

peer-address: Specifies an MSDP peer.

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Specifies the password string.

- If **simple** is specified, a plaintext password is a case-sensitive string of 1 to 80 characters.
- If **cipher** is specified, a plaintext password is a case-sensitive string of 1 to 80 characters, and a ciphertext password is a case-sensitive string of 33 to 137 characters.

Change description

Before modification: If **cipher** is specified, you can set a 24-character or 88-character ciphertext password.

After modification: A ciphertext password comprises 33 to 137 characters.

Modified command: portal server

Old syntax

portal server *server-name* **ip** *ip-address* [**key** *key-string* **| port** *port-id* **| url** *url-string* **| vpn-instance** *vpn-instance-name*] *

New syntax

portal server *server-name* **ip** *ip-address* [**key** [**cipher | simple**] *key-string* **| port** *port-id* **| url** *url-string* **| vpn-instance** *vpn-instance-name*] *

Views

System view

Parameters

server-name: Specifies the name of a portal server, a case-sensitive string of 1 to 32 characters.

ip *ip-address*: Specifies the IPv4 address of a portal server.

key: Specifies a shared key for communication with the portal server. Portal packets exchanged between the access device and the portal server carry an authenticator, which is generated with the shared key. The receiver uses the authenticator to check the correctness of the received portal packets.

cipher: Sets a ciphertext shared key.

simple: Sets a plaintext shared key.

key-string: Specifies the shared key. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **simple** nor **cipher** is specified, you set a plaintext shared key.

port *port-id*: Specifies the destination port number used when the device sends an unsolicited message to the portal server, in the range of 1 to 65534. The default is 50100.

url *url-string*: Specifies the uniform resource locator (URL) to which HTTP packets are to be redirected. The default URL is in the http://*ip-address* format, where *ip-address* is the IP address of the portal server. You can also specify the domain name of the portal server, in which case you must use the **portal free-rule** command to configure the IP address of the DNS server as a portal authentication-free destination IP address.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN to which the portal server belongs. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If the portal server is on the public network, do not specify this option.

Change description

Before modification: You can set only a plaintext shared key.

After modification: You can set a plaintext or a ciphertext shared key. A ciphertext shared key can comprise 53 characters at most.

Modified command: primary accounting (RADIUS scheme view)

Syntax

primary accounting { *ipv4-address* **| ipv6** *ipv6-address* } [*port-number* **| key** [**cipher | simple**] *key* **| vpn-instance** *vpn-instance-name*] *

Views

RADIUS scheme view

Parameters

ipv4-address: Specifies the IPv4 address of the primary RADIUS accounting server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the primary RADIUS accounting server, which must be a valid global unicast address.

port-number: Specifies the service port number of the primary RADIUS accounting server, which is a UDP port number in the range 1 to 65535 and defaults to 1813.

key [**cipher** | **simple**] *key*: Specifies the shared key for secure communication with the primary RADIUS accounting server.

- **cipher** *key*: Specifies a ciphertext shared key, which is a case-sensitive ciphertext string of 1 to 117 characters.
- [**simple**] *key*: Specifies a plaintext shared key, which is a case-sensitive string of 1 to 64 characters.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN that the primary RADIUS accounting server belongs to, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

Change description

Before modification: A ciphertext shared key must be of 12, 24, 32, 44, 64, 76, 88, or 96 characters.

After modification: A ciphertext shared key comprises 117 characters at most.

Modified command: primary authentication (RADIUS scheme view)

Syntax

primary authentication { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** [**cipher** | **simple**] *key* | **vpn-instance** *vpn-instance-name*] *

Views

RADIUS scheme view

Parameters

ipv4-address: Specifies the IPv4 address of the primary RADIUS authentication/authorization server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the primary RADIUS authentication/authorization server, which must be a valid global unicast address.

port-number: Specifies the service port number of the primary RADIUS authentication/authorization server, which is a UDP port number in the range 1 to 65535 and defaults to 1812.

key [**cipher** | **simple**] *key*: Specifies the shared key for secure communication with the primary RADIUS authentication/authorization server.

- **cipher** *key*: Specifies a ciphertext shared key, which is a case-sensitive ciphertext string of 1 to 117 characters.
- [**simple**] *key*: Specifies a plaintext shared key, which is a case-sensitive string of 1 to 64 characters.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN that the primary RADIUS authentication/authorization server belongs to, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

Change description

Before modification: A ciphertext shared key must be of 12, 24, 32, 44, 64, 76, 88, or 96 characters.

After modification: A ciphertext shared key comprises 117 characters at most.

Modified command: radius-server client-ip

Old syntax

radius-server client-ip *ip-address* [**key** *string*]

New syntax

radius-server client-ip *ip-address* [**key** [**cipher | simple**] *string*]

Views

System view

Parameters

ip-address: Specifies the IPv4 address of the RADIUS client.

key: Sets the shared key for secure communication with the RADIUS client.

cipher: Sets a ciphertext shared key.

simple: Sets a plaintext shared key.

string: Specifies the shared key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 64 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 117 characters. If neither **cipher** nor **simple** is specified, you set a plaintext shared key string.

all: Specifies all RADIUS clients.

Change description

Before modification: You can set only a plaintext shared key.

After modification: You can set a plaintext or a ciphertext shared key. A ciphertext shared key comprises 117 characters at most.

Modified command: rip authentication-mode

Old syntax

rip authentication-mode { **md5** { **rfc2082** *key-string key-id* **|** **rfc2453** *key-string* } **| simple** *password* }

New syntax

rip authentication-mode { **md5** { **rfc2082** [**cipher**] *key-string key-id* **|** **rfc2453** [**cipher**] *key-string* } **| simple** [**cipher**] *password* }

Views

Interface view

Parameters

md5: Specifies the MD5 authentication mode.

rfc2082: Uses the message format defined in RFC 2082.

cipher: Sets an authentication key or password in cipher text. If this keyword is not specified, set an authentication key or password in plain text.

key-string: MD5 key, a case-sensitive string of 1 to 16 characters in plain text, or 33 to 53 characters in cipher text.

key-id: MD5 key number, in the range of 1 to 255.

rfc2453: Uses the message format defined in RFC 2453 (IETF standard).

simple: Specifies the simple authentication mode.

password: Password in simple authentication mode, a case-sensitive string of 1 to 16 characters in plain text, or 33 to 53 characters in cipher text.

Change description

Before modification:

- For MD5 authentication, a ciphertext password comprises 1 to 24 characters.
- For simple authentication, you must set a plaintext password.

After modification:

- For MD5 authentication, a ciphertext password comprises 33 to 53 characters.
- For simple authentication, you can use the **cipher** keyword to set a ciphertext password of 33 to 53 characters.

Modified command: sa authentication-hex

Old syntax

sa authentication-hex { **inbound** | **outbound** } { **ah** | **esp** } *hex-key*

New syntax

sa authentication-hex { **inbound** | **outbound** } { **ah** | **esp** } [**cipher** | **simple**] *hex-key*

Views

IPsec policy view

Parameters

inbound: Specifies the inbound SA through which IPsec processes the received packets.

outbound: Specifies the outbound SA through which IPsec processes the packets to be sent.

ah: Uses AH.

esp: Uses ESP.

cipher: Sets a ciphertext authentication key.

simple: Sets a plaintext authentication key.

hex-key: Specifies the key string. If **cipher** is specified, this argument is case sensitive and must be a ciphertext string of 1 to 117 characters. If **simple** is specified, this argument is case insensitive, and must be a 16-byte hexadecimal string for MD5, a 20-byte hexadecimal string for SHA1, 32-byte hexadecimal string for SHA2, or a 16-byte hexadecimal string for AES-XBC-MAC. If neither **cipher** nor **simple** is specified, you set a plaintext authentication key string.

Change description

Before modification: You can set only a plaintext authentication key.

After modification: You can set a plaintext or a ciphertext authentication key. A ciphertext authentication key comprises 117 characters at most.

Modified command: sa encryption-hex

Old syntax

sa encryption-hex { **inbound** | **outbound** } **esp** *hex-key*

New syntax

sa encryption-hex { **inbound** | **outbound** } **esp** [**cipher** | **simple**] *hex-key*

Views

IPsec policy view

Parameters

inbound: Specifies the inbound SA through which IPsec processes the received packets.

outbound: Specifies the outbound SA through which IPsec processes the packets to be sent.

esp: Uses ESP.

cipher: Sets a ciphertext encryption key.

simple: Sets a plaintext encryption key.

hex-key: Specifies the key string. If **cipher** is specified, this argument is case sensitive and must be a ciphertext string of 1 to 117 characters. If **simple** is specified, this argument is case insensitive, and must be an 8-byte hexadecimal string for DES-CBC, a 16-byte hexadecimal string for AES128-CBC and camellia128-CBC, a 20-byte hexadecimal string for AESCTR-128, a 24-byte hexadecimal string for 3DES-CBC, AES192-CBC, and camellia192-CBC, or a 32-byte hexadecimal string for camellia256-CBC. If neither **cipher** nor **simple** is specified, you set a plaintext authentication key string.

Change description

Before modification: You can set only a plaintext encryption key.

After modification: You can set a plaintext or a ciphertext encryption key. A ciphertext encryption key comprises 117 characters at most.

Modified command: sa string-key

Old syntax

sa string-key { **inbound** | **outbound** } { **ah** | **esp** } *string-key*

New syntax

sa string-key { **inbound** | **outbound** } { **ah** | **esp** } [**cipher** | **simple**] *string-key*

Views

IPsec policy view

Parameters

inbound: Specifies the inbound SA through which IPsec processes the received packets.

outbound: Specifies the outbound SA through which IPsec processes the packets to be sent.

ah: Uses AH.

esp: Uses ESP.

cipher: Sets a ciphertext key.

simple: Sets a plaintext key.

string-key: Specifies the key string. This argument is case sensitive. If **cipher** is specified, it must be a ciphertext string of 1 to 373 characters. If **simple** is specified, it must be a string of 1 to 255 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string. For different algorithms, enter strings of any length in the specified range. Using this key string, the system automatically generates keys meeting the algorithm requirements. When the protocol is ESP, the system generates the keys for the authentication algorithm and encryption algorithm respectively.

Change description

Before modification: You can set only a plaintext key.

After modification: You can set a plaintext or a ciphertext key. A ciphertext key comprises 373 characters at most.

Modified command: secondary accounting (RADIUS scheme view)

Syntax

secondary accounting { *ipv4-address* **| ipv6** *ipv6-address* } [*port-number* **| key** [**cipher | simple**] *key* **| vpn-instance** *vpn-instance-name*] *

Views

RADIUS scheme view

Parameters

ipv4-address: Specifies the IPv4 address of the secondary RADIUS accounting server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the secondary RADIUS accounting server, which must be a valid global unicast address.

port-number: Specifies the service port number of the secondary RADIUS accounting server, which is a UDP port number in the range 1 to 65535 and defaults to 1813.

key [**cipher | simple**] *key*: Specifies the shared key for secure communication with the secondary RADIUS accounting server.

- **cipher** *key*: Specifies a ciphertext shared key, which is a case-sensitive ciphertext string of 1 to 117 characters.
- [**simple**] *key*: Specifies a plaintext shared key, which is a case-sensitive string of 1 to 64 characters.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN that the secondary RADIUS accounting server belongs to, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

Change description

Before modification: A ciphertext shared key must be of 12, 24, 32, 44, 64, 76, 88, or 96 characters.

After modification: A ciphertext shared key comprises 117 characters at most.

Modified command: secondary authentication (RADIUS scheme view)

Syntax

secondary authentication { *ipv4-address* **| ipv6** *ipv6-address* } [*port-number* **| key** [**cipher | simple**] *key* **| vpn-instance** *vpn-instance-name*] *

Views

RADIUS scheme view

Parameters

ipv4-address: Specifies the IPv4 address of the secondary RADIUS authentication/authorization server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the secondary RADIUS authentication/authorization server, which is a valid global unicast address.

port-number: Specifies the service port number of the secondary RADIUS authentication/authorization server, which is a UDP port number in the range 1 to 65535 and defaults to 1812.

key [**cipher | simple**] *key*: Specifies the shared key for secure communication with the secondary RADIUS authentication/authorization server.

- **cipher** *key*: Specifies a ciphertext shared key, which is a case-sensitive ciphertext string of 1 to 117 characters.
- [**simple**] *key*: Specifies a plaintext shared key, which is a case-sensitive string of 1 to 64 characters.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN that the secondary RADIUS authentication/authorization server belongs to, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

Change description

Before modification: A ciphertext shared key must be of 12, 24, 32, 44, 64, 76, 88, or 96 characters.

After modification: A ciphertext shared key comprises 117 characters at most.

Modified command: set authentication password

Syntax

set authentication password { **cipher** | **simple** } *password*

Views

User interface view

Parameters

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters.

Change description

Before modification:

- **cipher** *password*: Sets a plaintext password or a 24-character ciphertext password. This password will be displayed in cipher text.
- **simple** *password*: Sets a plaintext password. This password will be displayed in plain text.

After modification:

- **cipher** *password*: Sets a ciphertext password. This password must be a ciphertext string of 1 to 53 characters.
- **simple** *password*: Sets a plaintext password.

Modified command: snmp-agent usm-user v3

Syntax

snmp-agent usm-user v3 *user-name group-name* [**cipher**] [**authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **des56** } *priv-password*]] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *

Views

System view

Parameters

user-name: User name, a case-sensitive string of 1 to 32 characters.

group-name: Group name, a case-sensitive string of 1 to 32 characters.

cipher: Specifies that *auth-password* and *priv-password* are encrypted keys, which can be calculated to a hexadecimal string by using the **snmp-agent calculate-password** command. If this keyword is not specified, *auth-password* and *priv-password* are plaintext keys.

authentication-mode: Specifies an authentication algorithm. MD5 is faster but less secure than SHA.

- **md5**: Specifies the MD5 authentication algorithm.
- **sha**: Specifies the SHA-1 authentication algorithm.

auth-password: Specifies a case-sensitive plaintext or encrypted authentication key. A plaintext key is a string of 1 to 64 characters. If the **cipher** is specified, the encrypted authentication key length requirements differ by authentication algorithm and key string format, as shown in Table 1.

Table 1 Encrypted authentication key length requirements

Authentication algorithm	Hexadecimal string	Non-hexadecimal string
MD5	32 characters	53 characters
SHA	40 characters	57 characters

privacy-mode: Specifies an encryption algorithm for privacy. The three encryption algorithms AES, 3DES, and DES are in descending order of security. Higher security means more complex implementation mechanism and lower speed. DES is enough to meet general requirements.

- **3des**: Specifies the 3DES algorithm.
- **des56**: Specifies the DES algorithm.
- **aes128**: Specifies the AES algorithm.

priv-password: Specifies a case-sensitive plaintext or encrypted privacy key. A plaintext key is a string of 1 to 64 characters. If the **cipher** keyword is specified, the encrypted privacy key length requirements differ by authentication algorithm and key string format, as shown in Table 2.

Table 2 Encrypted privacy key length requirements

Authentication algorithm	Encryption algorithm	Hexadecimal string	Non-hexadecimal string
MD5	3DES	64 characters	73 characters
MD5	AES128 or DES-56	32 characters	53 characters
SHA	3DES	80 characters	73 characters
SHA	AES128 or DES-56	40 characters	53 characters

acl *acl-number*: Specifies a basic ACL to filter NMSs by source IPv4 address. The *acl-number* argument represents a basic ACL number in the range of 2000 to 2999. Only the NMSs with the IPv4 addresses permitted in the ACL can use the specified username to access the SNMP agent.

acl ipv6 *ipv6-acl-number*: Specifies a basic ACL to filter NMSs by source IPv6 address. The *ipv6-acl-number* argument represents a basic ACL number in the range of 2000 to 2999. Only the NMSs with the IPv6 addresses permitted in the ACL can use the specified username to access the SNMP agent.

local: Represents a local SNMP entity user.

engineid *engineid-string*: Specifies an SNMP engine ID as a hexadecimal string. The *engineid-string* argument must comprise an even number of hexadecimal characters, in the range of 10 to 64. All-zero and all-F strings are invalid.

Change description

Before modification:

- If the **cipher** and **md5** keywords are specified, the MD5 key is a hexadecimal string of 32 characters, the 3DES key is a hexadecimal string of 64 characters, and the AES128 or DES56 key is a hexadecimal string of 32 characters.
- If the **cipher** and **sha** keywords are specified, the SHA-1 key is a hexadecimal string of 40 characters, the 3DES key is a hexadecimal string of 80 characters, and the AES128 or DES56 key is a hexadecimal string of 40 characters.

After modification:

- See Table 1 for the encrypted authentication key length requirements.
- See Table 2 for the encrypted privacy key length requirements.

Modified command: super password

Syntax

super password [**level** *user-level*] { **cipher** | **simple** } *password*

Views

System view

Parameters

level *user-level*: User privilege level, which ranges from 1 to 3 and defaults to 3.

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters.

Change description

Before modification:

- **cipher** *password*: Sets a plaintext password or a 24-character ciphertext password. This password will be displayed in cipher text.
- **simple** *password*: Sets a plaintext password. This password will be displayed in plain text.

After modification:

- **cipher** *password*: Sets a ciphertext password. This password must be a ciphertext string of 1 to 53 characters.
- **simple** *password*: Sets a plaintext password.

Modified command: vlink-peer

syntax

vlink-peer *router-id* [**hello** *seconds* | **retransmit** *seconds* | **trans-delay** *seconds* | **dead** *seconds* | **simple** [**plain** | **cipher**] *password* | { **md5** | **hmac-md5** } *key-id* [**plain** | **cipher**] *password*] *

Views

OSPF area view

Parameters

router-id: Router ID of the neighbor on the virtual link.

hello *seconds*: Hello interval in seconds, in the range of 1 to 8192. The default is 10. It must be identical to the hello interval on the virtual link neighbor.

retransmit *seconds*: Retransmission interval in seconds, in the range of 1 to 3600. The default is 5.

trans-delay *seconds*: Transmission delay interval in seconds, in the range of 1 to 3600. The default is 1.

dead *seconds*: Dead interval in seconds, in the range of 1 to 32768. The default is 40. It must be identical to that on the virtual link neighbor. The dead interval is at least four times the hello interval.

md5: MD5 authentication.

hmac-md5: HMAC-MD5 authentication.

simple: Simple authentication.

key-id: Key ID for MD5 or HMAC-MD5 authentication, in the range of 1 to 255.

cipher: Specifies a ciphertext password.

plain: Specifies a plaintext password.

password: Password. In simple authentication mode, a plaintext password is a case-sensitive string of 1 to 8 characters, and a ciphertext password is a case-sensitive string of 1 to 41 characters. In MD5/HMAC-MD5 authentication mode, a plaintext password is a case-sensitive string of 1 to 16 characters, and a ciphertext password is a case-sensitive string of 1 to 53 characters.

Change description

Before modification: If **cipher** is specified, you can enter a plaintext password or a 24-character ciphertext password.

After modification: If **cipher** is specified, you must enter a ciphertext password. For simple authentication, it must be a ciphertext string of 1 to 41 characters. For MD5/HMAC-MD5 authentication, it must be a ciphertext string of 1 to 53 characters.

Modified command: vrrp ipv6 vrid authentication-mode

Old syntax

vrrp ipv6 vrid *virtual-router-id* **authentication-mode simple** *key*

New syntax

vrrp ipv6 vrid *virtual-router-id* **authentication-mode simple** [**cipher**] *key*

View

Interface view

Parameters

virtual-router-id: VRRP group number, which ranges from 1 to 255.

simple: Specifies the simple authentication mode.

cipher: Sets the authentication key in cipher text.

key: Authentication key, a case-sensitive string. It is a plain-text string of 1 to 8 characters if the **cipher** keyword is not specified; or a cipher text string of 1 to 41 characters if the **cipher** keyword is specified.

Change description

The **cipher** keyword is added. With **cipher** specified, you can set a ciphertext authentication key of 1 to 41 characters.

Modified command: vrrp vrid authentication-mode

Old syntax

vrrp vrid *virtual-router-id* **authentication-mode** { **md5 | simple** } *key*

New syntax

vrrp vrid *virtual-router-id* **authentication-mode** { **md5 | simple** } [**cipher**] *key*

View

Interface view

Parameters

virtual-router-id: VRRP group number, which ranges from 1 to 255.

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

cipher: Sets the authentication key in cipher text.

key: Authentication key, a case-sensitive string.

- When **md5** authentication applies, the authentication key is a plain-text string of 1 to 8 characters or a cipher text string of 24 characters if the **cipher** keyword is not specified; or a cipher text string of 1 to 41 characters if the **cipher** keyword is specified.
- When **simple** authentication applies, the authentication key is a plain-text string of 1 to 8 characters if the **cipher** keyword is not specified; or a cipher text string of 1 to 41 characters if the **cipher** keyword is specified.

Change description

The **cipher** keyword is added. With **cipher** specified, you can set a ciphertext authentication key of 1 to 41 characters for MD5 authentication or simple authentication.

Modified feature: Task ID for IPv6 socket display

Feature change description

Changed the task ID value range for IPv6 socket display.

Command changes

Modified command: display ipv6 socket

Syntax

display ipv6 socket [**socktype** *socket-type*] [*task-id socket-id*] [**slot** *slot-number*] [**|** { **begin | exclude | include** } *regular-expression*]

Views

Any view

Change description

Before modification: The task ID is in the range of 1 to 150.

After modification: The task ID is in the range of 1 to 255.

Removed feature: Local user password display

Feature change description

Deleted the feature used to set a display mode for all local user passwords.

Removed commands

local-user password-display-mode

Syntax

local-user password-display-mode { **auto** | **cipher-force** }

undo local-user password-display-mode

View

System view

A5500EI-CMW520-F2211

This release has the following changes:

- New feature: Critical VLAN
- New feature: SCP
- New feature: Specifying the source interface for DNS packets
- New feature: MVRP
- New feature: Enabling LLDP to automatically discover IP phones

New feature: Critical VLAN

Overview

The critical VLAN feature enables a port to assign a VLAN to 802.1X users or MAC authentication users when they fail authentication because all the RADIUS authentication servers in their ISP domains have been unreachable, for example, due to the loss of network connectivity. The critical VLAN feature takes effect when authentication is performed only through RADIUS servers. If an 802.1X or MAC authentication user fails local authentication after RADIUS authentication, the user is not assigned to the critical VLAN.

The critical VLANs for 802.1X users are called “802.1X critical VLANs” and the critical VLANs for MAC authentication users are called “MAC authentication critical VLANs.”

You can configure one 802.1X critical VLAN and one MAC authentication critical VLAN on a port.

Any of the following RADIUS authentication server change in the ISP domain for 802.1X or MAC authentication users can cause the users to be removed from the critical VLAN:

- An authentication server is reconfigured, added, or removed.
- The status of any RADIUS authentication server automatically changes to active or is administratively set to active.
- The RADIUS server probing function detects that a RADIUS authentication server is reachable and sets its state to active.

802.1X critical VLAN assignment

The way that the network access device handles VLANs on an 802.1X-enabled port differs by 802.1X access control mode.

1. On a port that performs port-based access control

Authentication status	VLAN manipulation
A user that has not been assigned to any VLAN fails 802.1X authentication because all the RADIUS servers are unreachable.	Assigns the critical VLAN to the port as the PVID. The 802.1X user and all subsequent 802.1X users on this port can access only resources in the critical VLAN.
A user in the 802.1X critical VLAN fails authentication because all the RADIUS servers are unreachable.	The critical VLAN is still the PVID of the port, and all 802.1X users on this port are in this VLAN.

Authentication status	VLAN manipulation
A user in the 802.1X critical VLAN fails authentication for any other reason than server unreachable.	If an Auth-Fail VLAN has been configured, the PVID of the port changes to Auth-Fail VLAN ID, and all 802.1X users on this port are moved to the Auth-Fail VLAN.
A user in the critical VLAN passes 802.1X authentication.	• Assigns the VLAN specified for the user to the port as the PVID, and removes the port from the critical VLAN. After the user logs off, the default or user-configured PVID restores. • If the authentication server assigns no VLAN, the default or user-configured PVID applies. The user and all subsequent 802.1X users are assigned to this port VLAN. After the user logs off, this PVID remains unchanged.
A user in the 802.1X guest VLAN or the Auth-Fail VLAN fails authentication because all the RADIUS servers is reachable.	The PVID of the port remains unchanged. All 802.1X users on this port can access only resources in the guest VLAN or the Auth-Fail VLAN.

2. On a port that performs MAC-based access control

Authentication status	VLAN manipulation
A user that has not been assigned to any VLAN fails 802.1X authentication because all the RADIUS servers are unreachable.	Maps the MAC address of the user to the critical VLAN. The user can access only resources in the critical VLAN.
A user in the 802.1X critical VLAN fails authentication because all the RADIUS servers are unreachable.	The user is still in the critical VLAN.
A user in the critical VLAN fails 802.1X authentication for any other reason than server unreachable.	If an Auth-Fail VLAN has been configured, re-maps the MAC address of the user to the Auth-Fail VLAN ID.
A user in the critical VLAN passes 802.1X authentication.	Re-maps the MAC address of the user to the server-assigned VLAN. If the authentication server assigns no VLAN, re-maps the MAC address of the user to the default or user-configured PVID on the port.
A user in the 802.1X guest VLAN or the Auth-Fail VLAN fails authentication because all the RADIUS server are unreachable.	The user remains in the 802.1X VLAN or the Auth-Fail VLAN.
A user in the MAC authentication guest VLAN fails 802.1X authentication because all the 802.1X authentication server are unreachable.	The user is removed from the MAC authentication VLAN and mapped to the 802.1X critical VLAN.

NOTE:

- To perform the 802.1X critical VLAN function on a port that performs MAC-based access control, you must make sure that the port is a hybrid port, and enable MAC-based VLAN on the port.
- The network device assigns a hybrid port to an 802.1X critical VLAN as an untagged member.
- For more information about VLAN configuration and MAC-based VLAN, see *Layer 2—LAN Switching Configuration Guide*.

MAC authentication critical VLAN assignment

The MAC authentication critical VLAN feature depends on the MAC-based VLAN feature and is available only on hybrid ports.

When a user fails MAC authentication because no RADIUS server is reachable, the switch maps the user's MAC address to the MAC authentication critical VLAN. The MAC-to-critical VLAN mapping for the user is removed when any RADIUS server change in the ISP domain for the user occurs or after the user passes MAC authentication.

Configuring a 802.1X critical VLAN

Configuration guidelines

- You can configure only one 802.1X critical VLAN on a port. The 802.1X critical VLANs on different ports can be different.
- Assign different IDs for the voice VLAN, the port VLAN, and the 802.1X critical VLAN on a port, so the port can correctly process VLAN tagged incoming traffic.
- You cannot specify a VLAN as both a super VLAN and an 802.1X critical VLAN. For information about super VLANs, see *Layer 2—LAN Switching Configuration Guide*.
- You can use the **dot1x critical recovery-action reinitialize** command to configure the port to trigger 802.1X re-authentication when the port or an 802.1X user on the port is removed from the critical VLAN.
    - If MAC-based access control is used, the port sends a unicast Identity EAP/Request to the 802.1X user to trigger authentication.
    - If port-based access control is used, the port sends a multicast Identity EAP/Request to the 802.1X users to trigger authentication.
- If no critical VLAN is configured, RADIUS server unreachable can cause an online user being re-authenticated to be logged off. If a critical VLAN is configured, the user remains online and in the original VLAN.

Configuration prerequisites

- Create the VLAN to be specified as a critical VLAN.
- If the 802.1X-enabled port performs port-based access control, enable 802.1X multicast trigger (**dot1x multicast-trigger**).
- If the 802.1X-enabled port performs MAC-based access control, configure the port as a hybrid port, enable MAC-based VLAN on the port, and assign the port to the critical VLAN as an untagged member. For more information about the MAC-based VLAN function, see *Layer 2—LAN Switching Configuration Guide*.

Configuration procedure

To configure an 802.1X critical VLAN on a port:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure an 802.1X critical VLAN on the port.	**dot1x critical vlan** *vlan-id*	By default, no 802.1X critical VLAN is configured.
4. (Optional) Configure the port to trigger 802.1X authentication on detection of a reachable authentication server for users in the critical VLAN.	**dot1x critical recovery-action reinitialize**	By default, when a reachable RADIUS server is detected, the system removes the port or 802.1X users from the critical VLAN without triggering authentication.

Configuring a MAC authentication critical VLAN

You can configure only one MAC authentication critical VLAN on a port.

Follow the guidelines in Table 1 when you configure a MAC authentication critical VLAN on a port.

Table 1 Relationships of the MAC authentication critical VLAN with other security features

Feature	Relationship description	Reference
Quiet function of MAC authentication	The MAC authentication critical VLAN function has higher priority. When a user fails MAC authentication because no RADIUS authentication server is reachable, the user can access the resources in the critical VLAN, and the user's MAC address is not marked as a silent MAC address.	*Security Configuration Guide*
Super VLAN	You cannot specify a VLAN as both a super VLAN and a MAC authentication critical VLAN.	*Layer 2—LAN Switching Configuration Guide*
Port intrusion protection	The MAC authentication critical VLAN function has higher priority than the block MAC action but lower priority than the shut down port action of the port intrusion protection feature.	*Security Configuration Guide*

Configuration prerequisites

- Enable MAC authentication.
- Enable MAC-based VLAN on the port.
- Create the VLAN to be specified as the MAC authentication critical VLAN.

Configuration procedure

To configure a MAC authentication critical VLAN on a port:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure a MAC authentication critical VLAN on the port.	**mac-authentication critical vlan** *critical-vlan-id*	By default, no MAC authentication critical VLAN is configured.

Configuring a RADIUS server probe

When you add a primary or secondary RADIUS authentication server to a RADIUS scheme, you can configure a probe to regularly detect the availability (or reachability) of the server. If the server is unreachable, its state is **block**. If the server is reachable, its state is **active**.

When a server status change is detected, the RADIUS server probe advertises the change to the authentication modules, including the 802.1X module, so these modules can take prompt responsive action. For example, the 802.1X module removes users from an 802.1X critical VLAN and makes authentication triggering decision immediately after the RADIUS authentication server probing function detects that a server in the ISP domain for the 802.1X users has become reachable and changes the server state to active.

To configure RADIUS authentication server probes:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter RADIUS scheme view.	**radius scheme** *radius-scheme-name*	N/A
3. Configure RADIUS authentication server probes.	• Configure the primary RADIUS authentication server probe: **primary authentication** { *ipv4-address* | **ipv6** *ipv6-address* } **probe username** *name* [**interval** *interval*] • Configure the secondary RADIUS server probe: **secondary authentication** { *ipv4-address* | **ipv6** *ipv6-address* } **probe username** *name* [**interval** *interval*]	By default, no RADIUS authentication server probes are configured.

Command reference

dot1x critical vlan

Use the **dot1x critical vlan** command to configure an 802.1X critical VLAN on a port for users that fail 802.1X authentication because all the RADIUS servers in their ISP domains have been unreachable.

Syntax

dot1x critical vlan *vlan-id*

undo dot1x critical vlan

Default

No critical VLAN is configured on any port.

Views

Layer 2 Ethernet interface view

Default command level

2: System level

Parameters

vlan-id: Specifies a VLAN ID, in the range of 1 to 4094. Make sure the VLAN has been created.

Usage guidelines

You can configure only one critical VLAN on a port. The 802.1X critical VLANs on different ports can be different.

When you change the access control method from MAC-based to port-based on the port, the mappings between MAC addresses and the 802.1X critical VLAN are removed. You can use the **display mac-vlan** command to display MAC-to-VLAN mappings.

When you change the access control method from port-based to MAC-based on a port that is in a critical VLAN, the port is removed from the critical VLAN.

To delete a VLAN that has been configured as an 802.1X critical VLAN, you must perform the **undo dot1x critical vlan** command first.

Examples

Specify VLAN 3 as the 802.1X critical VLAN on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x critical vlan 3
```

dot1x critical recovery-action

Use the **dot1x critical recovery-action** command to configure the action that a port takes when an active (reachable) RADIUS authentication server is detected for users in the 802.1X critical VLAN.

Use the **undo dot1x critical recovery-action** command to restore the default.

Syntax

dot1x critical recovery-action reinitialize

undo dot1x critical recovery-action

Default

When a reachable RADIUS server is detected, the system removes the port or 802.1X users from the critical VLAN without triggering authentication.

Views

Layer 2 Ethernet interface view

Default command level

2: System level

Parameters

reinitialize: Enables the port to trigger 802.1X re-authentication on detection of a reachable RADIUS authentication server for users in the critical VLAN.

Usage guidelines

The **dot1x critical recovery-action** command takes effect only for the 802.1X users in the critical VLAN on a port. It enables the port to take one of the following actions to trigger 802.1X authentication after removing 802.1X users from the critical VLAN on detection of a reachable RADIUS authentication server:

- If MAC-based access control is used, the port sends a unicast Identity EAP/Request to each 802.1X user.
- If port-based access control is used, the port sends a multicast Identity EAP/Request to all the 802.1X users attached to the port.

Examples

Configure port GigabitEthernet 1/0/1 to trigger 802.1X re-authentication on detection of an active RADIUS authentication server for users in the critical VLAN.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x critical recovery-action reinitialize
```

mac-authentication critical vlan

Use the **mac-authentication critical vlan** command to configure a MAC authentication critical VLAN on a port for MAC authentication users that have failed authentication because all the RADIUS authentication servers in their ISP domain are unreachable.

Use the **undo mac-authentication critical vlan** command to restore the default.

Syntax

mac-authentication critical vlan *critical-vlan-id*

undo mac-authentication critical vlan

Default

No MAC authentication critical VLAN is configured on a port.

Views

Layer 2 Ethernet interface view

Default command level

2: System level

Parameters

critical-vlan-id: Specifies a VLAN ID, in the range of 1 to 4094. Make sure the VLAN has been created.

Usage guidelines

You can configure only one MAC authentication critical VLAN on a port. The MAC authentication critical VLANs on different ports can be different.

You cannot specify a VLAN as both a super VLAN and a MAC authentication critical VLAN. For more information about super VLANs, see *Layer 2—LAN Switching Configuration Guide*.

To delete a VLAN that has been configured as a MAC authentication critical VLAN, you must perform the **undo mac-authentication critical vlan** command first.

Examples

Specify VLAN 5 as the MAC authentication critical VLAN on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication critical vlan 5
```

Related commands

- **mac-authentication**
- **mac-vlan enable**

primary authentication probe

Use the **primary authentication probe** command to configure a probe to detect the availability of the primary authentication server in a RADIUS scheme.

Use the **undo primary authentication** command to remove the primary RADIUS authentication server in a RADIUS scheme.

Syntax

primary authentication { *ipv4-address* **| ipv6** *ipv6-address* } **probe username** *name* [**interval** *interval*]

undo primary authentication

Default

No probe has been configured for any RADIUS authentication server.

Views

RADIUS scheme view

Default command level

2: System level

Parameters

ipv4-address: Specifies the IPv4 address of the primary RADIUS authentication server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the primary RADIUS authentication server. The *ipv6-address* argument must be a valid IPv6 global unicast address.

probe: Configure a probe for the primary authentication server.

username *name*: Assigns a name to the probe. This name is used as the username in the authentication requests sent by the probe to the RADIUS server. The *name* argument is a string of 1 to 64 characters and can be a username that has not been created on the RADIUS server.

interval *interval*: Sets the probing interval in minutes, in the range of 1 to 3600. If no probing interval is specified, the probe performs probing every 60 minutes.

Usage guidelines

A primary RADIUS authentication server probe periodically sends authentication requests to the primary RADIUS authentication server. If no response has been received from the server before timer set by the **timer response-timeout** command expires, the probe re-transmits the request. If a response is received from the server before the maximum number of retries (set by using the **retry** command) is reached, the probe considers the server is reachable and sets the server in **active** state. If not, the probe considers the server is unreachable and sets the server in **block** state.

The state of a blocked RADIUS server changes to **active** when the server probe detects that the server is reachable or the server quiet timer (set by using the **timer quiet** command) times out.

Quiet timer timeouts cause block-to-active changes regardless of the real server availability state. A short server quiet timer setting can cause frequent server state changes when network connectivity is poor. To avoid frequent server state changes causing frequent critical VLAN assignments and removals, make sure the server quiet timer is long enough.

Examples

Configure the probe **test** to detect the primary RADIUS authentication server in the RADIUS scheme **radius1** every 120 minutes.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary authentication 10.110.1.1 probe username test interval
120
```

secondary authentication probe

Use the **secondary authentication probe** command to configure a probe to detect the availability of the secondary authentication server in a RADIUS scheme.

Use the **undo secondary authentication** command to remove the secondary RADIUS authentication server in a RADIUS scheme.

Syntax

secondary authentication { *ipv4-address* **| ipv6** *ipv6-address* } **probe username** *name* [**interval** *interval*]

undo secondary authentication [*ipv4-address* **| ipv6** *ipv6-address*]

Default

No probe has been configured for any RADIUS authentication server.

Views

RADIUS scheme view

Default command level

2: System level

Parameters

ipv4-address: Specifies the IPv4 address of the secondary RADIUS authentication server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the secondary RADIUS authentication server. The *ipv6-address* argument must be a valid IPv6 global unicast address.

probe: Configure a probe for the secondary authentication server.

username *name*: Assigns a name to the probe. This name is used as the username in the authentication requests sent by the probe to the RADIUS server. The *name* argument is a string of 1 to 64 characters and can be a username that has not been created on the RADIUS server.

interval *interval*: Sets the probing interval in minutes, in the range of 1 to 3600. If no probing interval is specified, the probe performs probing every 60 minutes.

Usage guidelines

A secondary RADIUS authentication server probe periodically sends authentication requests to the secondary RADIUS authentication server. If no response has been received from the server before timer set by the **timer response-timeout** command expires, the probe re-transmits the request. If a response is received from the server before the maximum number of retries (set by using the **retry** command) is reached, the probe considers the server is reachable and sets the server in **active** state. If not, the probe considers the server is unreachable and sets the server in **block** state.

The state of a blocked RADIUS server changes to **active** when the server probe detects that the server is reachable or the server quiet timer (set by using the **timer quiet** command) times out.

Quiet timer timeouts cause block-to-active changes regardless of the real server availability state. A short server quiet timer setting can cause frequent server state changes when network connectivity is poor. To avoid frequent server state changes causing frequent critical VLAN assignments and removals, make sure the server quiet timer is long enough.

Examples

Configure the probe **test** to detect the secondary RADIUS authentication server in the RADIUS scheme **radius1** every 120 minutes.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1]secondary authentication 10.110.1.1 probe username test interval
120
```

New feature: SCP

Overview

Secure copy (SCP) is based on SSH2.0 and offers a secure approach to copying files.

SCP uses SSH connections for copying files. The switch can act as the SCP server, allowing a user to log in to the switch for file upload and download. The switch can also act as an SCP client, enabling a user to log in from the switch to a remote server for secure file transfer.

NOTE:

When the switch acts as an SCP server, only one of all the FTP, SFTP and SCP users can access the switch.

Configuring the switch as an SCP server

To configure the switch as an SCP server:

Step	Command	Remarks
1. Enter system view.	**system-view**	**N/A**
2. Configure the SSH server.	For more information, see the security guide for your switch.	N/A
3. Create an SSH user for a SCP client, set the service type to **all** or **scp**, and specify the authentication method.	**ssh user** *username* **service-type** { **all** | **scp** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* **work-directory** *directory-name* }	N/A
4. Create a user account and assign a working directory for the SSH user on the switch or a remote server if password authentication is used.	• On the remote server (details not shown) • On the switch: **a. local-user** **b. password** **c. service-type ssh** **d. authorization-attribute work-directory** *directory-name*	**Skip this step if** publickey authentication, whether with password authentication or not, is used. Make sure that the local user account has the name username as the username specified in the **ssh user** command.

When you set the working directory for the user, follow these guidelines:

- If only password authentication is used, the working directory specified in the **ssh user** command does not take effect. You must set the working directory on the remote server or in the local user account for the SSH user.
- If publickey authentication, whether with password authentication or not, is used, you must set the working directory in the **ssh user** command.

Configuring the switch as the SCP client

To upload or download files to or from an SCP server, perform the following tasks in any view:

Task	Command
Upload a file to an SCP server.	• Upload a file to the IPv4 SCP server: **scp** *server* [*port-number*] **put** *source-file-path* [*destination-file-path*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * • Upload a file to the IPv6 SCP server: **scp ipv6** *server* [*port-number*] **put** *source-file-path* [*destination-file-path*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *
Download a file from an SCP server.	• Download a file from the remote IPv4 SCP server: **scp** *server* [*port-number*] **get** *source-file-path* [*destination-file-path*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * • Download a file from the remote IPv6 SCP server: **scp ipv6** *server* [*port-number*] **get** *source-file-path* [*destination-file-path*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

NOTE:

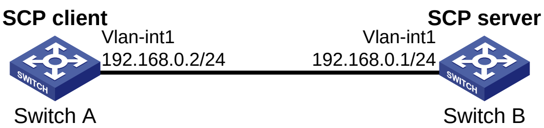
File transfer interruption during a downloading process can result in file fragments on the switch. You must manually delete them.

SCP client configuration example

Network requirements

As shown in Figure 1, switch A acts as a client and download the file **remote.bin** from switch B. The user has the username **test** and uses the password authentication method.

Figure 1 Network diagram



Configuration procedure

Create VLAN-interface 1 and assign an IP address to it.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 192.168.0.2 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

Download the file **remote.bin** from the SCP server, and save it with the file name **local.bin**.

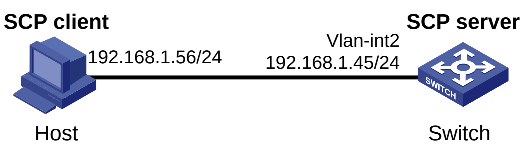
```
<SwitchA> scp 192.168.0.1 get remote.bin local.bin
Username: test
Trying 192.168.0.1 ...
Press CTRL+K to abort
Connected to 192.168.0.1 ...

The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
Enter password:
18471 bytes transfered in 0.001 seconds.
```

SCP server configuration example

Network requirements

As shown in Figure 2, the switch acts as the SCP server, and the host acts as the SCP client. The host establishes an SSH connection to the switch. The user uses the username **test** and the password **aabbcc.** The username and password are saved on the switch for local authentication.

Figure 2 Network diagram



Configuration procedure

Generate the RSA key pairs.

```
<Switch> system-view
[Switch] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++
++++++++++++++
+++++
++++++++
```

Generate the DSA key pair.

```
[Switch] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++
```

Enable the SSH server function.

```
[Switch] ssh server enable
```

Configure an IP address for VLAN-interface 1, which the client will use as the destination for SSH connection.

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.1.45 255.255.255.0
[Switch-Vlan-interface1] quit
```

Set the authentication mode of the user interfaces to AAA.

```
[Switch] user-interface vty 0 15
[Switch-ui-vty0-15] authentication-mode scheme
```

Enable the user interfaces to support all protocols including SSH.

```
[Switch-ui-vty0-15] protocol inbound all
[Switch-ui-vty0-15] quit
```

Create the local user **test** and specify a working directory for the user.

```
[Switch] local-user test
[Switch-luser-test] password simple aabbcc
[Switch-luser-test] service-type ssh
[Switch-luser-test] authorization-attribute work-directory flash:/
[Switch-luser-test] quit
```

Configure the SSH user authentication method as **password** and service type as **scp**.

```
[Switch] ssh user test service-type scp authentication-type password
```

Command reference

scp

Use the **scp** command to transfer files with an SCP server.

Syntax

scp [**ipv6**] *server* [*port-number*] { **get** | **put** } *source-file-path* [*destination-file-path*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

Views

User view

Default command level

3: Manage level

Parameters

ipv6: Specifies the type of the server as IPv6. If this keyword is not specified, the server is an IPv4 server.

server: Specifies an IPv4 or IPv6 address or host name of the server. For an IPv4 server, it is a case-insensitive string of 1 to 20 characters. For an IPv6 server, it is a case-insensitive string of 1 to 46 characters.

port-number: Specifies the port number of the server, in the range of 0 to 65535. The default is 22.

identity-key: Specifies the algorithm for publickey authentication, either **dsa** or **rsa**. The default is **dsa**.

- **dsa**: Specifies the publickey algorithm **dsa.**

- **rsa**: Specifies the publickey algorithm **rsa**.

prefer-ctos-cipher: Preferred encryption algorithm from client to server, defaulted to **aes128**.

- **3des**: Encryption algorithm 3des-cbc.
- **aes128**: Encryption algorithm aes128-cbc.
- **des**: Encryption algorithm des-cbc.

prefer-ctos-hmac: Preferred HMAC algorithm from client to server, defaulted to **sha1-96**.

- **md5**: HMAC algorithm hmac-md5.
- **md5-96**: HMAC algorithm hmac-md5-96.
- **sha1**: HMAC algorithm hmac-sha1.
- **sha1-96**: HMAC algorithm hmac-sha1-96.

prefer-kex: Preferred key exchange algorithm, defaulted to **dh-group-exchange**.

- **dh-group-exchange**: Key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1**: Key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14**: Key exchange algorithm diffie-hellman-group14-sha1.

prefer-stoc-cipher: Preferred encryption algorithm from server to client, defaulted to **aes128**.

prefer-stoc-hmac: Preferred HMAC algorithm from server to client, defaulted to **sha1-96**.

Usage guidelines

When the client's authentication method is publickey, the client needs to get the local private key for digital signature. As the publickey authentication includes RSA and DSA algorithms, you must specify an algorithm (by using the **identity-key** keyword) in order to get the correct data for the local private key. By default, the publickey algorithm is DSA.

Examples

Download the file **remote.bin** from the SCP server, save it locally and change the file name to **local.bin**

```
<Sysname> scp 192.168.0.1 get remote.bin local.bin
```

ssh user

Use the **ssh user** command to create an SSH user and specify the service type and authentication method.

Use the **undo ssh user** command to delete an SSH user.

Syntax

ssh user *username* **service-type stelnet authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* }

ssh user *username* **service-type** { **all** | **scp** | **sftp** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* **work-directory** *directory-name* }

undo ssh user *username*

Views

System view

Default command level

3: Manage level

Parameters

username: SSH username, a case-sensitive string of 1 to 80 characters.

service-type: Specifies the service type of an SSH user, which can be one of the following:

- **all**: Specifies Stelnet, SFTP, and SCP.
- **scp**: Specifies the service type as secure copy.
- **sftp**: Specifies the service type as secure FTP.
- **stelnet**: Specifies the service type of secure Telnet.

authentication-type: Specifies the authentication method of an SSH user, which can be one of the following:

- **password**: Performs password authentication. This authentication method features easy and fast encryption, but it is vulnerable. It can work with AAA to implement user authentication, authorization, and accounting.
- **any**: Performs either password authentication or publickey authentication.
- **password-publickey**: Performs both password authentication and publickey authentication (featuring higher security) if the client runs SSH2, and performs either type of authentication if the client runs SSH1.
- **publickey**: Performs publickey authentication. This authentication method has the downside of complicated and slow encryption, but it provides strong authentication that can defend against brute-force attacks. This authentication method is easy to use. Once it is configured, the authentication process completes automatically without the need of remembering or entering any password.

assign publickey *keyname*: Assigns an existing public key to an SSH user. The *keyname* argument indicates the name of the client public key and is a string of 1 to 64 characters.

work-directory *directory-name*: Specifies the working directory for an SCP or SFTP user. The *directory-name* argument indicates the name of the working directory and is a string of 1 to 135 characters.

Usage guidelines

For a publickey authentication user, you must configure the username and the public key on the switch. For a password authentication user, you can configure the account information on either the switch or the remote authentication server, such as a RADIUS server.

If you use the **ssh user** command to configure a public key for a user who has already had a public key, the new one overwrites the old one.

You can change the authentication method and public key of an SSH user when the user is communicating with the SSH server. However, your changes take effect only after the user logs out and logs in again.

If an SCP or SFTP user has been assigned a public key, it is necessary to set a working folder for the user.

The working folder of an SCP or SFTP user depends on the user authentication method. For a user using only password authentication, the working folder is the AAA authorized one. For a user using only publickey authentication or using both publickey authentication and password authentication, the working folder is the one set by using the **ssh user** command.

Examples

Create an SSH user named **user1**, setting the service type as **scp**, the authentication method as **publickey**, the working directory of the SCP server as **flash:/**, and assigning a public key named **key1** to the user.

```
<Sysname> system-view
[Sysname] ssh user user1 service-type scp authentication-type publickey assign publickey
key1 work-directory flash:/
```

Related commands

display ssh user-information

New feature: Specifying the source interface for DNS packets

Specifying the source interface for DNS packets

By default, the device uses the primary IP address of the output interface of the matching route as the source IP address of a DNS request. Therefore, the source IP address of the DNS packets may vary with DNS servers. In some scenarios, the DNS server only responds to DNS requests sourced from a specific IP address. In such cases, you must specify the source interface for the DNS packets so that the device can always uses the primary IP address of the specified source interface as the source IP address of DNS packets.

To specify the source interface for DNS packets:

Step	Command	Remarks
Enter system view.	**system-view**	N/A
Specify the source interface for DNS packets.	**dns source-interface** *interface-type interface-number*	By default, no source interface for DNS packets is specified; the device looks up its routing table for an output interface for a DNS request destined for a DNS server and uses the primary IP address of the interface as the source IP address of the packet.

Command reference

dns source-interface

Use **dns source-interface** to specify the source interface for DNS packets.

Use **undo dns source-interface** to restore the default.

Syntax

dns source-interface *interface-type interface-number*

undo dns source-interface

Default

No source interface for DNS packets is specified. The device uses the primary IP address of the output interface of the matching route as the source IP address of a DNS request.

Views

System view

Default command level

2. System level

Parameters

interface-type interface-number: Specifies the interface type and number.

Usage guidelines

The device uses the primary IP address of the specified source interface as the source IP address of a DNS request, which however is still forwarded through the output interface of the matching route.

Examples

Specify VLAN-interface 2 as the source interface of DNS requests.

```
<Sysname> system-view
[Sysname] dns source-interface vlan-interface2
```

New feature: MVRP

Overview

Multiple Registration Protocol (MRP) is an attribute registration protocol and transmits attribute messages. Multiple VLAN Registration Protocol (MVRP) is a typical MRP application. MVRP propagates and learns VLAN configuration among devices. MVRP enables a device to propagates the local VLAN configuration to the other devices, receive VLAN configuration from other devices, and dynamically update the local VLAN configuration (including the active VLANs and the ports through which a VLAN can be reached). MVRP makes sure that all MVRP-enabled devices in a LAN maintain the same VLAN configuration, and reduces the VLAN configuration workload. When the network topology changes, MVRP can propagate and learn VLAN configuration information again according to the new topology, and real-time synchronize the network topology.

MRP is an enhanced version of Generic Attribute Registration Protocol (GARP) and improves the declaration efficiency. MVRP is an enhanced version of GARP VLAN Registration Protocol (GVRP). MVRP delivers the following benefits over GVRP:

- GVRP does not support the multiple spanning tree instance (MSTI). MVRP runs on a per-MSTI basis, and implements per-VLAN redundant link calculation and load sharing.
- MVRP decreases the number of packets transmitted for the same amount of VLAN configuration, and improves the declaration efficiency.

For more information about GVRP or MSTI, see " *Layer 2—LAN Switching Configuration Guide*."

MRP

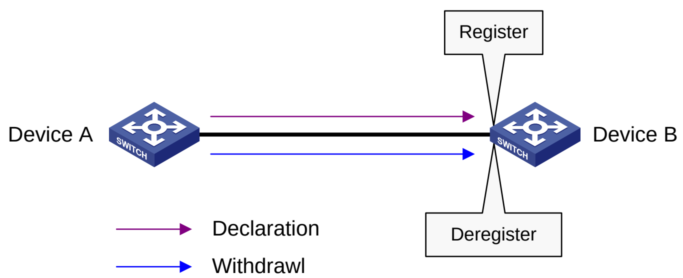
MRP allows participants in the same LAN to declare, propagate, and register information (for example, VLAN information) on a per Multiple Spanning Tree Instance (MSTI) basis.

MRP implementation

Each port that participates in an MRP application (for example, MVRP) is called an "MRP participant". Similarly, a port that participates in an MVRP application is called an "MVRP participant."

As shown in Figure 3, an MRP participant registers and deregisters its attribute values on other MRP participants by sending declarations and withdrawals, and registers and deregisters the attribute values of other participants according to the received declarations and withdrawals. MRP rapidly propagates the configuration information of an MRP participant throughout the LAN.

Figure 3 MRP implementation



MVRP registers and deregisters VLAN attributes as follows:

- When a port receives the declaration of a VLAN attribute, the port registers the VLAN and joins the VLAN.
- When a port receives the withdrawal of a VLAN attribute, the port deregisters the VLAN and leaves the VLAN.

Figure 3 shows a simple MVRP implementation on an MSTI. In a network with multiple MSTIs, VLAN registration and deregistration are performed on a per-MSTI basis.

MRP messages

MRP exchanges information among MRP participants by advertising MRP messages, including Join, New, Leave, and LeaveAll. Join and New messages are declarations, and Leave and LeaveAll messages are withdrawals.

- Join message
  - An MRP participant sends Join messages when it wishes to declare the attribute values configured on it and receives Join messages from other MRP participants.
  - When receiving a Join message, an MRP participant sends a Join message to all participants except the sender.

  Join messages fall into the following types:
  - **JoinEmpty**—An MRP participant sends JoinEmpty messages to declare attribute values that it has not registered. For example, when a static VLAN exists on a device, the attribute of the VLAN on the device is not changed even if the device learns the VLAN again through MRP. In this case, the Join message for the VLAN attribute is a JoinEmpty message, because the VLAN attribute is not registered.
  - **JoinIn**—An MRP participant sends JoinIn messages to declare attribute values that it has registered. For example, when the device learns a VLAN through MRP messages, and dynamically creates the VLAN, the Join message for the VLAN attribute is a JoinIn message.
- New message

  Similar to a Join message, a New message enables MRP participants to register attributes.
  - When the Multiple Spanning Tree Protocol (MSTP) topology changes, an MRP participant sends New messages to declare the topology change.
  - On receiving a New message, an MRP participant sends a New message out of each port except the receiving port.
- Leave message
  - An MRP participant sends Leave messages when it wishes other participants to deregister the attributes that is has deregistered.
  - When receiving a Leave message, an MRP participant sends a Leave message to all participants except the sender.
- LeaveAll message
  - Each MRP participant is configured with an individual LeaveAll timer. When the timer expires, the MRP participant sends LeaveAll messages to the remote participants, so that the local participant and the remote participants deregister all attributes and re-register all attributes. This process periodically clears the useless attributes in the network.
  - On receiving a LeaveAll message, MRP determines whether to send a Join message to request the sender to re-register these attributes according to attribute status.

MRP timers

The implementation of MRP uses the following timers to control MRP message transmission.

- Periodic timer

  On startup, an MRP participant starts its own Periodic timer to control MRP message transmission. The MRP participant collects the MRP messages to be sent before the Periodic timer expires, and sends the MRP messages in as few packets as possible when the Periodic timer expires and meanwhile restarts the Periodic timer. This mechanism reduces the number of MRP protocol packets periodically sent.

You can enable or disable the Periodic timer at the CLI. When you disable the Periodic timer, MRP will not periodically send MRP messages, and MRP messages are sent only when the LeaveAll timer expires or the local participant receives LeaveAll messages from a remote participant.

- Join timer

  The Join timer controls the transmission of Join messages. To make sure that Join messages can be reliably transmitted to other participants, an MRP participant waits for a period of the Join timer after sending a Join message. If the participant receives JoinIn messages from other participants and the attributes in the JoinIn messages are the same as the sent Join messages before the Join timer expires, the participant does not re-send the Join message. When both the Join timer and the Periodic timer expire, the participant re-sends the Join message.

- Leave timer

  The Leave timer controls the deregistration of attributes. When an MRP participant wishes other participants to deregister its attributes, it sends a Leave message. On receiving a Leave message, MRP starts the Leave timer, and deregisters the attributes if it does not receive any Join message for the attributes before the Leave timer expires. When an MRP participant sends or receives LeaveAll messages, it starts the Leave timer. MRP deregisters the attributes in the LeaveAll messages if it does not receive any Join message for the attributes before the Leave timer expires.

- LeaveAll timer

  On startup, an MRP participant starts its own LeaveAll timer. When the LeaveAll timer expires, MRP sends out a LeaveAll message and restarts the LeaveAll timer. On receiving the LeaveAll message, other participants re-register all the attributes and re-start their LeaveAll timer.

When you configure the MRP timers, follow these guidelines:

- When the LeaveAll timer of an MRP participant expires, the MRP participant sends LeaveAll messages to the remote participants. On receiving a LeaveAll message, a remote participant restarts its LeaveAll timer, and stops sending out LeaveAll messages. This mechanism effectively reduces the number of LeaveAll messages in the network.
- To avoid the case that the LeaveAll timer of a fixed participant always first expires, the switch randomly changes the LeaveAll timer within a certain range when the MRP participant restarts its LeaveAll timer.

MVRP registration modes

The VLAN information propagated by MVRP includes not only locally, manually configured static VLAN information but also dynamic VLAN information from other devices.

VLANs created manually, locally are called "static VLANs", and VLANs learned through MVRP are called "dynamic VLANs". The following MVRP registration modes are available.

- Normal

  An MVRP participant in normal registration mode performs dynamic VLAN registrations and deregistrations, and sends declarations and withdrawals for dynamic and static VLANs.

- Fixed

  An MVRP participant in fixed registration mode disables deregistering dynamic VLANs, sends declarations for dynamic VLANs and static VLANs, and drops received MVRP protocol packets. As a result, an MVRP participant port in fixed registration mode does not deregister or register dynamic VLANs.

- Forbidden

  An MVRP participant in forbidden registration mode disables registering dynamic VLANs, sends declarations for dynamic VLANs and static VLANs, and drops received MVRP protocol packets. As a result, an MVRP participant in forbidden registration mode does not register dynamic VLANs, and does not re-register a dynamic VLAN when the VLAN is deregistered.

Protocols and standards

IEEE 802.1ak *IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks – Amendment 07: Multiple Registration Protocol*

MVRP configuration task list

Task	Remarks
Enabling MVRP	Required.
Configuring the MVRP registration mode	Optional.
Configuring MRP timers	Optional.
Enabling GVRP compatibility	Optional.

Configuration prerequisites

Before configuring MVRP, perform the following tasks:

- Make sure that all MSTIs in the network are effective and each MSTI is mapped to an existing VLAN on each device in the network, because MVRP runs on a per-MSTI basis.
- Configure the involved ports as trunk ports, because MVRP is available only on trunk ports.

Enabling MVRP

This section describes how to enable MVRP.

Configuration restrictions and guidelines

- MVRP can work with STP, RSTP, or MSTP, but not other link layer topology protocols, including service loopback, PVST, RRPP, and Smart Link. Ports blocked by STP, RSTP, or MSTP can receive and send MVRP protocol packets. For more information about service loopback, STP, RSTP, MSTP, and PVST, see " *Layer 2—LAN Switching Configuration Guide*." For more information about RRPP and Smart Link, see *High Availability Configuration Guide*.
- Do not enable both MVRP and remote port mirroring on a port. Otherwise, MVRP may register the remote probe VLAN to incorrect ports, which would cause the monitor port to receive undesired duplicates. For more information about port mirroring, see *Network Management and Monitoring Configuration Guide*.
- Enabling MVRP on a Layer 2 aggregate interface enables both the aggregate interface and all Selected member ports in the link aggregation group to participate in dynamic VLAN registration and deregistration.

Configuration procedure

To enable MVRP:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable MVRP globally.	**mvrp global enable**	By default, MVRP is globally disabled. To enable MVRP on a port, first enable MVRP globally.

Step	Command	Remarks
3. Enter interface view.	• Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: **interface** *interface-type interface-number* • Enter port group view: **port-group manual** *port-group-name*	Use one of the commands.
4. Configure the port to permit the specified VLANs.	**port trunk permit vlan {** *vlan-list* **| all }**	By default, a trunk port permits only VLAN 1. Make sure that the trunk port permits all registered VLANs. For more information about the **port trunk permit vlan** command, see *Layer 2—LAN Switching Command Reference*.
5. Enable MVRP on the port.	**mvrp enable**	By default, MVRP is disabled on a port.

Configuring the MVRP registration mode

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	• Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: **interface** *interface-type interface-number* • Enter port group view: **port-group manual** *port-group-name*	Use one of the commands.
3. Configure the MVRP registration mode.	**mvrp registration** { **fixed** | **forbidden** | **normal** }	Optional. The default setting is normal registration mode.

Configuring MRP timers

CAUTION:

The MRP timers apply to all MRP applications, for example, MVRP, on a port. To avoid frequent VLAN registrations and deregistrations, use the same MRP timers throughout the network.

Each port maintains its own Periodic, Join, and LeaveAll timers, and each attribute of a port maintains a Leave timer.

To configure MRP timers:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Enter interface view.	• Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: **interface** *interface-type interface-number* • Enter port group view: **port-group manual** *port-group-name*	Use one of the commands.
3. Configure the LeaveAll timer.	**mrp timer leaveall** *timer-value*	Optional. The default setting is 1000 centiseconds.
4. Configure the Join timer.	**mrp timer join** *timer-value*	Optional. The default setting is 20 centiseconds.
5. Configure the Leave timer.	**mrp timer leave** *timer-value*	Optional. The default setting is 60 centiseconds.
6. Configure the Periodic timer.	**mrp timer periodic** *timer-value*	Optional. The default setting is 100 centiseconds.

Table 17 shows the value ranges for Join, Leave, and LeaveAll timers and their dependencies.

- If you set a timer to a value beyond the allowed value range, your configuration will fail. To do that, you can change the allowed value range by tuning the value of another related timer.
- To restore the default settings of the timers, restore the Join timer first, followed by the Leave and LeaveAll timers.

Table 17 Dependencies of the Join, Leave, and LeaveAll timers

Timer	Lower limit	Upper limit
Join	20 centiseconds	Half the Leave timer
Leave	Twice the Join timer	LeaveAll timer
LeaveAll	Leave timer on each port	32760 centiseconds

You can restore the Periodic timer to the default at any time.

Enabling GVRP compatibility

CAUTION:

- MVRP with GVRP compatibility enabled can work together with STP or RSTP, but cannot work together with MSTP. When MVRP with GVRP compatibility enabled works with MSTP, the network might operate improperly.
- When GVRP compatibility is enabled for MVRP, HP recommends disabling the Period timer. Otherwise, the VLAN status might frequently change when the system is busy.

MVRP can be compatible with GVRP. When the peer device supports GVRP, you can enable GVRP compatibility on the local end, so that the local end can receive and send MVRP and GVRP protocol packets at the same time.

To enable GVRP compatibility:

Step	Command	Remarks
1. Enter system view	**system-view**	N/A
2. Enable GVRP compatibility	**mvrp gvrp-compliance enable**	By default, GVRP compatibility is disabled.

Displaying and maintaining MVRP

Task	Command	Remarks
Display the MVRP status of the specified port and each MVRP interface in the specified VLAN.	**display mvrp state interface** *interface-type interface-number* **vlan** *vlan-id* [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the MVRP running status.	**display mvrp running-status** [**interface** *interface-list*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the MVRP statistics.	**display mvrp statistics** [**interface** *interface-list*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the dynamic VLAN operation information of the specified port.	**display mvrp vlan-operation interface** *interface-type interface-number* [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Clear the MVRP statistics of the specified ports.	**reset mvrp statistics** [**interface** *interface-list*]	Available in user view

Configuration example for MVRP in normal registration mode

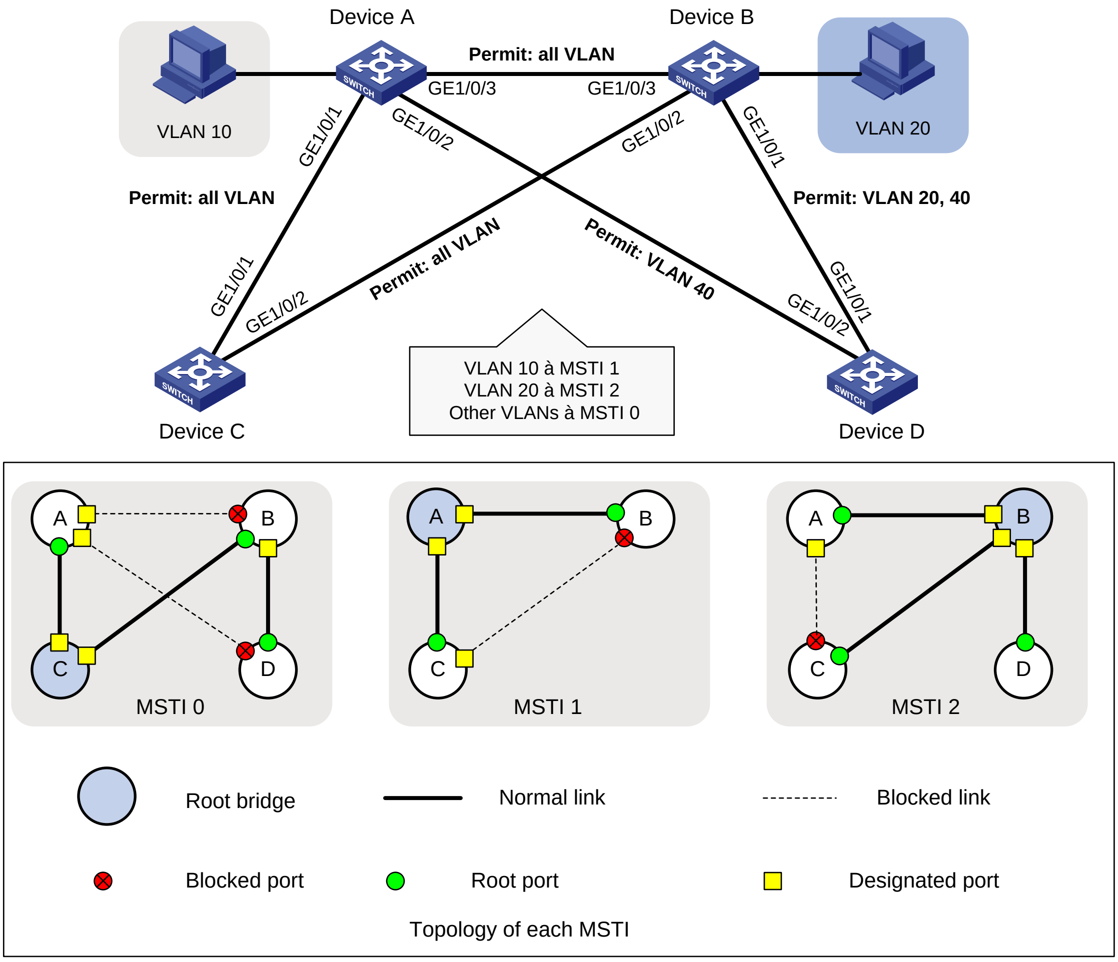
Network requirements

As shown in Figure 4, configure MSTP, map VLAN 10 to MSTI 1, map VLAN 20 MST 2, and map the other VLANs to MSTI 0.

Configure MVRP and set the MVRP registration mode to normal, so that Device A, Device B, Device C, and Device D can register and deregister dynamic and static VLANs and keep identical VLAN configuration for each MSTI.

When the network is stable, set the MVRP registration mode to fixed on the port that connecting Device B to Device A, so that the dynamic VLANs on Device B are not de-registered.

Figure 4 Network diagram



Configuration procedure

Configuring Device A

Enter MST region view.

```
<DeviceA> system-view
[DeviceA] stp region-configuration
```

Configure the MST region name, VLAN-to-instance mappings, and revision level.

```
[DeviceA-mst-region] region-name example
[DeviceA-mst-region] instance 1 vlan 10
[DeviceA-mst-region] instance 2 vlan 20
[DeviceA-mst-region] revision-level 0
```

Manually activate the MST region configuration.

```
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

Configure Device A as the primary root bridge of MSTI 1.

```
[DeviceA] stp instance 1 root primary
```

Globally enable the spanning tree feature.

```
[DeviceA] stp enable
```

Globally enable MVRP.

```
[DeviceA] mvrp global enable
```

Configure port GigabitEthernet 1/0/1 as a trunk port, and configure it to permit all VLANs.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan all
```

Enable MVRP on port GigabitEthernet 1/0/1.

```
[DeviceA-GigabitEthernet1/0/1] mvrp enable
[DeviceA-GigabitEthernet1/0/1] quit
```

Configure port GigabitEthernet1/0/2 as a trunk port, and configure it to permit VLAN 40.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 40
```

Enable MVRP on port GigabitEthernet1/0/2.

```
[DeviceA-GigabitEthernet1/0/2] mvrp enable
[DeviceA-GigabitEthernet1/0/2] quit
```

Configure port GigabitEthernet 1/0/3 as a trunk port, and configure it to permit all VLANs.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan all
```

Enable MVRP on port GigabitEthernet 1/0/3.

```
[DeviceA-GigabitEthernet1/0/3] mvrp enable
[DeviceA-GigabitEthernet1/0/3] quit
```

Create VLAN 10.

```
[DeviceA] vlan 10
[DeviceA-vlan10] quit
```

Configuring Device B

Enter MST region view.

```
<DeviceB> system-view
[DeviceB] stp region-configuration
```

Configure the MST region name, VLAN-to-instance mappings, and revision level.

```
[DeviceB-mst-region] region-name example
[DeviceB-mst-region] instance 1 vlan 10
[DeviceB-mst-region] instance 2 vlan 20
[DeviceB-mst-region] revision-level 0
```

Manually activate the MST region configuration.

```
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

Configure Device B as the primary root bridge of MSTI 2.

```
[DeviceB] stp instance 2 root primary
```

Globally enable the spanning tree feature.

```
[DeviceB] stp enable
```

Globally enable MVRP.

```
[DeviceB] mvrp global enable
```

Configure port GigabitEthernet 1/0/1 as a trunk port, and configure it to permit VLANs 20 and 40.

```
[DeviceB] interface gigabitethernet 1/0/1
```

```
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 20 40
```

Enable MVRP on port GigabitEthernet 1/0/1.

```
[DeviceB-GigabitEthernet1/0/1] mvrp enable
[DeviceB-GigabitEthernet1/0/1] quit
```

Configure port GigabitEthernet1/0/2 as a trunk port, and configure it to permit all VLANs.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan all
```

Enable MVRP on port GigabitEthernet1/0/2.

```
[DeviceB-GigabitEthernet1/0/2] mvrp enable
[DeviceB-GigabitEthernet1/0/2] quit
```

Configure port GigabitEthernet 1/0/3 as a trunk port, and configure it to permit all VLANs.

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan all
```

Enable MVRP on port GigabitEthernet 1/0/3.

```
[DeviceB-GigabitEthernet1/0/3] mvrp enable
[DeviceB-GigabitEthernet1/0/3] quit
```

Create VLAN 20.

```
[DeviceB] vlan 20
[DeviceB-vlan20] quit
```

Configuring Device C

Enter MST region view.

```
<DeviceC> system-view
[DeviceC] stp region-configuration
```

Configure the MST region name, VLAN-to-instance mappings, and revision level.

```
[DeviceC-mst-region] region-name example
[DeviceC-mst-region] instance 1 vlan 10
[DeviceC-mst-region] instance 2 vlan 20
[DeviceC-mst-region] revision-level 0
```

Manually activate the MST region configuration.

```
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

Configure Device C as the root bridge of MSTI 0.

```
[DeviceC] stp instance 0 root primary
```

Globally enable the spanning tree feature.

```
[DeviceC] stp enable
```

Globally enable MVRP.

```
[DeviceC] mvrp global enable
```

Configure port GigabitEthernet 1/0/1 as a trunk port, and configure it to permit all VLANs.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan all
```

Enable MVRP on port GigabitEthernet 1/0/1.

```
[DeviceC-GigabitEthernet1/0/1] mvrp enable
[DeviceC-GigabitEthernet1/0/1] quit
```

Configure port GigabitEthernet1/0/2 as a trunk port, and configure it to permit all VLANs.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan all
```

Enable MVRP on port GigabitEthernet1/0/2.

```
[DeviceC-GigabitEthernet1/0/2] mvrp enable
[DeviceC-GigabitEthernet1/0/2] quit
```

Configuring Device D

Enter MST region view.

```
<DeviceD> system-view
[DeviceD] stp region-configuration
```

Configure the MST region name, VLAN-to-instance mappings, and revision level.

```
[DeviceD-mst-region] region-name example
[DeviceD-mst-region] instance 1 vlan 10
[DeviceD-mst-region] instance 2 vlan 20
[DeviceD-mst-region] revision-level 0
```

Manually activate the MST region configuration.

```
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

Globally enable the spanning tree feature.

```
[DeviceD] stp enable
```

Globally enable MVRP.

```
[DeviceD] mvrp global enable
```

Configure port GigabitEthernet 1/0/1 as a trunk port, and configure it to permit VLANs 20 and 40.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 20 40
```

Enable MVRP on port GigabitEthernet 1/0/1.

```
[DeviceD-GigabitEthernet1/0/1] mvrp enable
[DeviceD-GigabitEthernet1/0/1] quit
```

Configure port GigabitEthernet1/0/2 as a trunk port, and configure it to permit VLAN 40.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 40
```

Enable MVRP on port GigabitEthernet1/0/2.

```
[DeviceD-GigabitEthernet1/0/2] mvrp enable[DeviceD-GigabitEthernet1/0/2] quit
```

Verifying the configuration

1. Verify the normal registration mode configuration.

   Use the **display mvrp running-status** command to display the local MVRP VLAN information to verify whether the configuration takes effect.

   # Check the local VLAN information on Device A.

   ```
   [DeviceA] display mvrp running-status
    -------[MVRP Global Info]-------
   ```

```
 Global Status     : Enabled
 Compliance-GVRP   : False

 ----[GigabitEthernet1/0/1]----
 Config  Status                     : Enabled
 Running Status                     : Enabled
 Join Timer                         : 20 (centiseconds)
 Leave Timer                        : 60 (centiseconds)
 Periodic Timer                     : 100 (centiseconds)
 LeaveAll Timer                     : 1000 (centiseconds)
 Registration Type                  : Normal
 Local VLANs :
  1(default),

 ----[GigabitEthernet1/0/2]----
 Config  Status                     : Enabled
 Running Status                     : Enabled
 Join Timer                         : 20 (centiseconds)
 Leave Timer                        : 60 (centiseconds)
 Periodic Timer                     : 100 (centiseconds)
 LeaveAll Timer                     : 1000 (centiseconds)
 Registration Type                  : Normal
 Local VLANs :
  1(default),

 ----[GigabitEthernet1/0/3]----
 Config  Status                     : Enabled
 Running Status                     : Enabled
 Join Timer                         : 20 (centiseconds)
 Leave Timer                        : 60 (centiseconds)
 Periodic Timer                     : 100 (centiseconds)
 LeaveAll Timer                     : 1000 (centiseconds)
 Registration Type                  : Normal
 Local VLANs :
  1(default), 20,
```

The output shows that: ports GigabitEthernet 1/0/1 and GigabitEthernet1/0/2 have learned only VLAN 1 through MVRP; port GigabitEthernet 1/0/3 has learned VLAN 1 and dynamic VLAN 20 created on Device B through MVRP.

Check the local VLAN information on Device B.

```
[DeviceB] display mvrp running-status
 -------[MVRP Global Info]-------
 Global Status     : Enabled
 Compliance-GVRP   : False

 ----[GigabitEthernet1/0/1]----
 Config  Status                     : Enabled
 Running Status                     : Enabled
 Join Timer                         : 20 (centiseconds)
 Leave Timer                        : 60 (centiseconds)
```

```
 Periodic Timer                    : 100 (centiseconds)
 LeaveAll Timer                    : 1000 (centiseconds)
 Registration Type                 : Normal
 Local VLANs :
  1(default),

 ----[GigabitEthernet1/0/2]----
 Config  Status                    : Enabled
 Running Status                    : Enabled
 Join Timer                        : 20 (centiseconds)
 Leave Timer                       : 60 (centiseconds)
 Periodic Timer                    : 100 (centiseconds)
 LeaveAll Timer                    : 1000 (centiseconds)
 Registration Type                 : Normal
 Local VLANs :
  1(default), 10,

 ----[GigabitEthernet1/0/3]----
 Config  Status                    : Enabled
 Running Status                    : Enabled
 Join Timer                        : 20 (centiseconds)
 Leave Timer                       : 60 (centiseconds)
 Periodic Timer                    : 100 (centiseconds)
 LeaveAll Timer                    : 1000 (centiseconds)
 Registration Type                 : Normal
 Local VLANs :
  1(default), 10,
```

The output shows that: port GigabitEthernet 1/0/1 has learned only VLAN 1 through MVRP; ports GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 have learned VLAN 1 and dynamic VLAN 10 created on Device A through MVRP.

Check the local VLAN information on Device C.

```
[DeviceC] display mvrp running-status
 -------[MVRP Global Info]-------
 Global Status     : Enabled
 Compliance-GVRP   : False

 ----[GigabitEthernet1/0/1]----
 Config  Status                    : Enabled
 Running Status                    : Enabled
 Join Timer                        : 20 (centiseconds)
 Leave Timer                       : 60 (centiseconds)
 Periodic Timer                    : 100 (centiseconds)
 LeaveAll Timer                    : 1000 (centiseconds)
 Registration Type                 : Normal
 Local VLANs :
  1(default), 10, 20,

 ----[GigabitEthernet1/0/2]----
 Config  Status                    : Enabled
```

```
 Running Status                    : Enabled
 Join Timer                        : 20 (centiseconds)
 Leave Timer                       : 60 (centiseconds)
 Periodic Timer                    : 100 (centiseconds)
 LeaveAll Timer                    : 1000 (centiseconds)
 Registration Type                 : Normal
 Local VLANs :
  1(default), 20,
```

The output shows that: port GigabitEthernet 1/0/1 has learned VLAN 1, dynamic VLAN 10 created on Device A, and dynamic VLAN 20 created on Device B through MVRP; port GigabitEthernet1/0/2 has learned VLAN 1 and dynamic VLAN 20 created on Device B through MVRP.

Check the local VLAN information on Device D.

```
[DeviceD] display mvrp running-status
 -------[MVRP Global Info]-------
 Global Status     : Enabled
 Compliance-GVRP   : False

 ----[GigabitEthernet1/0/1]----
 Config  Status                    : Enabled
 Running Status                    : Enabled
 Join Timer                        : 20 (centiseconds)
 Leave Timer                       : 60 (centiseconds)
 Periodic Timer                    : 100 (centiseconds)
 LeaveAll Timer                    : 1000 (centiseconds)
 Registration Type                 : Normal
 Local VLANs :
  1(default), 20,

 ----[GigabitEthernet1/0/2]----
 Config  Status                    : Enabled
 Running Status                    : Enabled
 Join Timer                        : 20 (centiseconds)
 Leave Timer                       : 60 (centiseconds)
 Periodic Timer                    : 100 (centiseconds)
 LeaveAll Timer                    : 1000 (centiseconds)
 Registration Type                 : Normal
 Local VLANs :
  1(default),
```

The output shows that: port GigabitEthernet 1/0/1 has learned VLAN 1 and dynamic VLAN 20 created on Device B through MVRP; port GigabitEthernet1/0/2 has learned only VLAN 1 through MVRP.

2. Change the registration mode and verify the configuration.

   Set the MVRP registration mode to fixed on GigabitEthernet 1/0/3 of Device B, so that the dynamic VLANs that Device B learns in VLAN 1 are not de-registered.

   # Set the MVRP registration mode to fixed on GigabitEthernet 1/0/3.

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] mvrp registration fixed
[DeviceB-GigabitEthernet1/0/3] quit
```

Display the local MVRP VLAN information on GigabitEthernet 1/0/3.

```
[DeviceB] display mvrp running-status interface gigabitethernet 1/0/3
 -------[MVRP Global Info]-------
 Global Status     : Enabled
 Compliance-GVRP   : False

 ----[GigabitEthernet1/0/3]----
 Config  Status                        : Enabled
 Running Status                        : Enabled
 Join Timer                            : 20 (centiseconds)
 Leave Timer                           : 60 (centiseconds)
 Periodic Timer                        : 100 (centiseconds)
 LeaveAll Timer                        : 1000 (centiseconds)
 Registration Type                     : Fixed
 Local VLANs :
  1(default), 10,
```

The output shows that the VLAN information on GigabitEthernet 1/0/3 is not changed after you set the MVRP registration mode to fixed on GigabitEthernet 1/0/3.

Delete VLAN 10 on Device A.

```
[DeviceA] undo vlan 10
```

Display the local MVRP VLAN information on GigabitEthernet 1/0/3.

```
[DeviceB] display mvrp running-status interface gigabitethernet 1/0/3
 -------[MVRP Global Info]-------
 Global Status     : Enabled
 Compliance-GVRP   : False

 ----[GigabitEthernet1/0/3]----
 Config  Status                        : Enabled
 Running Status                        : Enabled
 Join Timer                            : 20 (centiseconds)
 Leave Timer                           : 60 (centiseconds)
 Periodic Timer                        : 100 (centiseconds)
 LeaveAll Timer                        : 1000 (centiseconds)
 Registration Type                     : Fixed
 Local VLANs :
  1(default), 10,
```

The output shows that the dynamic VLAN information on GigabitEthernet 1/0/3 is not changed after you set the MVRP registration mode to fixed on GigabitEthernet 1/0/3.

Command reference

display mvrp running-status

Use **display mvrp running-status** to display the MVRP running status.

Syntax

display mvrp running-status [**interface** *interface-list*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

interface *interface-list*: Specifies an Ethernet interface list in the form of *interface-list* = { *interface-type interface-number1* [**to** *interface-type interface-number2*] }&<1-10>, where *interface-type interface-number* specifies an interface by its type and number and &<1-10> indicates that you can specify up to 10 *interface-type interface-number1* [**to** *interface-type interface-number2*] parameters. If this option is not specified, this command displays MVRP running status of all MVRP-enabled trunk ports.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Examples

Display the MVRP running status of all ports.

```
<Sysname> display mvrp running-status
 -------[MVRP Global Info]-------
 Global Status     : Enabled
 Compliance-GVRP   : False

 ----[GigabitEthernet1/0/1]----
 Config  Status                    : Enabled
 Running Status                    : Enabled
 Join Timer                        : 20 (centiseconds)
 Leave Timer                       : 60 (centiseconds)
 Periodic Timer                    : 100 (centiseconds)
 LeaveAll Timer                    : 1000 (centiseconds)
 Registration Type                 : Normal
 Local VLANs :
  1(default), 2-10,
```

Table 18 Command output

Field	Description
MVRP Global Info	Global MVRP information.
Global Status	Global MVRP status: • Enabled • Disabled
Compliance-GVRP	GVRP compatibility status: • **True**—Compatible • **False**—Incompatible

Field	Description
----[GigabitEthernet1/0/1] ----	Interface prompt. The information between the current interface prompt and the next interface prompt is information about the current interface.
Config Status	Whether MVRP is enabled on the port: • Enabled • Disabled
Running Status	Whether MVRP takes effect on the port (determined by the link state and MVRP enabling status of the port): • Enabled • Disabled
Join Timer	Join timer, in centiseconds.
Leave Timer	Leave timer, in centiseconds.
Periodic Timer	Periodic timer, in centiseconds.
LeaveAll Timer	LeaveAll timer, in centiseconds.
Registration Type	MVRP registration mode: • Fixed • Forbidden • Normal
Local VLANs	VLAN information in the local database, which displays the VLANs learned through MVRP.

display mvrp state

Use **display mvrp state** to display the MVRP state of an interface in a VLAN.

Syntax

display mvrp state interface *interface-type interface-number* **vlan** *vlan-id* [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

0: Visit level

Parameters

interface *interface-type interface-number*: Displays the MVRP state of an interface specified by its type and number.

vlan *vlan-id*: Displays the MVRP state of an interface in an VLAN specified by its VLAN ID, which ranges from 1 to 4094.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Examples

Display the MVRP state of port GigabitEthernet 1/0/1 in VLAN 2.

```
<Sysname> display mvrp state interface gigabitethernet 1/0/1 vlan 2
MVRP state of VLAN 2 on port GE1/0/1
    Port      VLAN   App-state   Reg-state
 ----------- ------ ----------- -----------
 GE1/0/1         2       VP          IN
```

Table 19 Command output

Field	Description
MVRP state of VLAN 2 on port GE1/0/1	MVRP state of GigabitEthernet 1/0/1 in VLAN 2.
App-state	Declaration state, which indicates the state of the attribute that the local participant declares to the remote participant. The state can be VO, VP, VN, AN, AA, QA, LA, AO, QO, AP, QP, or LO. Each state consists of two letters. The first letter indicates the state: • **V**—Very anxious, which means that the local participant has not declared the attribute or has not received any Join message containing the attribute. • **A**—Anxious, which means that the local participant has declared the attribute once or has received one Join message containing the attribute. • **Q**—Quiet, which means that the local participant has declared the attribute two times, the local participant has declared the attribute once and has received one Join message containing the attribute, or the local participant has received two Join messages containing the attribute. • **L**—Leaving, which means that the local participant is deregistering the attribute. The second letter indicates the membership state: • **A**—Active member, which means that the local participant is declaring the attribute, has sent at least one Join message containing the attribute, and may receive Join messages. • **P**—Passive member, which means that the local participant is declaring the attribute, has received Join messages containing the attribute, but has not sent Join messages containing the attribute. • **O**—Observer, which means that the local participant is not declaring the attribute but is monitoring the attribute. • **N**—New, which means that the local participant is declaring the attribute, is receiving the Join message containing the attribute, but is not sending Join messages for the attribute. For example, VP indicates "Very anxious, Passive member".
Reg-state	Registration state of attributes declared by remote participants on the local end. The state can be IN, LV, or MT: • **IN**—Registered. • **LV**—Previously registered, but now being timed out. • **MT**—Not registered.

display mvrp statistics

Use **display mvrp statistics** to display MVRP statistics.

Syntax

display mvrp statistics [**interface** *interface-list*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

interface *interface-list*: Specifies an Ethernet interface list in the form of *interface-list* = { *interface-type* *interface-number1* [**to** *interface-type* *interface-number2*] }&<1-10>, where *interface-type interface-number* specifies an interface by its type and number and &<1-10> indicates that you can specify up to 10 interfaces or interface ranges. If this option is not specified, this command displays MVRP statistics of all MVRP-enabled trunk ports.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Examples

Display MVRP statistics of all MVRP-enabled ports.

```
<Sysname> display mvrp statistics

 ----[GigabitEthernet1/0/1]----
 Failed Registrations           : 1
 Last PDU Origin                : 000f-e200-0010
 Frames Received                : 201
  New Event Received                 : 0
  JoinIn Event Received              : 1167
  In Event Received                  : 0
  JoinMt Event Received              : 22387
  Mt Event Received                  : 31
  Leave Event Received               : 210
  LeaveAll Event Received            : 63
 Frames Transmitted             : 47
  New Event Transmitted              : 0
  JoinIn Event Transmitted           : 311
  In Event Transmitted               : 0
  JoinMt Event Transmitted           : 873
  Mt Event Transmitted               : 11065
  Leave Event Transmitted            : 167
  LeaveAll Event Transmitted         : 4
 Frames Discarded               : 0

 ----[GigabitEthernet1/0/2]----
 Failed Registrations           : 0
 Last PDU Origin                : 0000-0000-0000
 Frames Received                : 0
  New Event Received                 : 0
```

```
  JoinIn Event Received           : 0
  In Event Received               : 0
  JoinMt Event Received           : 0
  Mt Event Received               : 0
  Leave Event Received            : 0
  LeaveAll Event Received         : 0
 Frames Transmitted          : 0
  New Event Transmitted           : 0
  JoinIn Event Transmitted        : 0
  In Event Transmitted            : 0
  JoinMt Event Transmitted        : 0
  Mt Event Transmitted            : 0
  Leave Event Transmitted         : 0
  LeaveAll Event Transmitted      : 0
 Frames Discarded            : 0
```

Table 20 Command output

Field	Description
----[GigabitEthernet1/0/1]----	Interface prompt. The statistics between the current interface prompt and the next interface prompt are statistics of the current interface.
Failed Registrations	Number of VLAN registration failures through MVRP on the local end.
Last PDU Origin	Source MAC address of the last MVRP PDU.
Frames Received	Number of MVRP protocol packets received
New Event Received	Number of New attribute events received.
JoinIn Event Received	Number of JoinIn attribute events received.
In Event Received	Number of In attribute events received.
JoinMt Event Received	Number of JoinMt attribute events received.
Mt Event Received	Number of Mt attribute events received.
Leave Event Received	Number of Leave attribute events received.
LeaveAll Event Received	Number of LeaveAll attribute events received.
Frames Transmitted	Number of MVRP protocol packets sent.
New Event Transmitted	Number of New attribute events sent.
JoinIn Event Transmitted	Number of JoinIn attribute events sent.
In Event Transmitted	Number of In attribute events sent.
JoinMt Event Transmitted	Number of JoinMt attribute events sent.
Mt Event Transmitted	Number of Mt attribute events sent.
Leave Event Transmitted	Number of Leave attribute events sent.
LeaveAll Event Transmitted	Number of LeaveAll attribute events sent.
Frames Discarded	Number of MVRP protocol packets dropped.

display mvrp vlan-operation

Use **display mvrp vlan-operation** to display the dynamic VLAN operations of an interface.

Syntax

display mvrp vlan-operation interface *interface-type interface-number* [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

0: Visit level

Parameters

interface *interface-type interface-number*: Displays the dynamic VLAN operations of an interface specified its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Usage guidelines

These dynamic VLANs refer to the VLANs that are dynamically learned through MVRP and have not taken effect on the local device.

If a dynamic VLAN learned through MVRP is an existing static VLAN on the device or a VLAN reserved for a protocol, the dynamic VLAN does not take effect on the local device.

Examples

Display the dynamic VLAN operations of GigabitEthernet 1/0/1.

```
<Sysname> display mvrp vlan-operation interface gigabitethernet 1/0/1
 Dynamic VLAN operations on port GigabitEthernet1/0/1
  Operations of creating VLAN:  2-100
  Operations of deleting VLAN:  none
  Operations of adding VLAN to Trunk:  2-100
  Operations of deleting VLAN from Trunk:  none
```

Table 21 Command output

Field	Description
Operations of adding VLAN to Trunk	Operations of adding VLANs to trunk ports
Operations of deleting VLAN from Trunk	Operations of removing VLAN from trunk ports

mrp timer join

Use **mrp timer join** to set the Join timer.

Use **undo mrp timer join** to restore the default.

Syntax

mrp timer join *timer-value*

undo mrp timer join

Default

The Join timer is 20 centiseconds.

Views

Layer 2 Ethernet port view, Layer 2 aggregate interface view, port group view

Default command level

2: System level

Parameters

timer-value: Specifies the Join timer value (in centiseconds). The Join timer must be less than half the Leave timer, and must be a multiple of 20.

Usage guidelines

You will fail to restore the default Join timer if the default Join timer is not less than half the Leave timer.

Examples

Set the Join timer to 40 centiseconds. (Suppose the Leave timer is 100 centiseconds)

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/1
[Sysname-GigabitEthernet1/0/1] mrp timer join 40
```

Related commands

- **display mvrp running-status**
- **mrp timer leave**

mrp timer leave

Use **mrp timer leave** to set the Leave timer.

Use **undo mrp timer leave** to restore the default.

Syntax

mrp timer leave *timer-value*

undo mrp timer leave

Default

The Leave timer is 60 centiseconds.

Views

Layer 2 Ethernet port view, Layer 2 aggregate interface view, port group view

Default command level

2: System level

Parameters

timer-value: Specifies the Leave timer value (in centiseconds). The Leave timer must be greater than two times the Join timer, less than the LeaveAll timer, and a multiple of 20.

Usage guidelines

You will fail to restore the default Leave timer if the default Leave timer is not greater than two times the Join timer or not less than the LeaveAll timer.

Examples

Set the Leave timer to 100 centiseconds. (Suppose the Join and LeaveAll timer use their default settings)

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mrp timer leave 100
```

Related commands

- **display mvrp running-status**
- **mrp timer join**
- **mrp timer leaveall**

mrp timer leaveall

Use **mrp timer leaveall** to set the LeaveAll timer.

Use **undo mrp timer leaveall** to restore the default.

Syntax

mrp timer leaveall *timer-value*

undo mrp timer leaveall

Default

The LeaveAll timer is 1000 centiseconds.

Views

Layer 2 Ethernet port view, Layer 2 aggregate interface view, port group view

Default command level

2: System level

Parameter

timer-value: Specifies the LeaveAll timer value (in centiseconds). The LeaveAll timer must be greater than any Leave timer on each port, no greater than 32760, and a multiple of 20.

Usage guidelines

You will fail to restore the default LeaveAll timer if the default LeaveAll timer is not greater than any Leave timer on each port.

Each time when the LeaveAll timer of a port expires, all attributes of the MSTIs on the port are deregistered throughout the network, and such a deregistration affects a large portion of the network. Do not set too small a value for the LeaveAll timer, and make sure that the LeaveAll timer is greater than any Leave timer on each port.

To keep the dynamic VLANs learned through MVRP stable, do not set the LeaveAll timer smaller than its default value (1000 centiseconds).

To avoid the case that the LeaveAll timer of a fixed participant always first expires, the switch randomly changes the LeaveAll timer within a certain range when the MRP participant restarts its LeaveAll timer.

Examples

Set the LeaveAll timer to 1500 centiseconds. (Suppose the Leave timer is restored to the default)

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mrp timer leaveall 1500
```

Related commands

- **display mvrp running-status**
- **mrp timer leave**

mrp timer periodic

Use **mrp timer periodic** to set the Periodic timer.

Use **undo mrp timer periodic** to restore the default.

Syntax

mrp timer periodic *timer-value*

undo mrp timer periodic

Default

The Periodic timer is 100 centiseconds.

Views

Layer 2 Ethernet port view, Layer 2 aggregate interface view, port group view

Default command level

2: System level

Parameters

timer-value: Specifies the Periodic timer (in centiseconds), which can be 0 or 100.

Usage guidelines

Setting the Periodic timer to 0 centiseconds disables the Periodic timer.

Setting the Periodic timer to 100 centiseconds enables the Periodic timer.

Examples

Set the Periodic timer to 0 centiseconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mrp timer periodic 0
```

Related commands

display mvrp running-status

mvrp global enable

Use **mvrp global enable** to enable MVRP globally.

Use **undo mvrp global enable** to restore the default.

Syntax

mvrp global enable

undo mvrp global enable

Default

MVRP is disabled globally.

Views

System view

Default command level

2: System level

Usage guidelines

Disabling MVRP globally also disables MVRP on all ports.

Examples

Enable MVRP globally.

```
<Sysname> system-view
[Sysname] mvrp global enable
```

Related commands

- **display mvrp running-status**
- **mvrp enable**

mvrp enable

Use **mvrp enable** to enable MVRP on a port.

Use **undo mvrp enable** to disable MVRP on a port.

Syntax

mvrp enable

undo mvrp enable

Default

MVRP is disabled on a port.

Views

Layer 2 Ethernet port view, Layer 2 aggregate interface view, port group view

Default command level

2: System level

Usage guidelines

To enable MVRP on a port, first enable MVRP globally.

Disabling MVRP globally also disables MVRP on each port.

This command is available only on trunk ports.

You cannot change the link type of MVRP-enabled trunk port.

Examples

Configure GigabitEthernet 1/0/1 as a trunk port, and enable MVRP on it.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk permit vlan all
[Sysname-GigabitEthernet1/0/1] mvrp enable
```

Related commands

- **display mvrp running-status**
- **mvrp global enable**

mvrp gvrp-compliance

Use **mvrp gvrp-compliance enable** to enable GVRP compatibility, so that the device can process both MVRP protocol packets and GVRP protocol packets.

Use **undo mvrp gvrp-compliance enable** to restore the default.

Syntax

mvrp gvrp-compliance enable

undo mvrp gvrp-compliance enable

Default

GVRP compatibility is disabled.

Views

System view

Default command level

2: System level

Examples

Enable GVRP compatibility.

```
<Sysname> system-view
[Sysname] mvrp gvrp-compliance enable
```

mvrp registration

Use **mvrp registration** to set the MVRP registration mode on the port.

Use **undo mvrp registration** to restore the default.

Syntax

mvrp registration { **fixed | forbidden | normal** }

undo mvrp registration

Default

The MVRP registration mode is normal.

Views

Layer 2 Ethernet port view, Layer 2 aggregate interface view, port group view

Default command level

2: System level

Parameters

fixed: Specifies the fixed registration mode.

forbidden: Specifies the forbidden registration mode.

normal: Specifies the normal registration mode.

Usage guidelines

This command is available only on trunk ports.

Examples

Configure GigabitEthernet 1/0/1 as a trunk port, and set the MVRP registration mode to fixed on the port.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk permit vlan all
[Sysname-GigabitEthernet1/0/1] mvrp registration fixed
```

Related commands

display mvrp running-status

reset mvrp statistics

Use **reset mvrp statistics** to clear the MVRP statistics of ports.

Syntax

reset mvrp statistics [**interface** *interface-list*]

Views

User view

Default command level

2: System level

Parameters

interface *interface-list*: Specifies an Ethernet interface list in the form of *interface-list* = { *interface-type interface-number1* [**to** *interface-type interface-number2*] }<1-10>, where *interface-type interface-number* specifies an interface by its type and number and <1-10> indicates that you can specify up to 10 interfaces or interface ranges. If this option is not specified, the command clears MVRP statistics of all ports.

Examples

Clear the MVRP statistics of all ports.

```
<Sysname> reset mvrp statistics
```

Related commands

display mvrp statistics

New feature: Enabling LLDP to automatically discover IP phones

Overview

In a traditional voice VLAN network, the switch maps the source MAC addresses of IP phones to a limited number of OUI addresses to allow them to access the network. This method restricts the types of IP phones on the network, if the IP phones with the source MAC addresses match the same OUI address are categorized as a type.

To break the restriction, you can enable the switch to automatically discover IP phones through LLDP. With this function, the switch can automatically discover the peer, and exchange LLDP TLVs with the peer. If the LLDP System Capabilities TLV received on a port shows that the peer is phone capable, the switch determines that the peer is an IP phone and sends an LLDP TLV carrying the voice VLAN configuration to the peer.

When the IP phone discovery process is complete, the port will automatically join the voice VLAN and improve the transmission priority of the voice traffic for the IP phone. To ensure that the IP phone can pass authentication, the switch will add the MAC address of the IP phone to the MAC address table.

NOTE:

- This function is available only when your IP phone supports LLDP. Identify whether your IP phone supports LLDP by checking its usage guide.
- For more information about voice VLANs, see the chapter "Voice VLAN configuration."

Configuration prerequisites

Before you enable the switch to automatically discover IP phones through LLDP, complete the following tasks:

- Enable LLDP globally and on ports.
- Configure voice VLANs.

Configuration procedure

Follow these steps to enable LLDP to automatically discover IP phones:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable LLDP to automatically discover IP phones	**voice vlan track lldp**	Required Disabled by default.

IMPORTANT:

- When the switch is enabled to automatically discover IP phones through LLDP, you can connect at most five IP phones to each port of the switch.
- You cannot use this function together with CDP compatibility.

Command reference

voice vlan track lldp

Use the **voice vlan track lldp** command to enable LLDP to automatically discover IP phones.

Use the **undo voice vlan track lldp** command to disable LLDP from automatically discovering IP phones.

Syntax

voice vlan track lldp

undo voice vlan track lldp

Default

LLDP is disabled from automatically discovering IP phones.

Views

System view

Default command level

2: System level

Examples

Enable the switch to automatically discover IP phones through LLDP.

```
<Sysname> system-view
[Sysname] voice vlan track lldp
```

A5500EI-CMW520-R2210

This release has the following changes:

- New feature: Displaying information about the patch package
- New feature: Displaying alarm information
- New feature: Configuring jumbo frame support on an Ethernet interface
- New feature: Restoring the default settings for the interface
- New feature: Configuring the link mode of Ethernet interfaces in system view
- New feature: Enabling MAC address roaming
- New feature: Configuring a Layer 3 aggregation group
- New feature: Configuring the MTU of a Layer 3 aggregate interface
- New feature: Assigning the port an aggregation priority
- New feature: Setting the minimum number of Selected ports for an aggregation group
- New feature: PVST
- New feature: Configuring TC snooping
- New feature: Setting the MTU for the VLAN interface
- New feature: Assigning an IPv6 address and enabling local proxy ND on a super VLAN interface
- New feature: Restoring the default operating mode of CDP-compatible LLDP
- New feature: PoE power negotiation through Power Via MDI TLV
- New feature: Configuring multicast ARP
- New feature: Specifying the IP address range for the DHCP clients of a specified vendor
- New feature: Specifying a server's IP address for the DHCP client
- New feature: Configuring DHCP packet rate limit
- New feature: Configuring DHCP snooping support for sub-option 9 in Option 82
- New feature: Configuring TCP path MTU discovery
- New feature: local ND proxy
- New feature: Specifying the AFTR address
- New feature: Enabling dropping of IPv6 packets using IPv4-compatible IPv6 addresses
- New feature: Displaying detailed information about neighbors
- New feature: Displaying IPv6 PMTU information for the specified VPN
- New feature: Configuring a static neighbor entry for a private network
- New feature: Configuring a static PMTU for a private network
- New feature: Displaying neighbor information for a specified VPN
- New feature: Configuring the interface as an uplink interface and disabling it from learning ND snooping entries
- New feature: Configuring permanent static route
- New feature: Enabling OSPF ISPF
- New feature: Enabling OSPF to calculate default routes received from other routers
- New feature: Assigning a high priority to IS-IS routes
- New feature: Enabling 4-byte AS number suppression

- New feature: Configuring BFD for OSPFv3
- New feature: Configuring BFD for IPv6 IS-IS
- New feature: Configuring BFD for IPv6 BGP
- New feature: Specifying a community list name to match IPv6 BGP routing information
- New feature: IPv6 MCE
- New feature: Configuring IPv6 routing protocols to support VPN instances
- New feature: Enabling the IGMP snooping & MLD snooping host tracking function
- New feature: Configuring IGMP & MLD fast-leave processing
- New feature: PIM snooping & IPv6 PIM snooping
- New feature: Configuring PIM & IPv6 PIM to work with BFD
- New feature: Configuring an MD5 authentication key for the TCP connection to be established with an MSDP peer
- New feature: Enabling the IGMP & MLD host tracking function
- New feature: Configuring rule range remark
- New feature: Configuring routing header type for an IPv6 ACL rule
- New feature: Configuring an IPv6 VPN in an IPv6 ACL rule
- New feature: Configuring byte-count or packet-based WFQ queuing
- New feature: Configuring SP+WFQ queuing
- New feature: Setting the validity time of the local user
- New feature: Specifying the local user as a guest or guest manager
- New feature: Setting the guest attribute for a user group
- New feature: Authorizing a local user to use the Web service
- New feature: Specifying ciphertext shared keys for RADIUS/HWTACACS servers
- New feature: Specifying supported domain name delimiters
- New feature: Enabling inactivity aging
- New feature: Enabling the dynamic secure MAC function
- New feature: Establishing a connection between a client to a VPN-specific IPv6 Stelnet server
- New feature: Establishing a connection between a client to a VPN-specific IPv6 SFTP server
- New feature: Enabling SSL client weak authentication
- New feature: Setting the maximum number of IPv4/IPv6 source guard binding entries
- New feature: Loose URPF check
- New feature: SAVI
- New feature: Blacklist
- New feature: Enabling Ethernet OAM remote loopback in user view and system view
- New feature: Restoring the default Ethernet OAM connection mode
- New feature: Configuring the collaboration between Smart Link and CC of CFD
- New feature: Configuring the VF tracking function to monitor an AVF
- New feature: CWMP
- Modified feature: Improving the isolate-user-VLAN usability
- Modified feature: Using the device to log in to a Telnet server
- Modified feature: Logging in to the FTP server from user view
- Modified feature: Downloading or uploading a file in an IPv6 network

New feature: Displaying information about the patch package

Displaying information about the patch package

For more information about displaying information about the patch package, see "Software upgrade configuration" in *HP A5500 EI & A5500 SI Switch Series Fundamentals Configuration Guide-Release 2210*.

Command reference

New commands: **display patch**.

For more information about this command, see "Software upgrade commands" in *HP A5500 EI & A5500 SI Switch Series Fundamentals Command Reference-Release 2210*.

New feature: Displaying alarm information

Displaying alarm information

For more information about displaying alarm information, see "Device management configuration" in *HP A5500 EI & A5500 SI Switch Series Fundamentals Configuration Guide-Release 2210*.

Command reference

New commands: **display alarm**.

For more information about this command, see "Device management commands" in *HP A5500 EI & A5500 SI Switch Series Fundamentals Command Reference-Release 2210*.

New feature: Configuring jumbo frame support on an Ethernet interface

Configuring jumbo frame support on an Ethernet interface

For more information about jumbo frame support configuration, see "Ethernet interface configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 2—LAN Switching Configuration Guide-Release 2210*.

Command reference

Modified command: The *value* argument was added to the **jumboframe enable** command.

For more information about this command, see "Ethernet interface configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 2—LAN Switching Command Reference-Release 2210*.

New feature: Restoring the default settings for the interface

Restoring the default settings for the interface

For more information about restoring the default settings for the interface configuration, see "Ethernet interface configuration", "Loopback and null interface configuration", "Ethernet link aggregation configuration", and "VLAN configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 2—LAN Switching Configuration Guide-Release 2210* and "Tunneling configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Configuration Guide-Release 2210*.

Command reference

New command: **default**.

For more information about this command, see "Ethernet interface configuration commands", "Loopback and null interface configuration commands", "Ethernet link aggregation configuration commands", and "VLAN configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 2—LAN Switching Command Reference-Release 2210* and "Tunneling configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Command Reference-Release 2210*.

New feature: Configuring the link mode of Ethernet interfaces in system view

Configuring the link mode of Ethernet interfaces in system view

For more information about configuring the link mode of Ethernet interfaces in system view, see "Ethernet interface configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 2—LAN Switching Configuration Guide-Release 2210*.

Command reference

New command: **port link-mode** *interface-list*, which can configure the link mode of Ethernet interfaces in system view.

For more information about this command, see "Ethernet interface configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 2—LAN Switching Command Reference-Release 2210*.

New feature: Enabling MAC address roaming

Enabling MAC address roaming

For more information about MAC address roaming configuration, see "MAC address table configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 2—LAN Switching Configuration Guide-Release 2210*.

Command reference

New command: **mac-address mac-roaming enable**.

For more information about this command, see "MAC address table configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 2—LAN Switching Command Reference-Release 2210*.

New feature: Configuring a Layer 3 aggregation group

Configuring a Layer 3 aggregation group

For more information about the Layer 3 aggregation group configuration, see " Ethernet link aggregation configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 2—LAN Switching Configuration Guide-Release 2210*.

Command reference

New command: **interface route-aggregation**.

Modified commands: The **route-aggregation** keyword was added to the **display interface**, **display link-aggregation load-sharing mode**, **display link-aggregation verbose**, and **reset counters interface** commands.

For more information about these commands, see "Ethernet link aggregation configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 2—LAN Switching Command Reference-Release 2210*.

New feature: Configuring the MTU of a Layer 3 aggregate interface

Configuring the MTU of a Layer 3 aggregate interface

For more information about the MTU of a Layer 3 aggregate interface configuration, see "Ethernet link aggregation configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 2—LAN Switching Configuration Guide-Release 2210*.

Command reference

For more information about the MTU of a Layer 3 aggregate interface configuration commands, see "Ethernet link aggregation configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 2—LAN Switching Command Reference-Release 2210*.

New feature: Assigning the port an aggregation priority

Assigning the port an aggregation priority

For more information about assigning the port an aggregation priority, see "Ethernet link aggregation configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 2—LAN Switching Configuration Guide-Release 2210*.

Command reference

New command: **link-aggregation port-priority**, which applies to dynamic and static aggregation groups.

Deleted command: **lacp port-priority**, which applies to only dynamic aggregation groups.

For more information about this command, see "Ethernet link aggregation configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 2—LAN Switching Command Reference-Release 2210*.

New feature: Setting the minimum number of Selected ports for an aggregation group

Setting the minimum number of Selected ports for an aggregation group

For more information about configuring the minimum number of Selected ports for an aggregation group, see "Ethernet link aggregation configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 2—LAN Switching Configuration Guide-Release 2210*.

Command reference

New command: **link-aggregation selected-port minimum**.

For more information about this command, see "Ethernet link aggregation configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 2—LAN Switching Command Reference-Release 2210*.

New feature: PVST

Configuring PVST

For more information about PVST configuration, see "Spanning tree configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 2—LAN Switching Configuration Guide-Release 2210*.

Command reference

Modified commands:

Keyword **pvst** was added to the **stp mode** command.

Option **vlan** *vlan-list* was added to the following commands:

- **display stp**
- **display stp history**
- **display stp tc**
- **stp bridge-diameter**
- **stp cost**
- **stp enable** (in system view)
- **stp port priority**
- **stp port-log**
- **stp priority**
- **stp root primary**
- **stp root secondary**
- **stp timer forward-delay**
- **stp timer hello**
- **stp timer max-age.**

For more information about PVST configuration commands, see "Spanning tree configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 2—LAN Switching Command Reference-Release 2210*.

New feature: Configuring TC snooping

Configuring TC snooping

For more information about TC snooping configuration, see "Spanning tree configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 2—LAN Switching Configuration Guide-Release 2210*.

Command reference

New command: **stp tc-snooping**.

For more information about this command, see "Spanning tree configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 2—LAN Switching Command Reference-Release 2210*.

New feature: Setting the MTU for the VLAN interface

Setting the MTU for the VLAN interface

For more information about VLAN interface MTU configuration, see "VLAN configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 2—LAN Switching Configuration Guide-Release 2210*.

Command reference

New command: **mtu**.

For more information about this command, see "VLAN configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 2—LAN Switching Command Reference-Release 2210*.

New feature: Assigning an IPv6 address and enabling local proxy ND on a super VLAN interface

Assigning an IPv6 address and enabling local proxy ND on a super VLAN interface

For more information about assigning an IPv6 address and enabling local proxy ND on a super VLAN interface, see "Super VLAN configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 2—LAN Switching Configuration Guide-Release 2210*.

Command reference

Modified commands: The following commands can be configured on the VLAN interface of a super VLAN.

- **ipv6 address**
- **ipv6 address anycast**
- **ipv6 address auto**
- **ipv6 address auto link-local**
- **ipv6 address eui-64**
- **ipv6 address link-local**
- **local-proxy-nd enable**

For more information about these commands, see "IPv6 basics configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Command Reference-Release 2210*.

New feature: Restoring the default operating mode of CDP-compatible LLDP

Restoring the default operating mode of CDP-compatible LLDP

The **undo lldp compliance admin-status cdp** command was added to restore the default operating mode of CDP-compatible LLDP.

For more information about the operating mode of CDP-compatible LLDP, see "LLDP configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 2—LAN Switching Configuration Guide-Release 2210*.

Command reference

New command: **undo lldp compliance admin-status cdp**.

For more information about this command, see "LLDP configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 2—LAN Switching Command Reference-Release 2210*.

New feature: PoE power negotiation through Power Via MDI TLV

Configuring PoE power negotiation through Power Via MDI TLV

NOTE:

This feature is available on only PoE+ capable switches.

The PSE devices that support this feature can autonegotiate the PoE power with the PD device connected to the port.

The feature does not need to be configured at the CLI. To implement the feature, you only need to enable PoE on the PSE device and PoE interface. After you use the **poe max-power** *max-power* command to configure the maximum power of a PoE interface, the configured value takes effect, and the PoE power autonegotiation feature is not supported.

For more information about "PoE configuration", see *HP A5500 EI & A5500 SI Switch Series Network Management and Monitoring Configuration Guide-Release 2210*.

Command reference

You can use the **display lldp local-information** command and the **display lldp neighbor-information** command to view the power autonegotiation state.

Modified command: display lldp local-information

Syntax

display lldp local-information [**global** | **interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Change description

The PoE power autonegotiation information was added to the output.

Display all LLDP information to be sent. (The example describes only the newly added fields in the output.)

```
<Sysname> display lldp local-information
...
LLDP local-information of port 1[GigabitEthernet1/0/1]:
...
```

```
  Power type                 : Type 2 PSE
  Power source               : Primary
  Power priority             : High
  PD requested power value   : 25.5(w)
  PSE allocated power value : 25.5(w)
...
```

Table 1 Command output

Field	Description
Power type	Power type when the device supports PoE+. **Type 2 PSE** supplies power from 0 to 30 W, a voltage from 50 to 57 V, and a maximum current of 600 mA.
Power source	Power supply type of a PSE when the device supports PoE+: • **Unknown**—Unknown power supply. • **Primary**—Primary power supply. • **Backup**—Backup power supply.
Power priority	Power supply priority on a PSE when the device supports PoE+: • **Unknown**—Unknown priority. • **Critical**—Priority 1. • **High**—Priority 2. • **Low**—Priority 3.
PD requested power value	Power (in watts) required by the PD that connects to the port. This field appears only on the devices that support PoE+.
PSE allocated power value	Power (in watts) supplied by the PSE to the connecting port. This field appears only on the devices that support PoE+.

Modified command: display lldp neighbor-information

Syntax

display lldp neighbor-information [**brief** | **interface** *interface-type interface-number* [**brief**] | **list** [**system-name** *system-name*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Change description

The PoE power autonegotiation information was added to the output.

Display the LLDP information sent from the neighboring devices received through all ports. (The example describes only the newly added fields in the output.)

```
<Sysname> display lldp neighbor-information
...
LLDP neighbor-information of port 1[GigabitEthernet1/0/1]:
...
  Power type                 : Type 2 PD
  Power source               : PSE and local
  Power priority             : High
  PD requested power value   : 25.5(w)
  PSE allocated power value : 25.5(w)
...
```

Table 2 Command output

Field	Description
Power type	This field appears only on the devices that support PoE+. PD type of an LLDP neighboring device which is a PD device: • **Type 1 PD**—This type power from 0 to 15.4 W, a voltage from 44 to 57 V, and a maximum current of 350 mA. • **Type 2 PD**—This type requires power from 0 to 30 W, a voltage from 50 to 57 V, and a maximum current of 600 mA.
Power source	This field appears only on the devices that support PoE+. Power source type of an LLDP neighboring device which is a PD device: • **Unknown**—Unknown power supply. • **PSE**—PSE power supply. • **Local**—Local power supply. • **PSE and local**—PSE and local power supply.
Power priority	This field appears only on the devices that support PoE+. Powered priority of ports on an LLDP neighboring device which is a PD device: • **Unknown**—Unknown priority. • **Critical**—Priority 1. • **High**—Priority 2. • **Low**—Priority 3.
PD requested power value	This field appears only on the devices that support PoE+. Power (in watts) requested by the LLDP neighboring device which is a PD device.
PSE allocated power value	This field appears only on the devices that support PoE+. Power (in watts) supplied by the PSE to the LLDP neighboring device which is a PD device.

New feature: Configuring multicast ARP

Configuring multicast ARP

For more information about configuring multicast ARP, see "ARP configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Configuration Guide-Release 2210*.

Command reference

No new command. Use the existing **arp static**, **mac-address multicast**, and **undo arp check enable** commands to implement multicast ARP.

For more information about these commands, see "ARP configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Command Reference-Release 2210*.

New feature: Specifying the IP address range for the DHCP clients of a specified vendor

Specifying the IP address range for the DHCP clients of a specified vendor

For more information about specifying the IP address range for the DHCP clients of a specified vendor, see "DHCP server configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Configuration Guide-Release 2210*.

Command reference

New command: **vendor-class-identifier**.

For more information about this command, see "DHCP server configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Command Reference-Release 2210*.

New feature: Specifying a server's IP address for the DHCP client

Specifying a server's IP address for the DHCP client

For more information about specifying a server's IP address for the DHCP client, see "DHCP server configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Configuration Guide-Release 2210*.

Command reference

New command: **next-server**.

For more information about this command, see "DHCP server configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Command Reference-Release 2210*.

New feature: Configuring DHCP packet rate limit

Configuring DHCP packet rate limit

For more information about configuring DHCP packet rate limit, see "DHCP snooping configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Configuration Guide-Release 2210*.

Command reference

New command: **dhcp-snooping rate-limit**.

For more information about this command, see "DHCP snooping configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Command Reference-Release 2210*.

New feature: Configuring DHCP snooping support for sub-option 9 in Option 82

Configuring DHCP snooping support for sub-option 9 in Option 82

For more information about configuring DHCP snooping support for sub-option 9 in Option 82, see "DHCP snooping configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Configuration Guide-Release 2210*.

Command reference

New command: **dhcp-snooping information sub-option**.

Option **private** *private* and keyword **standard** were added to the **dhcp-snooping information format** command.

Keyword **append** was added to the **dhcp-snooping information strategy** command.

For more information about these commands, see "DHCP snooping configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Command Reference-Release 2210*.

New feature: Configuring TCP path MTU discovery

Configuring TCP path MTU discovery

For more information about configuring TCP path MTU discovery, see "IP Performance Optimization configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Configuration Guide-Release 2210*.

Command reference

New command: **tcp path-mtu-discovery**.

For more information about this command, see "IP performance optimization configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Command Reference-Release 2210*.

New feature: local ND proxy

Configuring local ND proxy

For more information about configuring local ND proxy, see "IPv6 basics configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Configuration Guide-Release 2210*.

Command reference

New command: **local-proxy-nd enable**.

For more information about this command, see "IPv6 basics configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Command Reference-Release 2210*.

New feature: Specifying the AFTR address

Specifying the AFTR address

For more information about specifying the AFTR address, see "DHCPv6 server configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Configuration Guide-Release 2210*.

Command reference

New command: **ds-lite address**.

For more information about this command, see "DHCPv6 configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Command Reference-Release 2210*.

New feature: Enabling dropping of IPv6 packets using IPv4-compatible IPv6 addresses

Enabling dropping of IPv6 packets using IPv4-compatible IPv6 addresses

For more information about enabling dropping of IPv6 packets using IPv4-compatible IPv6 addresses, see "Tunneling configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Configuration Guide-Release 2210*.

Command reference

New command: **tunnel discard ipv4-compatible-packet**.

For more information about this command, see "Tunneling configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Command Reference-Release 2210*.

New feature: Displaying detailed information about neighbors

Displaying detailed information about neighbors

For more information about displaying detailed information about neighbors, see "IPv6 basics configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Configuration Guide-Release 2210*.

Command reference

Keyword **verbose** was added to the **display ipv6 neighbors** command to display detailed information about neighbors.

For more information about this command, see "IPv6 basics configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Command Reference-Release 2210*.

New feature: Displaying IPv6 PMTU information for the specified VPN

Displaying IPv6 PMTU information for the specified VPN

For more information about displaying IPv6 PMTU information for the specified VPN, see "IPv6 basics configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Configuration Guide-Release 2210*.

Command reference

Option **vpn-instance** *vpn-instance-name* was added to the **display ipv6 pathmtu** command to display IPv6 PMTU information for the specified VPN.

For more information about this command, see "IPv6 basics configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Command Reference-Release 2210*.

New feature: Configuring a static neighbor entry for a private network

Configuring a static neighbor entry for a private network

For more information about configuring a static neighbor entry for a private network, see "IPv6 basics configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Configuration Guide-Release 2210*.

Command reference

Option **vpn-instance** *vpn-instance-name* was added to the **ipv6 neighbor** command to specify the VPN to which the static neighbor entry belongs.

For more information about this command, see "IPv6 basics configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Command Reference-Release 2210*.

New feature: Configuring a static PMTU for a private network

Configuring a static PMTU for a private network

For more information about configuring a static PMTU for a private network, see "IPv6 basics configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Configuration Guide-Release 2210*.

Command reference

Option **vpn-instance** *vpn-instance-name* was added to the **ipv6 pathmtu** command to specify the VPN to which the PMTU belongs.

For more information about this command, see "IPv6 basics configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Command Reference-Release 2210*.

New feature: Displaying neighbor information for a specified VPN

Displaying neighbor information for a specified VPN

For more information about displaying neighbor information for a specified VPN, see "IPv6 basics configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Configuration Guide-Release 2210*.

Command reference

New command: **display ipv6 neighbors vpn-instance**.

For more information about this command, see "IPv6 basics configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Command Reference-Release 2210*.

New feature: Configuring the interface as an uplink interface and disabling it from learning ND snooping entries

Configuring the interface as an uplink interface and disabling it from learning ND snooping entries

For more information about configuring the interface as an uplink interface and disabling it from learning ND snooping entries, see "IPv6 basics configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Configuration Guide-Release 2210*.

Command reference

New command: **ipv6 nd snooping uplink**

For more information about this command, see "IPv6 basics configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Command Reference-Release 2210*.

New feature: Configuring permanent static route

Configuring permanent static route

For more information about this feature, see "Static routing configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Routing Configuration Guide-Release 2210*.

Command reference

Keyword **permanent** was added to the **ip route-static** command.

For more information about this command, see "Static routing configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Routing Command Reference-Release 2210*.

New feature: Enabling OSPF ISPF

Enabling OSPF ISPF

For more information about this feature, see "OSPF configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Routing Configuration Guide-Release 2210*.

Command reference

New command: **ispf enable**.

For more information about this command, see "OSPF configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Routing Command Reference-Release 2210*.

New feature: Enabling OSPF to calculate default routes received from other routers

Enabling OSPF to calculate default routes received from other routers

For more information about this feature, see "OSPF configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Routing Configuration Guide-Release 2210*.

Command reference

Modified command:

Keyword **permit-calculate-other** was added to the **default-route-advertise** command.

For more information about this command, see "OSPF configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Routing Command Reference-Release 2210*.

New feature: Assigning a high priority to IS-IS routes

Assigning a high priority to IS-IS routes

For more information about this feature, see "IS-IS configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Routing Configuration Guide-Release 2210*.

Command reference

New command: **priority high**.

For more information about this command, see "IS-IS configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Routing Command Reference-Release 2210*.

New feature: Enabling 4-byte AS number suppression

Enabling 4-byte AS number suppression

For more information about this feature, see "BGP configuration" and "IPv6 BGP configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Routing Configuration Guide-Release 2210*.

Command reference

New command: **peer capability-advertise suppress-4-byte-as**.

For more information about this command, see "BGP configuration commands" and "IPv6 BGP configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Routing Command Reference-Release 2210*.

New feature: Configuring BFD for OSPFv3

Configuring BFD for OSPFv3

For more information about this feature, see "OSPFv3 configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Routing Configuration Guide-Release 2210*.

Command reference

New command: **ospfv3 bfd enable**.

For more information about this command, see "OSPFv3 configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Routing Command Reference-Release 2210*.

New feature: Configuring BFD for IPv6 IS-IS

Configuring BFD for IPv6 IS-IS

For more information about this feature, see "IPv6 IS-IS configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Routing Configuration Guide-Release 2210*.

Command reference

New command: **isis ipv6 bfd enable**.

For more information about this command, see "IPv6 IS-IS configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Routing Command Reference-Release 2210*.

New feature: Configuring BFD for IPv6 BGP

Configuring BFD for IPv6 BGP

For more information about this feature, see "IPv6 BGP configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Routing Configuration Guide-Release 2210*.

Command reference

New command: **peer bfd**.

For more information about this command, see "IPv6 BGP configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Routing Command Reference-Release 2210*.

New feature: Specifying a community list name to match IPv6 BGP routing information

Specifying a community list name to match IPv6 BGP routing information

For more information about this feature, see "IPv6 BGP configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Routing Configuration Guide-Release 2210*.

Command reference

Modified command: Argument *comm-list-name* was added to the **display bgp ipv6 routing-table community-list** command.

For more information about this command, see "IPv6 BGP configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Routing Command Reference-Release 2210*.

New feature: IPv6 MCE

Configuring IPv6 MCE

For more information about configuring IPv6 MCE, see "MCE configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Routing Configuration Guide-Release 2210*.

Command reference

For more information about IPv6 MCE configuration commands, see "MCE configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Routing Command Reference-Release 2210*.

New feature: Configuring IPv6 routing protocols to support VPN instances

Configuring IPv6 routing protocols to support VPN instances

For more information about these features, see "IP routing basics configuration", "IPv6 static routing configuration", "RIPng configuration", "OSPFv3 configuration", "IPv6 IS-IS configuration", and "IPv6 BGP configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Routing Configuration Guide-Release 2210*.

Command reference

For more information about relevant configuration commands, see "IP routing basics configuration commands", "IPv6 static routing configuration commands", "RIPng configuration commands", "OSPFv3 configuration commands", "IPv6 IS-IS configuration commands", and "IPv6 BGP configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Routing Command Reference-Release 2210*.

New feature: Enabling the IGMP snooping & MLD snooping host tracking function

Enabling the IGMP snooping & MLD snooping host tracking function

For more information about enabling the IGMP snooping host tracking function and Enabling the MLD snooping host tracking function, see "IGMP snooping configuration" and "MLD snooping configuration" in *HP A5500 EI & A5500 SI Switch Series IP Multicast Configuration Guide-Release 2210*.

Command reference

New commands:

- **display igmp-snooping host**
- **host-tracking** (IGMP-Snooping view)
- **igmp-snooping host-tracking**
- **display mld-snooping host**
- **host-tracking** (MLD-Snooping view)
- **mld-snooping host-tracking**

For more information about these commands, see "IGMP snooping configuration commands" and "MLD snooping configuration commands" in *HP A5500 EI & A5500 SI Switch Series IP Multicast Command Reference-Release 2210*.

New feature: Configuring IGMP & MLD fast-leave processing

Configuring IGMP & MLD fast-leave processing

For more information about configuring IGMP fast-leave processing and configuring MLD fast-leave processing, see "IGMP configuration" and "MLD configuration" in *HP A5500 EI & A5500 SI Switch Series IP Multicast Configuration Guide-Release 2210*.

Command reference

New commands:

- **fast-leave** (IGMP view)
- **igmp fast-leave**
- **fast-leave** (MLD view)
- **mld fast-leave**

For more information about these commands, see "IGMP snooping configuration commands" and "MLD snooping configuration commands" in *HP A5500 EI & A5500 SI Switch Series IP Multicast Command Reference-Release 2210*.

New feature: PIM snooping & IPv6 PIM snooping

Configuring PIM snooping & IPv6 PIM snooping

For more information about PIM snooping configuration and IPv6 PIM snooping configuration, see *HP A5500 EI & A5500 SI Switch Series IP Multicast Configuration Guide-Release 2210*.

Command reference

For more information about PIM snooping configuration commands and IPv6 PIM snooping configuration commands, see *HP A5500 EI & A5500 SI Switch Series IP Multicast Command Reference-Release 2210*.

New feature: Configuring PIM & IPv6 PIM to work with BFD

Configuring PIM & IPv6 PIM to work with BFD

For more information about configuring PIM to work with BFD and configuring IPv6 PIM to work with BFD, see "PIM configuration" and "IPv6 PIM configuration" in *HP A5500 EI & A5500 SI Switch Series IP Multicast Configuration Guide-Release 2210*.

Command reference

New commands: **pim bfd enable** and **pim ipv6 bfd enable**.

For more information about these commands, see "PIM configuration commands" and "IPv6 PIM configuration commands" in *HP A5500 EI & A5500 SI Switch Series IP Multicast Command Reference-Release 2210*.

New feature: Configuring an MD5 authentication key for the TCP connection to be established with an MSDP peer

Configuring an MD5 authentication key for the TCP connection to be established with an MSDP peer

For more information about configuring an MD5 authentication key for the TCP connection to be established with an MSDP peer, see "MSDP configuration" in *HP A5500 EI & A5500 SI Switch Series IP Multicast Configuration Guide-Release 2210*.

Command reference

New command: **peer password**.

For more information about this command, see "MSDP configuration commands" in *HP A5500 EI & A5500 SI Switch Series IP Multicast Command Reference-Release 2210*.

New feature: Enabling the IGMP & MLD host tracking function

Enabling the IGMP & MLD host tracking function

For more information about enabling the IGMP host tracking function and enabling the MLD host tracking function, see "IGMP configuration" and "MLD configuration" in *HP A5500 EI & A5500 SI Switch Series IP Multicast Configuration Guide-Release 2210*.

Command reference

New commands:

- **display igmp host interface**
- **display igmp host port-info**
- **display igmp ssm-mapping host interface**
- **host-tracking** (IGMP view)
- **igmp host-tracking**
- **display mld host interface**
- **display mld host port-info**
- **display mld ssm-mapping host interface**
- **host-tracking** (MLD view)
- **mld host-tracking**

For more information about these commands, see "IGMP configuration commands" and "MLD configuration commands" in *HP A5500 EI & A5500 SI Switch Series IP Multicast Command Reference-Release 2210*.

New feature: Configuring rule range remark

Configuring rule range remark

For more information about configuring rule range remark, see "ACL configuration" in *HP A5500 EI & A5500 SI Switch Series ACL and QoS Configuration Guide-Release 2210*.

Command reference

New command: **rule remark**.

For more information about this command, see "ACL configuration commands" in *HP A5500 EI & A5500 SI Switch Series ACL and QoS Command Reference-Release 2210*.

New feature: Configuring routing header type for an IPv6 ACL rule

Configuring routing header type for an IPv6 ACL

For more information about configuring routing header type for an IPv6 rule, see "ACL configuration" in *HP A5500 EI & A5500 SI Switch Series ACL and QoS Configuration Guide-Release 2210*.

Command reference

Modified commands:

Keyword **routing** was added to the **rule** command in IPv6 advanced view and IPv6 basic view.

For more information about the commands, see "ACL configuration commands" in *HP A5500 EI & A5500 SI Switch Series ACL and QoS Command Reference-Release 2210*.

New feature: Configuring an IPv6 VPN in an IPv6 ACL rule

Configuring an IPv6 VPN in an IPv6 ACL rule

For more information about configuring VPN in an IPv6 rule, see "ACL configuration" in *HP A5500 EI & A5500 SI Switch Series ACL and QoS Configuration Guide-Release 2210*.

Command reference

Modified commands:

Keyword **vpn-instance** was added to the **rule** command in IPv6 advanced ACL view and IPv6 basic ACL view.

For more information about the commands, see "ACL configuration commands" in *HP A5500 EI & A5500 SI Switch Series ACL and QoS Command Reference-Release 2210*.

New feature: Configuring byte-count or packet-based WFQ queuing

Configuring byte-count or packet-based WFQ queuing

For more information about byte-count or packet-based WFQ queuing configuration, see "Congestion management configuration" in *HP A5500 EI & A5500 SI Switch Series ACL and QoS Configuration Guide-Release 2210*.

Command reference

Keywords **byte-count** and **weight** were added to the **qos wfq** command.

For more information about this command, see "Congestion management configuration commands" in *HP A5500 EI & A5500 SI Switch Series ACL and QoS Command Reference-Release 2210*.

New feature: Configuring SP+WFQ queuing

Configuring SP+WFQ queuing

For more information about SP+WFQ queuing configuration, see "Congestion management configuration" in *HP A5500 EI & A5500 SI Switch Series ACL and QoS Configuration Guide-Release 2210*.

Command reference

New commands: **qos wfq byte-count** and **qos wfq group sp**.

For more information about these commands, see "Congestion management configuration commands" in *HP A5500 EI & A5500 SI Switch Series ACL and QoS Command Reference-Release 2210*.

New feature: Setting the validity time of the local user

Setting the validity time of the local user

For more information about setting the validity time of the local user, see "AAA configuration" in *HP A5500 EI & A5500 SI Switch Series Security Configuration Guide-Release 2210*.

Command reference

New command: **validity-date**.

For more information about this command, see "AAA configuration commands" in *HP A5500 EI & A5500 SI Switch Series Security Command Reference-Release 2210*.

New feature: Specifying the local user as a guest or guest manager

Specifying the local user as a guest or guest manager

For more information about specifying the role user as a guest or guest manager, see "AAA configuration" in *HP A5500 EI & A5500 SI Switch Series Security Configuration Guide-Release 2210*.

Command reference

Keywords **user-role-guest** and **user-role guest-manager** are added to the **authorization-attribute** (local user view/user group view) command.

For more information about this command, see "AAA configuration commands" in *HP A5500 EI & A5500 SI Switch Series Security Command Reference-Release 2210*.

New feature: Setting the guest attribute for a user group

Setting the guest attribute for a user group

For more information about setting the guest attribute for a user group, see "AAA configuration" in *HP A5500 EI & A5500 SI Switch Series Security Configuration Guide-Release 2210*.

Command reference

New command: **group-attribute allow-guest**.

For more information about the command, see "AAA configuration commands" in *HP A5500 EI & A5500 SI Switch Series Security Command Reference-Release 2210*.

New feature: Authorizing a local user to use the Web service

Authorizing a local user to use the Web service

For more information about authorizing a local user to use the Web service, see "AAA configuration" in *HP A5500 EI & A5500 SI Switch Series Security Configuration Guide-Release 2210*.

Command reference

Modified commands:

- The **web** keyword is added to the **service-type** command.
- The **service-type web** keyword is added to **display local-user** and **undo local-user** commands.

For more information about the commands, see "AAA configuration commands" in *HP A5500 EI & A5500 SI Switch Series Security Command Reference-Release 2210*.

New feature: Specifying ciphertext shared keys for RADIUS/HWTACACS servers

Specifying ciphertext shared keys for RADIUS/HWTACACS servers

For more information about specifying ciphertext shared keys for RADIUS and HWTACACS servers, see "AAA configuration" in *HP A5500 EI & A5500 SI Switch Series Security Configuration Guide-Release 2210*.

Command reference

Keywords **cipher** and **simple** are added to the following commands:

- **key** (HWTACACS scheme view)
- **key** (RADIUS scheme view)
- **primary accounting** (RADIUS scheme view)
- **primary authentication** (RADIUS scheme view)

- **secondary accounting** (RADIUS scheme view)
- **secondary authentication** (RADIUS scheme view)

For more information about the commands, see "AAA configuration commands" in *HP A5500 EI & A5500 SI Switch Series Security Command Reference-Release 2210*.

New feature: Specifying supported domain name delimiters

Specifying supported domain name delimiters

For more information about specifying supported domain name delimiters configuration, see "802.1X configuration" in *HP A5500 EI & A5500 SI Switch Series Security Configuration Guide-Release 2210*.

Command reference

For more information about specifying supported domain name delimiters configuration commands, see "802.1X configuration commands" in *HP A5500 EI & A5500 SI Switch Series Security Command Reference-Release 2210*.

New feature: Enabling inactivity aging

Enabling inactivity aging

For more information about enabling inactivity aging configuration, see "Port security configuration" in *HP A5500 EI & A5500 SI Switch Series Security Configuration Guide-Release 2210*.

Command reference

New command: **port-security mac-address aging-type inactivity**.

For more information about this command, see "Port security configuration commands" in *HP A5500 EI & A5500 SI Switch Series Security Command Reference-Release 2210*.

New feature: Enabling the dynamic secure MAC function

Enabling the dynamic secure MAC function

For more information about enabling the dynamic secure MAC function configuration, see "Port security configuration" in *HP A5500 EI & A5500 SI Switch Series Security Configuration Guide-Release 2210*.

Command reference

New command: **port-security mac-address dynamic**.

For more information about this command, see "Port security configuration commands" in *HP A5500 EI & A5500 SI Switch Series Security Command Reference-Release 2210*.

New feature: Establishing a connection between a client to a VPN-specific IPv6 Stelnet server

Establishing a connection between a client to a VPN-specific IPv6 Stelnet server

For more information about establishing a connection between a client to a VPN-specific IPv6 Stelnet server, see "SSH2.0 configuration" in *HP A5500 EI & A5500 SI Switch Series Security Configuration Guide-Release 2210*.

Command reference

The **vpn-instance** *vpn-instance-name* option was added to the **ssh2 ipv6** command.

For more information about this command, see "SSH2.0 configuration commands" in *HP A5500 EI & A5500 SI Switch Series Security Command Reference-Release 2210.*

New feature: Establishing a connection between a client to a VPN-specific IPv6 SFTP server

Establishing a connection between a client to a VPN-specific IPv6 SFTP server

For more information about establishing a connection between a client to a VPN-specific IPv6 SFTP server, see "SFTP configuration" in *HP A5500 EI & A5500 SI Switch Series Security Configuration Guide-Release 2210*.

Command reference

The **vpn-instance** *vpn-instance-name* option was added to the **sftp ipv6** command.

For more information about this command, see "SSH2.0 configuration commands" in *HP A5500 EI & A5500 SI Switch Series Security Command Reference-Release 2210.*

New feature: Enabling SSL client weak authentication

Enabling SSL client weak authentication

For more information about enabling SSL client weak authentication, see "SSL configuration" in *HP A5500 EI & A5500 SI Switch Series Security Configuration Guide-Release 2210.*

Command reference

New command: **client-verify weaken**.

For more information about this command, see "SSL configuration commands" in *HP A5500 EI & A5500 SI Switch Series Security Command Reference-Release 2210.*

New feature: Setting the maximum number of IPv4/IPv6 source guard binding entries

Setting the maximum number of IPv4/IPv6 binding entries

For more information about setting the maximum number of IPv4/IPv6 binding entries, see "IP source guard configuration" in *HP A5500 EI & A5500 SI Switch Series Security Configuration Guide-Release 2210.*

Command reference

New commands: **ip verify source max-entries** and **ipv6 verify source max-entries**.

For more information about these commands, see "IP source guard configuration commands" in *HP A5500 EI & A5500 SI Switch Series Security Command Reference-Release 2210.*

New feature: Loose URPF check

Enabling loose URPF check

For more information about enabling loose URPF check, see "URPF configuration" in *HP A5500 EI & A5500 SI Switch Series Security Configuration Guide-Release 2210.*

Command reference

New command: **ip urpf loose**.

For more information about this command, see "URPF configuration commands" in *HP A5500 EI & A5500 SI Switch Series Security Command Reference-Release 2210*.

New feature: SAVI

Configuring SAVI

For more information about configuring SAVI, see *HP A5500 EI & A5500 SI Switch Series Security Configuration Guide-Release 2210.*

Command reference

For more information about SAVI configuration commands, see *HP A5500 EI & A5500 SI Switch Series Security Command Reference-Release 2210.*

New feature: Blacklist

Configuring blacklist

For more information about configuring blacklist, see *HP A5500 EI & A5500 SI Switch Series Security Configuration Guide-Release 2210.*

Command reference

For more information about blacklist configuration commands, see *HP A5500 EI & A5500 SI Switch Series Security Command Reference-Release 2210.*

New feature: Enabling Ethernet OAM remote loopback in user view and system view

Enabling Ethernet OAM remote loopback in user view and system view

For more information about enabling Ethernet OAM remote loopback in user view and system view, see "Ethernet OAM configuration" in *HP A5500 EI & A5500 SI Switch Series High Availability Configuration Guide-Release 2210*.

Command reference

New command: **oam loopback interface**.

For more information about this command, see "Ethernet OAM configuration commands" in *HP A5500 EI & A5500 SI Switch Series High Availability Command Reference-Release 2210*.

New feature: Restoring the default Ethernet OAM connection mode

Restoring the default Ethernet OAM connection mode

For more information about restoring the default Ethernet OAM connection mode, see "Ethernet OAM configuration" in *HP A5500 EI & A5500 SI Switch Series High Availability Configuration Guide-Release 2210*.

Command reference

New command: **undo oam mode**.

For more information about this command, see "Ethernet OAM configuration commands" in *HP A5500 EI & A5500 SI Switch Series High Availability Command Reference-Release 2210*.

New feature: Configuring the collaboration between Smart Link and CC of CFD

Configuring the collaboration between Smart Link and CC of CFD

For more information about configuring the collaboration between Smart Link and CC of CFD, see "Smart Link configuration" in *HP A5500 EI & A5500 SI Switch Series High Availability Configuration Guide-Release 2210*.

Command reference

New command: **port smart-link group track**.

For more information about this command, see "Smart Link configuration commands" in *HP A5500 EI & A5500 SI Switch Series High Availability Command Reference-Release 2210*.

New feature: Configuring the VF tracking function to monitor an AVF

Configuring the VF tracking function to monitor an AVF

For more information about configuring the VF tracking function to monitor an AVF, see "VRRP configuration" in *HP A5500 EI & A5500 SI Switch Series High Availability Configuration Guide-Release 2210*.

Command reference

Modified commands:

- Option **forwarder-switchover member-ip** *ip-address* was added to the **vrrp vrid track** command.
- Option **forwarder-switchover member-ip** *ipv6-address* was added to the **vrrp ipv6 vrid track** command.

For more information about these commands, see "VRRP configuration commands" in *HP A5500 EI & A5500 SI Switch Series High Availability Command Reference-Release 2210*.

New feature: CWMP

Configuring CWMP

For more information about CWMP configuring, see *HP A5500 EI & A5500 SI Switch Series Network Management and Monitoring Configuration Guide-Release 2210*.

Command reference

For more information about CWMP configuration commands, see *HP A5500 EI & A5500 SI Switch Series Network Management and Monitoring Command Reference-Release 2210*.

Modified feature: Improving the isolate-user-VLAN usability

Feature change description

Compared with Release 2208, to make the isolate-user-VLAN easier to configure, the feature was modified as follows:

1. After an isolate-user-VLAN is associated with secondary VLANs, you can perform the following configurations:

- Adding an access port to and deleting an access port from the isolate-user-VLAN and secondary VLANs.
- Deleting the isolate-user-VLAN or secondary VLANs.
- Isolating the ports in the secondary VLANs at Layer 2 by using the **isolated-vlan enable** command.
- Modifying the promiscuous or host mode of ports.

2. When you use the **port isolate-user-vlan** *vlan-id* **promiscuous** command to configure an uplink port, the port is automatically assigned to the isolate-user-VLAN specified by the *vlan-id* argument and the secondary VLANs associated with the isolate-user-VLAN. You do not need to manually add the uplink port to the isolate-user-VLAN.
3. You can assign a trunk port to the isolate-user-VLAN or secondary VLANs.

For more information about configuring an isolate-user-VLAN after the feature is modified, see "Isolate-user-VLAN configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 2—LAN Switching Configuration Guide-Release 2210*.

Command changes

Modified command: port isolate-user-vlan promiscuous

Old Syntax

port isolate-user-vlan promiscuous

New syntax

port isolate-user-vlan *vlan-id* **promiscuous**

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Change description

Before modification: You must manually add the uplink port to the isolate-user-VLAN.

After modification: When you use the **port isolate-user-vlan** *vlan-id* **promiscuous** command to configure an uplink port, the port is automatically assigned to the isolate-user-VLAN specified by the *vlan-id* argument and the secondary VLANs associated with the isolate-user-VLAN. You do not need to manually add the uplink port to the isolate-user-VLAN.

Modified feature: Using the device to log in to a Telnet server

Feature change description

The **telnet ipv6** command now supports specifying a VPN instance.

Command changes

Modified command: telnet ipv6

Old syntax

telnet ipv6 *remote-host* [**-i** *interface-type interface-number*] [*port-number*]

New syntax

telnet ipv6 *remote-host* [**-i** *interface-type interface-number*] [*port-number*] [**vpn-instance** *vpn-instance-name*]

Views

System view

Change description

Before modification: The **telnet ipv6** command does not support specifying a VPN instance.

After modification: The **telnet ipv6** command supports specifying a VPN instance.

Modified feature: Logging in to the FTP server from user view

Feature change description

The **ftp ipv6** command now supports specifying a VPN instance.

Command changes

Modified command: ftp ipv6

Old syntax

ftp ipv6 [*server-address* [*service-port*] [**source ipv6** *source-ipv6-address*] [**-i** *interface-type interface-number*]]

New syntax

ftp ipv6 [*server-address* [*service-port*] [**vpn-instance** *vpn-instance-name*] [**source ipv6** *source-ipv6-address*] [**-i** *interface-type interface-number*]]

Views

System view

Change description

Before modification: The **ftp ipv6** command does not support specifying a VPN instance.

After modification: The **ftp ipv6** command supports specifying a VPN instance.

Modified feature: Downloading or uploading a file in an IPv6 network

Feature change description

The **tftp ipv6** command now supports specifying a VPN instance.

Command changes

Modified command: ftp ipv6

Old syntax

tftp ipv6 *tftp-ipv6-server* [**-i** *interface-type interface-number*] { **get** | **put** } *source-filename* [*destination-filename*]

New syntax

tftp ipv6 *tftp-ipv6-server* [**-i** *interface-type interface-number*] { **get** | **put** } *source-filename* [*destination-filename*] [**vpn-instance** *vpn-instance-name*]

Views

System view

Change description

Before modification: The **tftp ipv6** command does not support specifying a VPN instance.

After modification: The **tftp ipv6** command supports specifying a VPN instance.

Modified feature: Installing patches in one step

Feature change description

The **patch install** command now supports specifying a patch package file name.

Command changes

Modified command: patch install

Old syntax

patch install *patch-location*

New syntax

patch install { *patch-location* | **file** *filename* }

Views

User view

Change description

Before modification: To install patches in one step, you must specify the patch file path.

After modification: To install patches in one step, you can choose to specify a patch package file name.

Modified feature: Displaying file or directory information

Feature change description

The **dir** command now can display files and folders in the root directories of all storage media on the device.

Command changes

Modified command: dir

Old syntax

dir [**/all**] [*file-url*]

New syntax

dir [**/all**] [*file-url* | **/all-filesystems**]

Views

User view

Change description

Before modification: The **dir** command displays a specific file or all files and folders in the current directory.

After modification: The **dir** command can also display files and folders in the root directories of all storage media on the device.

Modified feature: Loopback interface numbering

Feature change description

The maximum loopback interface number was modified into 1023.

Command changes

Modified command: interface loopback

Syntax

interface loopback *interface-number*

Views

System view

Change description

Before modification: The loopback interface number ranges from 0 to 127.

After modification: The loopback interface number ranges from 0 to 1023.

Modified feature: Configuring the link mode of a combo interface

Feature change description

A combo interface supports configuring the link mode, which can be bridge or route.

Command changes

Modified command: port link-mode

Syntax

port link-mode { **bridge** | **route** }

Views

Ethernet interface view

Change description

Before modification: A combo interface does not support configuring the link mode.

After modification: A combo interface supports configuring the link mode.

Modified feature: Enabling address check

Feature change description

The command for this feature changes.

Command changes

Modified command: dhcp relay address-check enable

Old syntax

dhcp relay address-check { disable | enable }

New syntax

dhcp relay address-check enable

undo dhcp relay address-check enable

Views

interface view

Change description

The command was changed from **dhcp relay address-check** { **disable** | **enable** } to **dhcp relay address-check enable**.

Modified feature: Enabling ND proxy

Feature change description

The command for this feature changes.

Command changes

Modified command: proxy-nd enable

Old syntax

ipv6 nd proxy enable

undo ipv6 nd proxy enable

New syntax

proxy-nd enable

undo proxy-nd enable

Views

interface view

Change description

The command was changed from **ipv6 nd proxy enable** to **proxy-nd enable**.

Modified feature: ND snooping

Feature change description

The device with the new feature can create ND snooping entries based on DAD NS messages that contain link local addresses or global unicast addresses. Configure at least one type of ND snooping.

Command changes

New command: ipv6 nd snooping enable global

Syntax

ipv6 nd snooping enable global

undo ipv6 nd snooping enable global

View

System view

Default level

2: System level

Parameters

None

Description

Use the **ipv6 nd snooping enable global** command to enable ND snooping based on global unicast addresses. The device uses DAD NS messages containing global unicast addresses to create ND snooping entries.

Use the **undo nd snooping enable global** command to restore the default.

By default, ND snooping based on global unicast addresses is disabled.

Examples

Enable NS snooping based on global unicast addresses.

```
<Sysname> system-view
[Sysname] ipv6 nd snooping enable global
```

New command: ipv6 nd snooping enable link-local

Syntax

ipv6 nd snooping enable link-local

undo ipv6 nd snooping enable link-local

View

System view

Default level

2: System level

Parameters

None

Description

Use the **ipv6 nd snooping enable link-local** command to enable ND snooping based on link local addresses. The device uses DAD NS messages containing link local addresses to create ND snooping entries.

Use the **undo nd snooping enable link-local** command to restore the default.

By default, ND snooping based on link local addresses is disabled.

Examples

Enable ND snooping based on link local addresses.

```
<Sysname> system-view
[Sysname] ipv6 nd snooping enable link-local
```

Modified feature: Displaying IPv6 information for tunnel interfaces

Feature change description

The keyword in the **display ipv6 interface tunnel** command changes.

Command changes

Modified command: display ipv6 interface tunnel

Old syntax

display ipv6 interface tunnel [*number*] [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

New syntax

display ipv6 interface tunnel [*number*] [**brief**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Change description

Before modification: Keyword **verbose** is used to display detailed information for the tunnel interface.

After modification: Keyword **verbose** is replaced with keyword **brief** to display brief information for the tunnel interface.

Modified feature: Displaying IPv6 FIB entries

Feature change description

The keyword in the **display ipv6 fib** command changes.

Command changes

Modified command: display ipv6 fib

Old syntax

display ipv6 fib [**slot** *slot-number*] [*ipv6-address*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

New syntax

display ipv6 fib [**vpn-instance** *vpn-instance-name*] [**acl6** *acl6-number* | **ipv6-prefix** *ipv6-prefix-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

display ipv6 fib [**vpn-instance** *vpn-instance-name*] *ipv6-address* [*prefix-length*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Change description

Before modification: Option **slot** *slot-number* was supported in the command.

After modification: Option **slot** *slot-number* is deleted and options **vpn-instance** *vpn-instance-name*, **acl6** *acl6-number*, and **ipv6-prefix** *ipv6-prefix-name* are added to display the IPv6 FIB entries of the specified VPN, entries permitted by a specified ACL or matching a specified prefix list. Argument *prefix-length* is added to display the prefix length for the destination address.

Modified feature: Displaying the IPv6 information of an interface

Feature change description

The keyword in the **display ipv6 interface** command changes.

Command changes

Modified command: display ipv6 interface

Old syntax

display ipv6 interface [*interface-type* [*interface-number*]] [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

New syntax

display ipv6 interface [*interface-type* [*interface-number*]] [**brief**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Change description

Before modification: Keyword **verbose** is used to display detailed information about the interface.

After modification: Keyword **verbose** is replaced with keyword **brief** to display brief information about the interface.

Modified feature: Routing policy

Feature change description

The value range of the *route-policy-name* argument changed to 1 to 63.

Command changes

Modified command: route-policy

Syntax

route-policy *route-policy-name* { **deny** | **permit** } **node** *node-number*

Views

System view

Change description

Before modification: The *route-policy-name* argument ranges from 1 to 19.

After modification: The *route-policy-name* argument ranges from 1 to 63.

Modified feature: Setting the register suppression time for PIM/IPv6 PIM

Feature change description

Changed the register suppression time.

Command changes

Modified command: register-suppression-timeout

Syntax

register-suppression-timeout *interval*

Views

Public network PIM view, VPN instance PIM view, IPv6 PIM view

Change description

Before modification: The *interval* argument ranges from 1 to 3600.

After modification: The *interval* argument ranges from 1 to 65535.

Modified feature: Setting the maximum delay for sending a hello message in PIM/IPv6 PIM

Feature change description

Changed the maximum delay for sending a hello message.

Command changes

Modified command: pim triggered-hello-delay

Syntax

pim triggered-hello-delay *interval*

Views

Interface view

Change description

Before modification: The *interval* argument ranges from 1 to 5.

After modification: The *interval* argument ranges from 1 to 60.

Modified command: pim ipv6 triggered-hello-delay

Syntax

pim ipv6 triggered-hello-delay *interval*

Views

Interface view

Change description

Before modification: The *interval* argument ranges from 1 to 5.

After modification: The *interval* argument ranges from 1 to 60.

Modified feature: Displaying routing information matching the specified MBGP&IPv6 BGP community list

Feature change description

Changed the command that displays routing information matching the specified MBGP&IPv6 BGP community list.

Command changes

Modified command: display bgp multicast routing-table community-list

Old syntax

display bgp multicast routing-table community-list { *basic-community-list-number* [**whole-match**] | *adv-community-list-number* } &<1-16> [**|** { **begin** | **exclude** | **include** } *regular-expression*]

New syntax

display bgp multicast routing-table community-list { { *basic-community-list-number* **|** *comm-list-name* } [**whole-match**] **|** *adv-community-list-number* } [**|** { **begin** **|** **exclude** **|** **include** } *regular-expression*]

Views

Any view

Change description

Before modification:

- The *comm-list-name* argument was not supported.
- The *basic-community-list-number* or *adv-community-list-number* argument can be entered up to 16 times.

After modification:

- The *comm-list-name* argument is supported.
- The *basic-community-list-number*, *comm-list-name*, or *adv-community-list-number* argument can be entered only once.

Modified command: display bgp ipv6 multicast routing-table community-list

Old syntax

display bgp ipv6 multicast routing-table community-list { *basic-community-list-number* [**whole-match**] | *adv-community-list-number* } &<1-16> [**|** { **begin** | **exclude** | **include** } *regular-expression*]

New syntax

display bgp ipv6 multicast routing-table community-list { { *basic-community-list-number* **|** *comm-list-name* } [**whole-match**] **|** *adv-community-list-number* } [**|** { **begin** **|** **exclude** **|** **include** } *regular-expression*]

Views

Any view

Change description

Before modification:

- The *comm-list-name* argument was not supported.
- The *basic-community-list-number* or *adv-community-list-number* argument can be entered up to 16 times.

After modification:

- The *comm-list-name* argument is supported.
- The *basic-community-list-number*, *comm-list-name*, or *adv-community-list-number* argument can be entered only once.

Modified feature: CFD

Feature change description

The command levels or views of certain CFD commands have changed.

Command changes

Before modification:

- Default command level of the commands **cfd linktrace** and **cfd loopback** was system, and the commands were available in system view.
- Default command level of these commands was system: **display cfd ais**, **display cfd dm one-way history**, **display cfd linktrace-reply**, **display cfd linktrace-reply auto-detection**, **display cfd ma**, **display cfd md**, **display cfd mep**, **display cfd remote-mep**, **display cfd service-instance**, **display cfd status**, **display cfd tst**, **reset cfd dm one-way history**, and **reset cfd tst**.

After modification:

- Default command level of the commands **cfd linktrace** and **cfd loopback** was visit, and the commands were available in any view.
- Default command level of these commands was monitor: **display cfd ais**, **display cfd dm one-way history**, **display cfd linktrace-reply**, **display cfd linktrace-reply auto-detection**, **display cfd ma**, **display cfd md**, **display cfd mep**, **display cfd remote-mep**, **display cfd service-instance**, **display cfd status**, **display cfd tst**, **reset cfd dm one-way history**, and **reset cfd tst**.

For more information about these commands, see "CFD configuration commands" in *HP A5500 EI & A5500 SI Switch Series High Availability Command Reference-Release 2210*.

Modified feature: Value range of the RRPP domain ID

Feature change description

The value range of the RRPP domain ID has changed.

Command changes

Modified command: display rrpp statistics

Syntax

display rrpp statistics domain *domain-id* [**ring** *ring-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Change description

Before modification: The *domain-id* argument ranges from 1 to 8.

After modification: The *domain-id* argument ranges from 1 to 24.

Modified command: display rrpp verbose

Syntax

display rrpp verbose domain *domain-id* [**ring** *ring-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Change description

Before modification: The *domain-id* argument ranges from 1 to 8.

After modification: The *domain-id* argument ranges from 1 to 24.

Modified command: domain ring

Syntax

domain *domain-id* **ring** *ring-id-list*

undo domain *domain-id* [**ring** *ring-id-list*]

View

RRPP ring group view

Change description

Before modification: The *domain-id* argument ranges from 1 to 8.

After modification: The *domain-id* argument ranges from 1 to 24.

Modified command: reset rrpp statistics

Syntax

reset rrpp statistics domain *domain-id* [**ring** *ring-id*]

View

User view

Change description

Before modification: The *domain-id* argument ranges from 1 to 8.

After modification: The *domain-id* argument ranges from 1 to 24.

Modified command: rrpp domain

Syntax

rrpp domain *domain-id*

undo rrpp domain *domain-id*

View

System view

Change description

Before modification: The *domain-id* argument ranges from 1 to 8.

After modification: The *domain-id* argument ranges from 1 to 24.

Modified feature: Configuring the protected VLANs for the RRPP domain

Feature change description

The **protected-vlan** command configures the protected VLANs for the RRPP domain by referencing MSTIs. As PVST is introduced in this release, the value range of the *instance-id-list* argument changes accordingly.

Command changes

Modified command: protected-vlan

Syntax

protected-vlan reference-instance *instance-id-list*

undo protected-vlan [**reference-instance** *instance-id-list*]

Views

RRPP domain view

Change description

Before modification: The *instance-id-list* argument ranges from 0 to 32.

After modification: The *instance-id-list* argument ranges from 0 to 128.

Modified feature: Configuring the protected VLANs for a smart link group

Feature change description

The **protected-vlan** command configures the protected VLANs for a smart link group by referencing MSTIs. As PVST is introduced in this release, the value range of the *instance-id-list* argument changes accordingly.

Command changes

Modified command: protected-vlan

Syntax

protected-vlan reference-instance *instance-id-list*

undo protected-vlan [**reference-instance** *instance-id-list*]

Views

Smart link group view

Change description

Before modification: The *instance-id-list* argument ranges from 0 to 32.

After modification: The *instance-id-list* argument ranges from 0 to 128.

Modified feature: Displaying and maintaining BFD

Feature change description

Command levels of certain BFD **display** and **reset** commands have changed.

Command changes

Command levels of these commands changed from system to monitor: **display bfd debugging-switches**, **display bfd interface**, **display bfd session**, and **reset bfd session statistics**.

For more information about these commands, see "BFD configuration commands" in *HP A5500 EI & A5500 SI Switch Series High Availability Command Reference-Release 2210*.

Modified feature: Enabling traps globally

Feature change description

The **snmp-agent trap enable** command has keyword changes.

Command changes

Modified command: snmp-agent trap enable

Old syntax

snmp-agent trap enable [arp rate-limit | bfd | bgp |configuration | flash | ospf [process-id] [ifauthfail | ifcfgerror | ifrxbadpkt | ifstatechange | iftxretransmit | lsdbapproachoverflow | lsdboverflow | maxagelsa | nbrstatechange | originatelsa | vifcfgerror | virifauthfail | virifrxbadpkt | virifstatechange | viriftxretransmit | virnbrstatechange] * | pim [candidatebsrwinelection | electedbsrlostelection | interfaceelection | invalidjoinprune | invalidregister | neighborloss | rpmappingchange] * | standard [authentication | coldstart | linkdown | linkup | warmstart]* | system | vrrp [authfailure | newmaster]]

undo snmp-agent trap enable [arp rate-limit | bfd | bgp | configuration | flash | ospf [process-id] [ifauthfail | ifcfgerror | ifrxbadpkt | ifstatechange | iftxretransmit |

lsdbapproachoverflow | lsdboverflow | maxagelsa | nbrstatechange | originatelsa | vifcfgerror | virifauthfail | virifrxbadpkt | virifstatechange | viriftxretransmit | virnbrstatechange] * | pim [candidatebsrwinelection | electedbsrlostelection | interfaceelection | invalidjoinprune | invalidregister | neighborloss | rpmappingchange] * | standard [authentication | coldstart | linkdown | linkup | warmstart]* | system | vrrp [authfailure | newmaster]]

New syntax

snmp-agent trap enable [arp rate-limit | bgp | configuration | default-route | flash | ospf [process-id] [ifauthfail | ifcfgerror | ifrxbadpkt | ifstatechange | iftxretransmit | lsdbapproachoverflow | lsdboverflow | maxagelsa | nbrstatechange | originatelsa | vifcfgerror | virifauthfail | virifrxbadpkt | virifstatechange | viriftxretransmit | virnbrstatechange] * | pim [candidatebsrwinelection | electedbsrlostelection | interfaceelection | invalidjoinprune | invalidregister | neighborloss | rpmappingchange] * | standard [authentication | coldstart | linkdown | linkup | warmstart]* | system | vrrp [authfailure | newmaster]]

undo snmp-agent trap enable [arp rate-limit | bgp | configuration | default-route | flash | ospf [process-id] [ifauthfail | ifcfgerror | ifrxbadpkt | ifstatechange | iftxretransmit | lsdbapproachoverflow | lsdboverflow | maxagelsa | nbrstatechange | originatelsa | vifcfgerror | virifauthfail | virifrxbadpkt | virifstatechange | viriftxretransmit | virnbrstatechange] * | pim [candidatebsrwinelection | electedbsrlostelection | interfaceelection | invalidjoinprune | invalidregister | neighborloss | rpmappingchange] * | standard [authentication | coldstart | linkdown | linkup | warmstart]* | system | vrrp [authfailure | newmaster]]

Views

Any view

Change description

The **default-route** keyword was added, and the **bfd** keyword was deleted.

Modified feature: Configuring IP source guard

Feature change description

- Changed the commands for configuring static IPv4/IPv6 source guard binding entries.
- Changed the commands for enabling the IPv4/IPv6 source guard function.
- Changed the commands for displaying IP source guard binding entries.
- Removed the commands for configuring the exceptional ports for the global static IP source guard binding entries.

Command changes

Modified command: display ip source binding

Old syntax

display ip check source [**interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

New syntax

display ip source binding [**static**] [**interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Change description

Before modification: **display ip check source**

After modification: **display ip source binding**

Modified command: display ipv6 source binding

Old syntax

display ip check source ipv6 [**interface** *interface-type interface-number* **| ip-address** *ip-address* **| mac-address** *mac-address*] [**slot** *slot-number*] [**|** { **begin | exclude | include** } *regular-expression*]

New syntax

display ipv6 source binding [**static**] [**interface** *interface-type interface-number* **| ipv6-address** *ipv6-address* **| mac-address** *mac-address*] [**slot** *slot-number*] [**|** { **begin | exclude | include** } *regular-expression*]

Views

Any view

Change description

Before modification: **display ip check source ipv6**

After modification: **display ipv6 source binding**

Modified command: ip source binding (system view)

Old syntax

user-bind ip-address *ip-address* **mac-address** *mac-address*

undo user-bind { **all | ip-address** *ip-address* **mac-address** *mac-address* }

New syntax

ip source binding ip-address *ip-address* **mac-address** *mac-address*

undo ip source binding { **all | ip-address** *ip-address* **mac-address** *mac-address* }

Views

System view

Change description

Before modification: **user-bind** (system view)

After modification: **ip source binding**(system view)

Modified command: ipv6 source binding (system view)

Old syntax

user-bind ipv6 ip-address *ip-address* **mac-address** *mac-address*

undo user-bind ipv6 { **all | ip-address** *ip-address* **mac-address** *mac-address* }

New syntax

ipv6 source binding ipv6-address *ipv6-address* **mac-address** *mac-address*

undo ipv6 source binding { **all | ipv6-address** *ipv6-address* **mac-address** *mac-address* }

Views

System view

Change description

Before modification: **user-bind ipv6**(system view)

After modification: **ipv6 source binding**(system view)

Modified command: ip source binding (interface view)

Old syntax

user-bind { **ip-address** *ip-address* **|** **ip-address** *ip-address* **mac-address** *mac-address* **|** **mac-address** *mac-address* } [**vlan** *vlan-id*]

undo user-bind { **ip-address** *ip-address* **|** **ip-address** *ip-address* **mac-address** *mac-address* **|** **mac-address** *mac-address* } [**vlan** *vlan-id*]

New syntax

ip source binding { **ip-address** *ip-address* **|** **ip-address** *ip-address* **mac-address** *mac-address* **|** **mac-address** *mac-address* } [**vlan** *vlan-id*]

undo ip source binding { **ip-address** *ip-address* **|** **ip-address** *ip-address* **mac-address** *mac-address* **|** **mac-address** *mac-address* } [**vlan** *vlan-id*]

Views

Ethernet interface view

Change description

Before modification: **user-bind** (interface view)

After modification: **ip source binding**(interface view)

Modified command: ipv6 source binding (interface view)

Old syntax

user-bind ipv6 { **ip-address** *ip-address* **|** **ip-address** *ip-address* **mac-address** *mac-address* **|** **mac-address** *mac-address* } [**vlan** *vlan-id*]

undo user-bind ipv6 { **ip-address** *ip-address* **|** **ip-address** *ip-address* **mac-address** *mac-address* **|** **mac-address** *mac-address* } [**vlan** *vlan-id*]

New syntax

ipv6 source binding { **ipv6-address** *ipv6-address* **|** **ipv6-address** *ipv6-address* **mac-address** *mac-address* **|** **mac-address** *mac-address* } [**vlan** *vlan-id*]

undo ipv6 source binding { **ipv6-address** *ipv6-address* **|** **ipv6-address** *ipv6-address* **mac-address** *mac-address* **|** **mac-address** *mac-address* } [**vlan** *vlan-id*]

Views

Ethernet interface view

Change description

Before modification: **user-bind ipv6**(interface view)

After modification: **ipv6 source binding**(interface view)

Modified command: ip verify source

Old syntax

ip check source { **ip-address | ip-address mac-address | mac-address** }

undo ip check source

New syntax

ip verify source { **ip-address | ip-address mac-address | mac-address** }

undo ip verify source

Views

Ethernet interface view, VLAN interface view, port group view

Change description

Before modification: **ip check source**

After modification: **ip verify source**

Modified command: ipv6 verify source

Old syntax

ip check source ipv6 { **ip-address | ip-address mac-address | mac-address** }

undo ip check source ipv6

New syntax

ipv6 verify source { **ipv6-address | ipv6-address mac-address | mac-address** }

undo ipv6 verify source

Views

Ethernet interface view, port group view

Change description

Before modification: **ip check source ipv6**

After modification: **ipv6 verify source**

Removed command: display user-bind

Syntax

display user-bind [**ipv6**] [**interface** *interface-type interface-number* **| ip-address** *ip-address* **| mac-address** *mac-address*] [**slot** *slot-number*] [**|** { **begin | exclude | include** } *regular-expression*]

Views

Any view

Removed command: user-bind uplink

Syntax

user-bind uplink

undo user-bind uplink

Views

Ethernet interface view

A5500EI-CMW520-R2208

This release has the following changes:

- New feature: Setting the age timer for ND entries in stale state

New feature: Setting the age timer for ND entries in stale state

Setting the age timer for ND entries in stale state

For more information about setting the age timer for ND entries in stale state, see "IPv6 basics configuration" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Configuration Guide-Release 2210*.

Command reference

New command: **ipv6 neighbor stale-aging**.

For more information about this command, see "IPv6 basics configuration commands" in *HP A5500 EI & A5500 SI Switch Series Layer 3—IP Services Command Reference-Release 2210*.

S5500EI-CMW520-R2208

Related documentation:

- H3C S5500-SI[EI] Series Ethernet Switches Configuration Guides-Release 2208
- H3C S5500-SI[EI] Series Ethernet Switches Command References-Release 2208