HPE 6125XLG-CMW710-R2432P03 Release Notes

The information in this document is subject to change without notice.
© Copyright 2017 Hewlett Packard Enterprise Development LP

Contents

List of Tables

This document describes the features, restrictions and guidelines, open problems, and workarounds for version 6125XLG-CMW710-R2432P03. Before you use this version in 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 6125XLG-CMW710-R2432P03 Release Notes (Software Feature Changes) and the documents listed in "Related documents"

Version information

Version number

Comware software, Version 7.1.045, Release 2432P03

Note: You can see the version number with the command display version in any view.

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
6125XLG-CMW710-R2432P03	6125XLG-CMW710-R2432P02	2017-04-17	Release version	This version fixed bugs and introduced feature changes. New features include: • Gratuitous ARP packet retransmission for the device MAC address change Modified features include: • Shutting down a Layer 2 aggregate interface by using OpenFlow
6125XLG-CMW710-R2432P02	6125XLG-CMW710-R2432P01	2017-03-10	Release version	This version fixed bugs and introduced feature changes. New features include: • Setting the MAC address for a Layer 3 Ethernet interface, Layer 3 Ethernet subinterface or Layer 3 aggregate interface Modified features include: • Value range for the interval for an OpenFlow instance to reconnect to a controller.
6125XLG-CMW710-R2432P01	6125XLG-CMW710-R2432	2017-01-20	Release version	Added new features Modified features Fixed bugs
6125XLG-CMW710-R2432	6125XLG-CMW710-F2428	2017-01-05	Release version	Added new features Modified features Fixed bugs

Version number	Last version	Release date	Release type	Remarks
6125XLG-CMW710-F2428	6125XLG-CMW710-F2426	2016-05-05	Feature version	Added new features Modified features Fixed bugs
6125XLG-CMW710-F2426	6125XLG-CMW710-R2423	2016-02-02	Feature version	Added new features Modified features Fixed bugs
6125XLG-CMW710-R2423	6125XLG-CMW710-R2422P02	2015-11-19	Release version	Added new features Modified features Fixed bugs
6125XLG-CMW710-R2422P02	6125XLG-CMW710-R2422P01	2016-09-01	Release version	Modified features • Modified feature: NTP support for ACL Fixed bugs
6125XLG-CMW710-R2422P01	6125XLG-CMW710-R2422	2015-12-18	Release version	Added new features New feature: Peer Zone Modified features Fixed bugs
6125XLG-CMW710-R2422	6125XLG-CMW710-R2418P01	2015-11-13	Release version	Added new features Modified features Fixed bugs HPE rebranding.
6125XLG-CMW710-R2418P01	6125XLG-CMW710-R2417	2015-05-29	Release version	Added features: • Link-aggregation load sharing for MAC-in-MAC traffic • Enabling Monitor Link globally • NETCONF logging • Displaying the load sharing path selected for a flow • Symmetric load sharing • Displaying the PFC information for an interface • Link-aggregation traffic forwarding information display • 802.1X online user handshake reply • MAC authentication requests carrying user IP addresses • Authentication interval for users in the MAC authentication guest VLAN • Local portal Web server • BGP IPv4 MDT address family • Displaying BGP MDT routing informaiton Modified features: • The default user role feature for remote AAA users • ARP MAD configuration • Displaying BGP peer group information • Displaying BGP peer or peer group information • Displaying BGP update group information

Version number	Last version	Release date	Release type	Remarks
				• Resetting BGP sessions • Enabling route reflection between clients • Configuring the cluster ID for a route reflector • Enabling BGP to exchange routing information with a peer or peer group • Displaying default-group information Fixed bugs.
6125XLG-CMW710-R2417	6125XLG-CMW710-R2406P02	2015-02-06	Release version	Added features: • Login delay • Disabling SSL 3.0 • Outgoing packets filtering on a portal-enabled interface • Link-aggregation load sharing for MAC-in-MAC traffic • NQA UDP tracert operation • NQA UDP template • Output interface for probe packets • PIM NSR • IPv6 PIM NSR • Support for LLDP configuration on IRF physical interfaces • Disabling PVID inconsistency check • EEE energy saving for an Ethernet interface MDIX mode of an Ethernet interface • Testing the cable connection of an Ethernet interface Modified features: • Setting the duplex mode for an Ethernet interface • Setting the speed for an Ethernet interface • Port status detection timer • Configuring the NQA HTTP template • User roles for a schedule • Support for advertising the COMMUNITY attribute to a peer or peer group in new views • Configuring an NSSA area • Packet statistics for Ethernet service instances Fixed bugs.
6125XLG-CMW710-R2406P02	6125XLG-CMW710-R2406P01	2014-12-30	Release version	None
6125XLG-CMW710-R2406P01	6125XLG-CMW710-R2406	2014-9-15	Release version	None
6125XLG-CMW710-R2406	6125XLG-CMW710-R2403	2014-8-9	Release version	None

Version number	Last version	Release date	Release type	Remarks
6125XLG-CMW710-R2403	6125XLG-CMW710-R2402	2014-3-6	Release version	None
6125XLG-CMW710-R2402	6125XLG-CMW710-E2402	2014-1-9	Release version	None
6125XLG-CMW710-E2402	6125-CMW710-R2306	2013-12-13	ESS version	None
6125-CMW710-R2306	6125-CMW710-E2302	2013-8-28	Release version	None
6125-CMW710-E2302	First release	2013-6-07	ESS version	None

Hardware and software compatibility matrix

Table 2 Hardware and software compatibility matrix

Item	Specifications
Product family	HPE 6125XLG Blade Switch
Hardware platform	HPE 6125XLG Blade Switch
Memory	2GB DDR3
Flash	512MB Nand Flash
BootWare image	Shipped with the switch. (Use the **display version** command in any view to view the BootWare version.)
System software image	6125XLG-CMW710-R2432P03.ipe
iMC version	iMC BIMS 7.2 (E0402) iMC EAD 7.2 (E0402) iMC TAM 7.2 (E0402) iMC UAM 7.2 (E0402) iMC MVM 7.2 (E0402) iMC NTA 7.2 (E0401) iMC PLAT 7.2 (E0403P04) iMC QoSM 7.2 (E0403) iMC RAM 7.2 (E0402) iMC SDNM 7.2 (E0402) iMC SHM 7.2 (E0402) iMC UBA 7.2 (E0401) iMC VCM 7.2 (E0402) iMC VFM 7.2 (E0403)

Item	Specifications
iNode version	iNode PC 7.2 (E0401)

To display version information for the system software and Boot ROM of 6125xlg:

```
<HPE> display version
HPE Comware Software, Version 7.1.045, Release 2432P03
Copyright (c) 2010-2017 Hewlett-Packard Enterprise Development L.P.
HPE 6125XLG Blade Switch uptime is 0 weeks, 0 days, 0 hours, 2 minutes
Last reboot reason : Power on

Boot image: flash:/6125xlg-cmw710-boot-r2432p03.bin
Boot image version: 7.1.045, Release 2432P03
  Compiled Apr 07 2017 16:00:00
System image: flash:/6125xlg-cmw710-system-r2432p03.bin
System image version: 7.1.045, Release 2432P03
  Compiled Apr 07 2017 15:00:00

Slot 1
HPE 6125XLG Blade Switch with 2 Processors
Last reboot reason : Power on
2048M    bytes SDRAM
4M       bytes Nor Flash Memory
512M     bytes Nand Flash Memory
Hardware Version is Ver.B
CPLD Version is 002
BootWare Version is 109
[SubSlot 0] 16*10Gb/1Gb Downlinks + 4*10Gb CrossLinks
[SubSlot 1] 8*SFP Plus + 4*QSFP Plus
```

ISSU compatibility list

Table 3 ISSU compatibility list

Current version	Earlier version	ISSU compatibility
6125XLG-CMW710-R2432P03	6125XLG-CMW710-R2432P02	Yes
	6125XLG-CMW710-R2432P01	Yes
	6125XLG-CMW710-R2432	Yes
	6125XLG-CMW710-F2431	Yes
	6125XLG-CMW710-F2428	Yes
	6125XLG-CMW710-F2426	Yes
	6125XLG-CMW710-R2422P02	Yes
	6125XLG-CMW710-R2422P01	Yes

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 detailed information about feature configuration and commands.

Hardware feature updates

R2432P03

Support HPE 10GBase-T 813874-B21 Optical Transceiver Module.

R2432P02

None.

R2432P01

None.

R2432

None.

F2428

None.

F2426

None.

R2423

None.

R2422P02

None.

R2422P01

None.

R2422

None.

R2418P01

- Support SFP+ AOC.
- Support QSFP+ AOC.

R2417

- None.

R2406P02

- None.

R2406P01

- None.

R2406

Added support for the following modules:

- Support HPE X180 10G SFP+ LC LH 80km 1538.19nm DWDM Transceiver.
- Support HPE X180 10G SFP+ LC LH 80km 1537.40nm DWDM Transceiver.

R2403

None.

R2402

None.

E2402

First release.

Software feature and command updates

For more information about the software feature and command update history, see HPE 6125XLG-CMW710-R2432P03 Release Notes (Software Feature Changes).

MIB updates

Table 4 MIB updates

Item	MIB file	Module	Description
6125XLG-CMW710-R2432P03			
New	None	None	None
Modified	None	None	None
6125XLG-CMW710-R2432P02			
New	None	None	None
Modified	None	None	None
6125XLG-CMW710-R2432P01			
New	None	None	None
Modified	None	None	None
6125XLG-CMW710-R2432			
New	None	None	None
Modified	hh3c-entity-ext.mib	HH3C-ENTITY-EXT-MIB	Modified hh3cProcessTable Modified hh3cEntityExtPowerPhysicalIndex hh3cEntityExtNominalPower hh3cEntityExtCurrentPower
6125XLG-CMW710-F2428			
New	None	None	None
Modified	None	None	None
6125XLG-CMW710-F2426			
New	None	None	None
Modified	None	None	None
6125XLG-CMW710-R2423			
New	None	None	None
Modified	None	None	None
6125XLG-CMW710-R2422P02			
New	hh3c-ifqos2.mib	HH3C-IFQOS2-MIB	Added hh3cIfQoSHardwareQueueRunInfoTable
Modified	ieee8021-spb.mib	IEEE8021-SPB-MIB	Modified ieee8021SpbEctStaticTable
6125XLG-CMW710-R2422P01			
New	None	None	None
Modified	None	None	None

Item	MIB file	Module	Description
6125XLG-CMW710-R2422			
New	ieee8021-secy.mib ieee8021x-pae.mib hh3c-macsec.mib hh3c-common-system.mib rfc4044-fc-mgmt.mib	IEEE8021-SECY-MIB IEEE8021X-PAE-MIB HH3C-MACSEC-MIB HH3C-COMMON-SYSTEM-MIB FC-MGMT-MIB	Added IEEE8021-SECY-MIB Added IEEE8021X-PAE-MIB Added hh3cMACsecCFGPortTable Added hh3cSystemWorkingMode hh3cSystemWorkingModeTable Added fcmPortErrorsTable
Modified	ieee8021-secy.mib rfc2233-if.mib	IEEE8021-SECY-MIB IF-MIB	Modified secyTXSATable Modified ifTable
6125XLG-CMW710-R2418P01			
New	hh3c-flash-man.mib	HH3C-FLASH-MAN-MIB	Added hh3cFlhHCSize hh3cFlhPartHCSpace hh3cFlhPartHCSpaceFree hh3cFlhFileHCSize
Modified	None	None	None
6125XLG-CMW710-R2417			
New	hh3c-stack.mib	HH3C-STACK-MIB	Added hh3cStackDomainId
Modified	None	None	None
6125XLG-CMW710-R2406P02			
New	hh3c-stack.mib	HH3C-STACK-MIB	Added hh3cStackDomainId
Modified	None	None	None
6125XLG-CMW710-R2406P01			
New	None	None	None
Modified	rfc4444-isis.mib	ISIS-MIB (for TRILL)	isisCircLevelHelloMultiplier change “Range from 2 to 100” to “Range from 2 to 100”. isisCircLevelHelloTimerchange “Range from 3000” to “Range from 1000”.
6125XLG-CMW710-R2406			
New	hh3c-mpm.mib hh3c-splat-igsp.mib	HH3C-MPM-MIB HH3C-LswIGSP-MIB	For detailed information, see < Comware V7 S5820V2&S5830V2&HP6125XLG MIB

Item	MIB file	Module	Description
			Companion(R2406).docx>
Modified	hh3c-trap.mib lldp-ext-dot1-v2.mib hh3c-entity-ext.mib hh3c-lsw-dev-adm.mib rfc1213.mib hh3c-lsw-dev-adm.mib	HH3C-TRAP-MIB LLDP-EXT-DOT1-V2-MIB HH3C-ENTITY-EXT-MIB HH3C-LSW-DEV-ADM-MIB RFC1213-MIB HH3C-LSW-DEV-ADM-MIB	For detailed information, see < Comware V7 S5820V2&S5830V2&HP6125XLG MIB Companion(R2406).docx>
6125XLG-CMW710-R2403			
New	None	None	None
Modified	hh3c-config-man.mib lldp-ext-dot1-v2.mib hh3c-entity-ext.mib	HH3C-CONFIG-MAN-MIB LLDP-EXT-DOT1-V2-MIB HH3C-ENTITY-EXT-MIB	For detailed information, see < Comware V7 S5820V2&S5830V2&HP6125XLG MIB Companion(R2403)>
6125XLG-CMW710-R2402			
New	None	None	None
Modified	None	None	None
6125XLG-CMW710-E2402			
New	None	None	None
Modified	None	None	None

Operation changes

Operation changes in R2432P03

- Added the check for switching chip DMA and switching logic components

  This software version added the check for switching chip DMA and switching logic components to determine whether they are running correctly.
- Modified the value range of the interval for an OpenFlow instance to reconnect to a controller

  Before modification: The interval for an OpenFlow instance to reconnect to a controller is in the range of 10 to 120 seconds.

  After modification: The interval for an OpenFlow instance to reconnect to a controller is in the range of 1 to 120 seconds.

Operation changes in R2432P02

None.

Operation changes in R2432P01

None.

Operation changes in R2432

- Added support for domain name separators forward slashes (/) and back slashes (\).

  Before modification: When a user logs in to the device by using Telnet, SSH, or FTP, forward slashes (/) and back slashes (\) cannot be used as domain name separators.

  After modification: When a user logs in to the device by using Telnet, SSH, or FTP, forward slashes (/) and back slashes (\) can be used as domain name separators.
- Added response of IBGP to interface down events.

  Before modification: If an IBGP neighbor relationship is established through a directly-connected interface and the **peer connect-interface** command is used to specify a source interface or source address for establishing TCP connections to a peer or peer group, when the corresponding interface (a non-loopback interface) goes down, BGP must wait for the hold timer to expire before disconnecting the neighbor relationship. Before the neighbor relationship is disconnected, route blackholes will appear.

  After modification: If an IBGP neighbor relationship is established through a directly-connected interface and the **peer connect-interface** command is used to specify a source interface or source address for establishing TCP connections to a peer or peer group, when the corresponding interface (a non-loopback interface) goes down, BGP immediately disconnects the neighbor relationship. This implementation accelerates route convergence.
- Added support for connecting member ports of two local Layer 3 dynamic aggregate interfaces.
  - Before modification: If two Layer 3 Ethernet interfaces on the device are assigned to different dynamic aggregation groups, the interfaces cannot be Selected when they are connected.
  - After modification: If two Layer 3 Ethernet interfaces on the device are assigned to different dynamic aggregation groups, the interfaces can be Selected when they are connected.
- Added support for configuring the MAC address for a Layer 3 Ethernet subinterface or Layer 3 aggregate subinterface.

  Before modification: You cannot configure the MAC address for a Layer 3 Ethernet subinterface or Layer 3 aggregate subinterface.

  After modification: You can configure the MAC address for a Layer 3 Ethernet subinterface or Layer 3 aggregate subinterface.
- Changed the value of "Input interface" field for outgoing unicast packets sampled by sFlow.

  Before modification: This field displays **N/A**.

  After modification: This field displays the name of the input interface.
- Added the support for deploying an extensibility flow entry with match field VLAN ID 0000 and action **push vlan**.

  Before modification: The extensibility flow entry cannot be deployed.

  After modification: The extensibility flow entry can be deployed.
- Modified the method for assigning FIPS NORMAL ACLs to aggregate interfaces.

  Before modification: The device assigns FIPS NORMAL ACLs to aggregate interfaces on a per-member-port basis.

  After modification: The device assigns FIPS NORMAL ACLs to aggregate interfaces on a per-aggregation-group basis.
- Added support for NSR after MDT is configured for BGP

  Before modification, NSR is not supported after MDT is configured for BGP.

  After modification, NSR is supported after MDT is configured for BGP.

Operation changes in F2428

- Added support of NETCONF for the **ospf bfd enable** command

  Before modification, NETCONF does not support the **ospf bfd enable** command.

  After modification, NETCONF supports the **ospf bfd enable** command.
- Modified the **Vendor** field in the **display install package all** command output

  Before modification, the Vendor field displays **HP**.

  After modification, the Vendor field displays **HPE**.
- Modified the LLDP aggregation port ID index carried by an aggregation group member port

  Before modification, the LLDP aggregation port ID index carried by an aggregation group member port is the ifindex of the port.

  After modification, the LLDP aggregation port ID index carried by an aggregation group member port is the ifindex of the aggregate interface.
- Modified the maximum number of static multicast MAC address entries

  Before modification, the maximum number of static MAC address entries is 256.

  After modification, the maximum number of static MAC address entries is 4096.
- Modified the forwarding method for traffic matching two flow tables

  Before modification, if packets match both OpenFlow table 0 and table 1, and table 1 is ineffective, the switch forwards the packets by using table 0.

  After modification, if packets match both OpenFlow table 0 and table 1, and table 1 is ineffective, the switch forwards the packets by using table 1.

Operation changes in F2426

- The maximum number of secondary IP addresses supported on an interface was changed from 64 to 1024.
- Modified the processing of tagged frames on the incoming interfaces for the encapsulation default command

  Before modification, an interface does not process the VLAN tags of incoming frames.

  After modification, an interface removes the VLAN tags of incoming frames.
- Added the unit pps to the car command

  Before modification, you can configure the CIR and PIR only in kbps in the **car** command.

  After modification, you can configure the CIR and PIR in kbps or pps in the **car** command.
- Increased the length of error packets that a controller can capture

  Before modification, a controller can capture error packets with the length of 64 bytes.

  After modification, a controller can capture error packets with the length of 128 bytes.

Operation changes in R2423

None.

Operation changes in R2422P02

- Modified the default of endless loop detection

  Before modification, endless loop detection is disabled by default.

After modification, endless loop detection is enabled by default.

- Logging of reboots triggered by watch dog timer expiration

  This release added logging of reboots triggered by watch dog timer expiration. Error information is recorded after the system is rebooted for expiration of the watch dog timer.

Operation changes in R2422P01

None.

Operation changes in R2422

- Added the DSCP priority field to OpenFlow and NETCONF protocol packets before sending them.

  Before modification, these packets do not carry the DSCP priority field.

  After modification, these packets carry the DSCP priority field.

- Added the auto restart feature in high temperature environments.

  Added the auto restart feature for the switch to restart repeatedly to protect the hardware when the temperature of the switch reaches the upper limit.

- Modified the processing flow for DHCP and ARP packets on a VSI when the switch acts as a DHCP server.

  Before modification, a VSI sends DHCP and ARP packets to the CPU for processing.

  After modification, an OpenFlow entry is used to permit the DHCP and ARP packets received on a VSI. The packets are not sent to the CPU.

- Modified the value of the VRF field in the information obtained through the GET/GET-BULK operation for the BGP Netconf SessionCounts table.

  Before modification, the VRF field displays the number of VRF sessions for both public and private networks.

  After modification, the VRF field displays the number of VRF sessions for the public network.

- Added statistics for the meter action in an OpenFlow instance.

  Before modification, the meter action rate-limits normal data packets.

  After modification, the meter action rate-limits normal data packets and collects statistics about forwarded packets and dropped packets.

- Added check for outbound traffic forwarding on an interface.

  Before modification, check for outbound traffic forwarding on an interface is not supported.

  After modification, check for outbound traffic forwarding on an interface is supported. When outbound traffic forwarding is not operating correctly, the system displays logs.

- Change to the return value for a multi-part request sent by a port that is not in an OpenFlow instance.

  Before modification, the return value is port error.

  After modification, the return value is bad queue error.

- Increased the maximum number of Layer 3 subinterfaces supported by a port from 512 to 1024 .

- Increased the maximum number of syslog servers that can be configured on a switch from 4 to 20.

- Added support for processing broadcast ARP requests.

  Before modification, the switch does not support broadcast ARP requests.

  After modification, the switch supports broadcast ARP requests.

- Change to the default rate limits for OSPF protocol packets in hardware, software, and CPU queues.

  Before modification, the default rate limits for OSPF protocol packets are as follows:
  - Hardware: 256 kbps.
  - Software: 100 pps.
  - CPU queue: 200 pps.

  After modification, , the default rate limits for OSPF protocol packets are as follows:
  - Hardware: 1 Mbps.
  - Software: 1000 pps.
  - CPU queue: 2000 pps.
- Added the following functions to NETCONF:
  - Network querying and summary route querying for BGP.
  - Routing policy.
- Added support for tunnel interfaces to OpenFlow:
  - Before modification, flow entries do not support tunnel interfaces.
  - After modification, flow entries support tunnel interfaces.
- Added support for the **mac-address static source-check enable** command in Layer 2 aggregate interface view and Layer 3 aggregate interface view.

Operation changes in R2418P01

- Increased the maximum number of secondary VLANs that can be associated with a primary VLAN from 96 to 256.
- Change to the count of IfInDiscards for an IRF physical interface

  Before modification, the value of dropped packets by blocking is collected.

  After modification, the value of dropped packets by blocking is not collected.

Operation changes in R2417

- Modified the **Protection** field in the **display stp** command output.

  Before modification, the **Protection** field displays the protection type configured for an interface.

  After modification, the **Protection** field displays the active protection type on an interface.
- Enhanced the feature of establishing neighborship through LLDP

  Before modification, LLDP cannot establish neighborship when both PSE and PD features are set in the TLVs sent by the neighbor.

  After modification, LLDP can establish neighborship when both PSE and PD features are set in the TLVs sent by the neighbor.
- Change to the forwarding of CRC error frames after the **cut-through enable** command is used to enable cut-through forwarding

  Before modification, the switch cannot forward CRC error frames after cut-through forwarding is enabled.

  After modification, the switch supports forwarding CRC frames after cut-through forwarding is enabled.
- Change to the rate limit

  Before modification, the rate limit for the following item is 200 pps.

```
120 OFP_MISS          0      0          0          200  S   On  SMAC 0
121 OFP_MATCH         0      0          0          200  S   On  SMAC 0
122 OFP_DEVCONF       0      43         0          200  S   On  SMAC 0
123 OFP_MACIP_MISS    0      0          0          200  S   On  SMAC 0
```

After modification, the rate limit is 600 pps.

- Change to the priority of OpenFlow protocol packets

  Before modification, the OpenFlow protocol packets are assigned to queue 2 of the CPU.

  After modification, the OpenFlow protocol packets are assigned to queue 41 of the CPU.

Operation changes in R2406P02

- Clearing the useless fields of zone merge packets

  Before modification, some reserved fields of zone merge packets are set to random values rather than cleared. These fields are useful in later versions. As a result, zone merge might fail during interoperation with later versions.

  After modification, the reserved fields in zone merge packets are cleared to ensure interoperation with later versions.

- Change to using the DHCPv6 client to obtain IPv6 addresses

  Before modification, route prefixes cannot be obtained through RA messages.

  After modification, route prefixes can be obtained through RA messages.

- Enhanced the feature of establishing neighbor ship through LLDP

  Before modification, LLDP cannot establish neighbor ship when both PSE and PD features are set in the TLVs sent by the neighbor.

  After modification, LLDP can establish neighbor ship when both PSE and PD features are set in the TLVs sent by the neighbor.

- Support of OpenFlow for adding and deleting flow entries with invalid buffer IDs

  Before modification, when OpenFlow issues or deletes a flow entry, it checks the buffer ID carried in the packet. If the buffer ID does not exist, OpenFlow does not add or delete the flow entry, and it returns an error code.

  After modification, when OpenFlow issues or deletes a flow entry, it checks the buffer ID carried in the packet. If the buffer ID does not exist, OpenFlow continues to add or delete the flow entry, and it prints a trace message.

- Added a command to configure dropping for packets with options

  Before modification, Layer 2 and Layer 3 packets with options are dropped.

  After modification, the **packet-filter filter** { **route | all** } command is added. If the command is executed with the **route** keyword, Layer 3 packets with options are dropped. If the command is executed with the **all** keyword, Layer 2 and Layer 3 packets with options are dropped.

- Collecting statistics about packets that do not match flow entries in an OpenFlow network

  Before modification, the number of replies to aggregate statistic multi-part requests does not contain the number of packets that do not match flow entries.

  After modification, the number of replies to aggregate statistic multi-part requests contains the number of packets that do not match flow entries.

- Collecting port statistics at a nanosecond-level interval in an OpenFlow network

  Before modification, OpenFlow does not support collecting reply statistics for a port at a nanosecond-level interval.

  After modification, OpenFlow supports collecting reply statistics for a port at a nanosecond-level interval.

- Cancelling responding to OpenFlow multipart reply messages with blank messages

Before modification, the system responds to a multipart reply message with two messages. The second message is blank, which indicates that the message ends.

After modification, the system does not respond to a multipart reply message with a blank message.

- Change to the response to the pop VLAN action in an OpenFlow network

  Before modification, when a pop VLAN action is executed for packets that match flow entries and do not have VLAN tags, the switch returns an OFPET_BAD_ACTION OFPBAC_MATCH_INCONSISTENT error message.

  After modification, when a pop VLAN action is executed for packets that match flow entries and do not have VLAN tags, the switch returns an OFPBAC_BAD_TYPE message.

- Returning error codes when the switch receives unsupported configuration sets in an OpenFlow network

  Before modification, when the switch receives unsupported configuration sets in an OpenFlow network, the switch ignores them and does not return error codes to the controller.

  After modification, when the switch receives unsupported configuration sets in an OpenFlow network, the switch returns error codes to the controller.

- Change to the processing when the packet out action is modified into the normal action in an OpenFlow network

  Before modification, when the packet out action is modified into the normal action, Layer 2 packets whose destination MAC address is not the MAC address of a local VLAN interface and Layer 2 packets that do not match MAC address entries are dropped.

  After modification, when the packet out action is modified into the normal action, Layer 2 packets whose destination MAC address is not the MAC address of a local VLAN interface and Layer 2 packets that do not match MAC address entries are broadcast.

- Change to the output for the startup self test on a switch in non-FIPS mode

  Before modification, when the switch operates in non-FIPS mode, the following output appears for the startup self test:

```
Cryptographic Algorithms Tests are running ...
Slot 1:
Starting Known-Answer tests in the user space.
Known-answer test for SHA1 passed.
Known-answer test for SHA224 passed.
Known-answer test for SHA256 passed.
Known-answer test for SHA384 passed.
Known-answer test for SHA512 passed.
Known-answer test for HMAC-SHA1 passed.
Known-answer test for HMAC-SHA224 passed.
Known-answer test for HMAC-SHA256 passed.
Known-answer test for HMAC-SHA384 passed.
Known-answer test for HMAC-SHA512 passed.
Known-answer test for AES passed.
Known-answer test for RSA(signature/verification) passed.
Pairwise conditional test for RSA(signature/verification) passed.
Pairwise conditional test for RSA(encrypt/decrypt) passed.
Pairwise conditional test for DSA(signature/verification) passed.
Pairwise conditional test for ECDSA(signature/verification) passed.
Known-answer test for DRBG passed.
Known-Answer tests in the user space passed.
Starting Known-Answer tests in the kernel.
Known-answer test for AES passed.
```

```
Known-answer test for SHA1 passed.
Known-answer test for HMAC-SHA1 passed.
Known-Answer tests in the kernel passed.
Cryptographic Algorithms Tests passed.
```

After modification, when the switch operates in non-FIPS mode, the following output appears for the startup self test:

```
Cryptographic algorithms tests passed.
```

- Change to the random number algorithm

  Before modification, the randomness of random numbers generated by the random number algorithm is low.

  After modification, the randomness of random numbers generated by the random number algorithm is high.

- Change to the prompt message if the underlayer resources are insufficient when the ip verify source command is used

  Before modification, when the underlayer resources are insufficient, no message appears, a user can obtain an IP address, but the user cannot access the network.

  After modification, the following message appears when the underlayer resources are insufficient.

```
Failed to add an IP source guard binding (IP 1.1.1.1, MAC 0001-0001-0001, and VLAN 65535)
on interface Vlan-interface1. Feature not supported.
```

- Change to the maximum number of characters allowed in the system prompt

  Before modification, the system prompt can contain up to 127 characters, and the exceeding characters are truncated.

  After modification, the system prompt can contain up to 360 characters.

- A domain ID cannot contain letters

  Before modification, when the domain ID is configured as 123abc in the configuration file and the switch starts up with the configuration file, the domain ID is automatically parsed into 123. A domain ID cannot be configured as 123abc at the CLI.

  After modification, when a domain ID contains letters, it cannot be issued either in a configuration file or at the CLI. A domain ID must meet the following requirements:

  - A domain ID supports 0 and positive decimal integers, and does not support negative numbers.
  - A domain ID can start with multiple zeros, for example, 000123568.
  - The domain ID configuration command supports multiple spaces, for example, irf   domain 333
  - The domain ID configuration command supports adding a plus sign before the domain ID, for example, irf domain +333
  - A domain ID can be up to 4294967295. When you configure the **irf domain 4294967296** command, the configuration fails and the domain ID will be set to the default value (0).

- Change to the output from the display openflow instance command

  Before modification, the output does not contain a colon after the **Classification** field, as follows:

```
Classification VLAN, total VLANs(1)
```

After modification, the output contains a colon after the **Classification** field, as follows:

```
Classification: VLAN, total VLANs(1).
```

Operation changes in R2406P01

- Added the **bcm** *slot-number* **0 show/c** command to show MAC chip statistics in the output from the **display diagnostic-information** command.
- Added a default setting of **ipv6 dhcp client duid** to configure DUID for the DHCPv6 client (blade) on the management Ethernet port:

  Before modification, the switch uses the bridge MAC address as the DUID of the DHCPv6 client on the management Ethernet port after the switch starts up using default settings.

  After modification, the switch uses the MAC address of the management Ethernet port as the DUID of the DHCPv6 client on the management Ethernet port after the switch starts up using default settings.
- Added a requirement of configuring a multiport service loopback group by using **service-loopback group** for multiport ARP:

  Before modification, there is no need to configure a multiport service loopback group for multiport ARP.

  After modification, a multiport service loopback group must be configured to support multiport ARP.

Operation changes in R2406

- Change to management user login information:

  Before modification, the system does not record login failure times for management users.

  After modification, the system, if enabled with password control, displays the last login time, and the number of login failure times between the last login and this login for a management user that logs into the system.
- Change to user authentication and login information:

  Before modification, the system does not record information about authentication success, authentication failure, login, and logout for users.

  After modification, the system records information about authentication success, authentication failure, login, and logout for users.
- Change to FIPS log information:

  Before modification, if the old password entered for password modification is incorrect, the switch in FIP mode prompts a message but does not record the message.

  After modification, if the old password entered for password modification is incorrect, the switch in FIP mode prompts a message and records the message.
- Change to the maximum number of IPv6 routes that have a prefix longer than 64 bits:

  Before modification, the maximum number of IPv6 routes that have a prefix longer than 64 bits is 128.

  After modification, the maximum number of IPv6 routes that have a prefix longer than 64 bits is 256.
- Change to MAC learning for LLDP:

  Before modification, the switch learns the source MAC addresses of LLDP packets.

  After modification, the switch does not learn the source MAC addresses of LLDP packets.
- Change to SSH login banner information:

  Before modification, the SSH login banner information is displayed in the sequence of username, password, copyright, legal, motd, login, and shell.

  After modification, the SSH login banner information is displayed in the sequence of username, login, password, copyright, legal, motd, and shell.

- Change to the number of MAC addresses that can be displayed:

  Before modification, MAC addresses from the maximum number of preserved MAC addresses plus 1 to the maximum number of preserved MAC addresses plus 41 cannot be displayed. Preserved MAC addresses include the bridge MAC address and Layer 3 interfaces' MAC addresses. Preserved MAC addresses are from the bridge MAC address to the bridge MAC address plus n. The following shows the value of n on different switch models:

  - 85 for HPE 6125XLG Blade Switch.

  After modification, MAC addresses from the maximum number of preserved MAC addresses plus 1 to the maximum number of preserved MAC addresses plus 41 can be displayed.

- Change to BGP MED operation

  Before modification, BGP considers a MED being 0 and a MED being empty are different values. Routes with those MEDs cannot form ECMP routes.

  After modification, BGP considers a MED being 0 and a MED being empty are the same value. Routes with those MEDs can form ECMP routes.

- Change to the maximum number of IRF physical ports in an IRF port

  Before modification: Up to four physical ports can be bound to an IRF port.

  After modification: Up to eight physical ports can be bound to an IRF port.

- Added support for both Ctrl+D and Ctrl+C to quit automatic configuration:

  Before modification, the command for quitting automatic configuration is Ctrl+D in R2403, R2402, and E2402.

  After modification, both Ctrl+C and Ctrl+D for quitting automatic configuration are supported.

- Changed the default transfer mode for the FTP client from ASCII to Binary.

- Added support for carrying multiple values in the level attribute assigned by the login server:

  Before modification, the level attribute assigned by the login server carries no or one value.

  After modification, the level attribute assigned by the login server carries multiple values.

- Changed ARP/ND learning method for private VLAN:

  Before modification, ARP/ND entries are learned in the secondary VLAN.

  After modification, ARP/ND entries are learned in the primary VLAN.

- Changed ACL policy for OSPF:

  Before modification, the system reserves 256 ACLs for OSPF that are used to identify OSPF packets encapsulated in TRILL packets, regardless of whether TRILL is enabled.

  After modification, the system does not reserve 256 ACLs for OSPF if TRILL is not enabled.

Operation changes in R2403

- hh3cPeriodicalTrap removed

  Before modification, hh3cPeriodicalTrap was sent every 60 seconds by default, after SNMP trap host is configured.

  After modification, this trap is no longer sent by the switch.

Operation changes in R2402

- Action changes for OAM down state

  Before modification, if the physical layer of an interface that is in OAM down state goes down, the flag for OAM down state is removed. After the physical layer of the interface goes up, the OAM down state cannot be recovered. If the physical layer of an interface where an OAM connection has been established goes down, the OAM down state is not set for the interface.

After modification, if the physical layer of an interface that is in OAM down state goes down, the flag for OAM down state is kept. After the physical layer of the interface goes up, the interface is still in OAM down state. If the physical layer of an interface where an OAM connection has been established goes down, the OAM down state is set for the interface.

- Changes to 802.1X/MAC authentication users per interface

  Before modification, 802.1X authentication, MAC authentication, or port security supports a maximum of 1024 concurrent users on an interface ;an interface card supports a maximum of 1024 secure MAC addresses.

  After modification, 802.1X authentication, MAC authentication, or port security supports a maximum of 2048 concurrent users on an interface ;an interface card supports a maximum of 2048 secure MAC addresses.

- Display command response time

  Before modification, most display commands have unacceptable interruption during information output. This symptom is more evident when a question mark is input or a Tab is pressed to complete a keyword.

  After modification, this problem no longer exists.

- PFC and flow-control

  Before modification, **priority-flow-control no-drop dot1p** and **flow-control** commands can both be issued.

  After modification, **priority-flow-control no-drop dot1p** and **flow-control** commands cannot be both issued.

- ACL-based packet filtering on a VLAN interface

  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.

Operation changes in E2402

None.

Restrictions and cautions

- PFC does not work on an IRF fabric where **burst-mode** is enabled, the traffic egress port belongs to a 6125XLG blade switch, and the traffic ingress port belongs to another switch.
- If more than 7 VSANs are configured on a 6125XLG blade switch's VFC interface that connects to HPE storage device, the 6125XLG blade switch cannot establish a connection to HPE storage.

Use one of the following methods to avoid this problem:

  - Change the default VLAN on the FCoE port of HPE storage to a VLAN that is permitted by the connected port on the 6125XLG blade switch.
  - Change the configuration on 6125XLG blade switch; configure one VSAN on the VFC interface that connects to HPE storage device.

- Since version R2422, H3C switches cannot load HPE software, and HPE switches cannot load H3C software.

Open problems and workarounds

LSV7D008033

- Symptom: An SSH connection cannot be terminated by using the compound key CTRL+C or CTRL+K.
- Condition: This symptom occurs when you use the compound key CTRL+C or CTRL+K to terminate a connection to the SSH server.
- Workaround: None.

201509180260

- Symptom: ARP information moves successfully between interfaces after the switch receives RARP requests, but the MAC address move records displayed by using the **display mac-address mac-move** command are incorrect.
- Condition: This symptom might occur if the **display mac-address mac-move** command is executed.
- Workaround: None.

List of resolved problems

Resolved problems in R2432P03

201704120179

- Symptom: A TRILL-enabled IRF fabric cannot forward part of TRILL traffic after loops are eliminated automatically from the TRILL network.
- Condition: This symptom might occur if loops are eliminated automatically from a TRILL network.

201703300059

- Symptom: In a dynamic aggregation group, interface A is Selected, and interface B is Unselected. After interface A is removed from the aggregation group, interface B becomes Selected, and the two interfaces cannot communicate.
- Condition: This symptom might occur if the following operations are performed:
    - **a.** Execute **link-aggregation lacp traffic-redirect-notification enable** in system view.
    - **b.** Set the mode of an aggregation group to dynamic.
    - **c.** Assign interface A to the aggregation group. The interface becomes Selected.
    - **d.** Assign interface B to the aggregation group. The interface becomes Unselected.
    - **e.** Remove interface A from the aggregation group.

201703290336

- Symptom: Member interfaces of an aggregation group might fail to be Selected when certain operations are repeatedly performed.
- Condition: This symptom might occur if the following operations are repeatedly performed:
    - **a.** Create an aggregation group and assign interfaces to it.
    - **b.** Remove the aggregation member interfaces and delete the aggregation group.

201703280369

- Symptom: The **issu commit** command fails to complete an ISSU.

- Condition: This symptom occurs if the following operations are performed:
  a. Three or more devices form a ring-topology IRF fabric.
  b. Perform an ISSU to downgrade the software from version R2432, R2432P01, or R2432P02 to an earlier version and execute the **issu commit** command to complete the ISSU.

201703210044

- Symptom: Constant BFD session flapping occurs after an IRF master/subordinate switchover.
- Condition: This symptom might occur if a master/subordinate switchover occurs on an IRF fabric after BFD is enabled and the running configuration is saved.

201703110247

- Symptom: After an interface is split into four breakout interfaces, only one breakout interface is up.
- Condition: This symptom might occur if the following operations are performed on an interface:
  a. Install an adaptor into the interface, split the interface into four breakout interfaces, and combine the breakout interfaces.
  b. Remove the adaptor.
  c. Install a 40-GE transceiver module into the interface and split the interface into four breakout interfaces.

201703060503

- Symptom: OSPF route calculation errors result in residual routes.
- Condition: This symptom might occur if the switch learns multiple routes that have the same network address and different mask lengths from Type-3 LSAs after OSPF neighbor relationships are established.

201703060484

- Symptom: Packet loss occurs on a dynamic aggregate interface if it is configured as an edge aggregate interface and the member ports do not receive LACPDUs.
- Condition: This symptom might occur if the member ports of an edge aggregate interface do not receive LACPDUs.

201704060499

- Symptom: The **openflow shutdown** setting on an IRF subordinate member might be missing after the IRF fabric reboots.
- Condition: This symptom might occur if the **openflow shutdown** command is executed on a subordinate member of an IRF fabric configured with OpenFlow and the IRF fabric reboots.

201704060491

- Symptom: On an OpenFlow-enabled IRF fabric, the status of an interface becomes **OFP DOWN** after the controller issues the port_mod(up) setting to the interface.
- Condition: This symptom might occur if the following conditions exist:
  a. The **openflow shutdown** command is executed on an interface.
  b. The controller issues the port_mod(up) setting to the interface.
  c. An IRF master/subordinate switchover occurs.

201703060493

- Symptom: The switch is connected to an upstream ZTE device in an MPLS TE network, and the tunnel to the ZTE device cannot come up because RSVP fails to set up a CRLSP.
- Condition: This symptom might occur if the switch is connected to an upstream ZTE device in an MPLS TE network.

201702220649

- Symptom: CVE-2017-3731
- Condition: OpenSSL is prone to denial-of-service vulnerability. An attacker may exploit this issue to crash the application, resulting in denial-of-service condition.
- Symptom: CVE-2017-3732
- Condition: OpenSSL is prone to an information-disclosure vulnerability. An attacker can exploit this issue to gain access to sensitive information that may aid in further attacks.

201612050642

- Symptom: CVE-2016-7427
- Condition: The broadcast mode of NTP is expected to only be used in a trusted network. If the broadcast network is accessible to an attacker, a potentially exploitable denial of service vulnerability in ntpd's broadcast mode replay prevention functionality can be abused. 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.
- Symptom: CVE-2016-7428
- Condition: The broadcast mode of NTP is expected to only be used in a trusted network. If the broadcast network is accessible to an attacker, a potentially exploitable denial of service vulnerability in ntpd's broadcast mode poll interval enforcement functionality can be abused. To limit abuse, ntpd restricts the rate at which each broadcast association will process incoming packets. ntpd will reject broadcast mode packets that arrive before the poll interval specified in the preceding broadcast packet expires. 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.
- Symptom: CVE-2016-7431
- Condition: Zero Origin timestamp problems were fixed by Bug 2945 in ntp-4.2.8p6. However, subsequent timestamp validation checks introduced a regression in the handling of some Zero origin timestamp checks.

201702140091

- Symptom: The processes might exit abnormally.
- Condition: This symptom occurs if IRF master/subordinate switchover is performed frequently.

201701220483

- Symptom: The switch reboots unexpectedly when certain operations are performed.
- Condition: This symptom occurs if the following operations are performed:
  - **a.** Two or more equal-cost BGP routes exist for IPv6 traffic. Both the source address and destination address of the IPv6 traffic have equal-cost routes in the BGP routing table.
  - **b.** sFlow sampling is configured on the incoming interface or outgoing interface of the traffic.
  - **c.** The **balance** command is configured on two BGP neighbor devices.

Resolved problems in R2432P02

201702170070

- Symptom: Attempt to change a Layer 2 interface to a Layer 3 interface (routed mode) fails, and the console port stops responding.
- Condition: This symptom might occur if the following operations have been performed:
  - **a.** Enable MAC authentication on the switch.

b. Issue ACLs to the switch from IMC.

c. Set the operating mode of the interface to routed mode when a large number of MAC authentication users are online.

201701200084

- Symptom: IMC cannot display information about the ports on the switch.
- Condition: This symptom might occur when IMC reads port information from the switch.

Resolved problems in R2432P01

201701120396

- Symptom: The system prompts that "MAD BFD cannot be configured in this interface." when BFD MAD is enabled on a VLAN interface by using the **mad bfd enable** command.
- Condition: None.

201612300373

- Symptom: The device might reboot unexpectedly.
- Condition: This symptom occurs with a low probability if the CPU sends a unicast IP packet and the destination IP address of the packet is deleted from the outgoing interface.

201701130106

- Symptom: Multicast traffic cannot be forwarded correctly.
- Condition: This symptom occurs if the following tasks are performed on the switch:
  a. Create a Layer 3 aggregation group and add multiple Layer 3 interfaces to the aggregation group.
  b. Enable PIM-SM or PIM-DM on the Layer 3 aggregate interface.

201612280545

- Symptom: A user fails to change the password for logging in to the device.
- Condition: This symptom occurs if the user logs in to the device through the Web interface and clicks the **Change Password** button to change the password.

Resolved problems in R2432

201603140235

- Symptom: MPLS LDP neighbor flapping occurs when a MAC address is assigned to a multichassis Layer 3 aggregate interface on an IRF fabric.
- Condition: This symptom might occur if a MAC address is assigned to a multichassis Layer 3 aggregate interface on an IRF fabric.

201612130462

- Symptom: After an interface is configured as a customer-side port, IPv4 routes and ARP entries fail to be issued.
- Condition: This symptom occurs if the following operations are performed:
  - Execute the **arp mode uni** command on a VLAN interface, and bind the VLAN interface to a VPN instance. Configure another VLAN interface in the same way. ARP packets are transmitted between the two VLAN interfaces.

- Execute the **arp mode uni** command on a VSI interface，and bind the VSI interface to a VPN instance. Configure another VSI interface in the same way. ARP packets are transmitted between the two VSI interfaces.

201611280365

- Symptom: OSPF neighbor relationship cannot be established.
- Condition: This symptom occurs if the following operations are performed:
  a. Establish OSPF neighbor relationship among multiple devices, and configure the network type as P2MP for the OSPF interfaces.
  b. Execute the **reset ospf** command multiple times.

201611150075

- Symptom: After an interface is installed with a GE transceiver module, the interface cannot come up.
- Condition: This symptom occurs if the following operations are performed:
  a. Bind the interface to an IRF port, and then unbind the interface from the IRF port.
  b. Install a GE transceiver module in the interface.

201610270242

- Symptom: A service loopback group fails to be created.
- Condition: This symptom occurs if the following operations are performed:
  a. Before creating a service loopback group, configure multiport ARP entries on the device.
  b. Delete multiport ARP entries or clear all ARP entries.
  c. Configure multiport ARP entries again and create the service loopback group.

201608300066

- Symptom: Some NQA operation intervals are different from those configured.
- Condition: This symptom occurs if the device is configured with multiple NQA operations.

201612170183

- Symptom: STP loops might occur at a low probability.
- Condition: This symptom occurs if the following operations are performed:
  a. Configure STP on an IRF fabric.
  b. View the STP status after a master/subordinate switchover.

201612120417

- Symptom: The OpenFlow connections between the device and controller continuously flap.
- Condition: This symptom occurs if the following operations are performed:
  a. The device is configured with the OpenFlow connection backup feature by default.
  b. The whole IRF fabric is rebooted.

201612090546

- Symptom: After an IRF member device leaves an IRF fabric, the aggregation group member ports on the member device are not deleted from the OpenFlow instance.
- Condition: This symptom occurs if an IRF member device leaves an IRF fabric because the IRF physical interface that connects the master device to the member device is shut down.

201612090352

- Symptom: The aggregation group MAC address on the device is different from the MAC address reported to the controller.

- Condition: This symptom occurs if the aggregation group is down and the device reports the aggregation group MAC address to the controller.

201612080309

- Symptom: Though the Leap indicator is changed to 01 on the NTP packet sender, the Leap indicator is still 00 in the NTP packets received on the NTP packet receiver.
- Condition: This symptom occurs if NTP is configured and the Leap indicator field is manually changed to 01 on the NTP packet sender.

201612070503

- Symptom: Memory leaks occur in an OpenFlow instance.
- Condition: This symptom occurs if the OpenFlow instance is activated and then deactivated.

201611180181

- Symptom: When the configuration of the device is rolled back by using an .mdb configuration file, the Smart Link configuration is lost.
- Condition: This symptom occurs if the index of the interface configured with Smart Link changes.

201611070207

- Symptom: The LowFree memory of the device keeps decreasing.
- Condition: This symptom occurs if users frequently log in to the device by using SSH or Telnet.

201609060517

- Symptom: Because the bandwidth of a VFC interface uses the default value and does not respond to the bandwidth of the Layer 2 aggregate interface bound to the VFC interface, the FSPF route calculated is not the optimal route.
- Condition: This symptom occurs if the VFC interface is bound to a Layer 2 aggregate interface and the corresponding Layer 2 aggregation group has multiple member ports.

201611160492

- Symptom: A user might fail to log in to an IRF fabric through the console port of the master device.
- Condition: This symptom occurs if the following operations are performed:
  - **a.** Log out from the IRF fabric, and log in to the IRF fabric through the console port of the master device again.
  - **b.** Restart the ttymgr process.

201611100160

- Symptom: An OpenFlow controller receives incorrect PVID change logs.
- Condition: This symptom occurs if the following operations are performed:
  - **a.** An interface on the device and an OpenFlow controller establish a connection.
  - **b.** In interface view, change the link type of the interface from access to trunk.

201609070089/201611080312

- Symptom: The interface management process is always running and cannot be stopped. The CLI does not respond to input commands.
- Condition: This symptom occurs at a low probability if the following operations are performed:
  - **a.** Bind a 40-GE interface to an IRF port.
  - **b.** Unbind the 40-GE interface from its IRF port.
  - **c.** Split the 40-GE interface into four 10-GE breakout interfaces, and bind the 10-GE breakout interfaces to an IRF port.

d. Unbind the 10-GE breakout interfaces from the IRF port.

e. Repeat the steps above.

201611080299

- Symptom: All IRF member devices reboot unexpectedly at a low probability.
- Condition: This symptom occurs if the following operations are performed:

  a. Bind a 40-GE interface to an IRF port.

  b. Unbind the 40-GE interface from its IRF port.

  c. Split the 40-GE interface into four 10-GE breakout interfaces, and bind the 10-GE breakout interfaces to an IRF port.

  d. Unbind the 10-GE breakout interfaces from the IRF port

  e. Repeat the steps above.

201610170074/201611040063

- Symptom: The BGP sessions between BGP peers on the IRF master member might go down.
- Condition: This symptom occurs if the following operations are performed:

  a. Configure BGP NSR for the IRF fabric.

  b. A subordinate member device fails and the IRF fabric splits. As a result, the subordinate member device becomes MAD Down.

201611020283

- Symptom: Multicast packets cannot be forwarded.
- Condition: This symptom occurs if both 802.1X authentication and MAC authentication are configured in interface view.

201610260898

- Symptom: The CLI might fail to respond to input commands.
- Condition: This symptom occurs if the following operations are performed:

  a. An IRF fabric is connected to a server. Distributed aggregation groups are set up.

  b. A large number of LACP packets cause the LACP protocol to repeatedly flap.

201610260589

- Symptom: The memory leaks.
- Condition: This symptom occurs if the following operations are performed:

  a. Install and remove the patch file.

  b. Use the **install commit** command to refresh the next startup software image list for the master device.

201610210440

- Symptom: Switching an IRF physical interface to a normal Ethernet interface fails.
- Condition: This symptom occurs if the following operations are performed:

  a. Bind a physical interface to an IRF port.

  b. Install a GE transceiver module in the interface.

201609280064

- Symptom: A DHCP client fails to obtain an IP address.
- Condition: This symptom occurs if the following operations are performed:

  a. Configure the load sharing mode for an aggregation group spanning multiple IRF member devices.

b. Enable DHCP relay on all IRF member devices.
c. Use the **link-aggregation management-port** command to configure the management port for the aggregation group member ports.

201608050297

- Symptom: Some aggregation group member ports flap.
- Condition: This symptom occurs if the following operations are performed:
  a. Assign a large number of ports to an aggregation group.
  b. In aggregation group view, configure the **port trunk permit vlan all** command.

201608240186

- Symptom: Deleting traffic behaviors failed.
- Condition: This symptom occurs if the following operations are performed:
  a. Configure 100 traffic classes and 100 traffic behaviors in a QoS policy.
  b. Configure a flow mirroring action in a traffic behavior.
  c. Apply the QoS policy to 10-GE breakout interfaces split from a 40-GE interface.
  d. Combine the breakout interfaces, and delete the traffic behaviors in the QoS policy.

201611030383/201610290030

- Symptom: The CLI does not respond after a user logs in through a management interface or console port when certain conditions exist.
- Condition: This symptom might occur if the following conditions exist:
  a. Password control is enabled.
  b. A large number of users log in to the switch at the same time.

201610260431

- Symptom: An SSH or Telnet user cannot log in when certain conditions exist.
- Condition: This symptom might occur if the following conditions exist:
  a. SYN Cookie is enabled.
  b. The client is not directly connected to the switch.
  c. The SSH or Telnet user uses an IPv6 address of the switch.

201610120394

- Symptom: Memory leaks occur when more than 500 VLAN interfaces are created on the switch.
- Condition: This symptom might occur if more than 500 VLAN interfaces are created on the switch.

201608300620

- Symptom: It takes a long time to install a patch on the master device of an IRF fabric.
- Condition: This symptom occurs if this patch is first installed on the master device rather than the subordinate devices.

201610240077

- Symptom: After packets on GRE tunnel interfaces are decapsulated, the VRF IDs of L3 entries obtained are incorrect.
- Condition: This symptom occurs if the following operations are performed:
  a. Configure GRE tunnels on an IRF fabric.
  b. Associate GRE tunnel interfaces with VPN instances.
  c. Reboot the IRF fabric.

201611240492

- Symptom: A QoS policy fails to be applied.
- Condition: This symptom occurs if the OVSDB controller deploys a QoS policy that does not contain a DSCP marking action.

201609300136/201609300233

- Symptom: When binding a VFC interface to a physical interface fails, using the MIB to obtain the failure reason fails.
- Condition: This symptom occurs if the following operations are performed:
  a. On an FCF switch, create a VFC interface and bind the VFC interface to a physical interface.
  b. The binding fails.

201611180048

- Symptom: The switch prints parity error and recovery logs every five minutes.
- Condition: This symptom occurs if the L3 module has parity errors on the switch.

201611110084

- Symptom: An IRF master/subordinate switchover occurs unexpectedly and the OVSDB server function fails to be enabled after the switchover.
- Condition: This symptom occurs if the OVSDB server function is repeatedly enabled and disabled on an IRF fabric.

201611090112

- Symptom: An OVSDB controller fails to deploy a QoS policy.
- Condition: This symptom occurs if the controller deploys the QoS policy that contains a CAR action for rate limiting and the CAR rate limit parameters are not configured according to the granularity.

201610310073

- Symptom: Incompatibility problems occur after the software is upgraded for the device configured with OVSDB.
- Condition: This symptom occurs if the following operations are performed:
  a. Start the OVSDB process on the device.
  b. Upgrade the software for the device. In the new software version, OVSDB entries change.
  c. In the new software version, start the OVSDB process.

201610190100

- Symptom: The QoS entry name is incorrect, and the QoS entry fails to be deployed.
- Condition: This symptom occurs if OVSDB is configured on the device and the OVSDB controller is used to deploy a QoS entry to the device.

201609200237

- Symptom: Configuring a VSAN to allow any WWN to log in through the specified interfaces fails.
- Condition: This symptom occurs if the following operations are performed:
  a. In a VSAN, configure the **any-wwn interface** *interface-list* command to allow any WWN to log in through the specified interfaces.
  b. In the same VSAN, configure the **any-wwn interface** *interface-list* command again.

201611170145

- Symptom: The OVSDB process fails to be started.
- Condition: This symptom occurs if the OVSDB process is restarted when the vtep.db file is corrupt.

201611080340

- Symptom：CVE-2016-5195
- Condition：An unprivileged local user could use this flaw to gain write access to otherwise read-only memory mappings and thus increase their privileges on the system.

201611070389

- Symptom：CVE-2016-8858
- Condition：A remote user can send specially crafted data during the key exchange process to trigger a flaw in kex_input_kexinit() and consume excessive memory on the target system. This can be exploited to consume up to 384 MB per connection.

201610290084

- Symptom: The log buffer cannot record log messages after the system time is set back.
- Condition: This symptom might occur if the system time is set back.

201610220217

- Symptom：CVE-2016-6304:
- Condition: Multiple memory leaks in t1_lib.c in OpenSSL before 1.0.1u, 1.0.2 before 1.0.2i, and 1.1.0 before 1.1.0a allow remote attackers to cause a denial of service (memory consumption) via large OCSP Status Request extensions.
- Symptom：CVE-2016-6306
- Condition: The certificate parser in OpenSSL before 1.0.1u and 1.0.2 before 1.0.2i might allow remote attackers to cause a denial of service (out-of-bounds read) via crafted certificate operations, related to s3_clnt.c and s3_srvr.c.

201608290406

- 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

201609080061/201609080062

- Symptom: The BFD MAD status of an IRF fabric is **Faulty**.
- Condition: This symptom occurs if the following conditions exist:
  - Two IRF fabrics configured with BFD MAD are connected with each other.
  - One IRF fabric receives BFD MAD detection packets from the other IRF fabric.

201608310495

- Symptom: The error message "Scanning is interrupted" occurs during ARP scanning.
- Condition: This symptom occurs if the following tasks are performed:
  a. Assign secondary addresses to a Layer 3 interface when no primary address is assigned to the interface.
  b. Enable ARP scanning on the Layer 3 interface to scan secondary IP addresses.

201608290242

- Symptom: The unknown unicast storm control configuration does not take effect.

- Condition: This symptom occurs if unknown unicast storm control is enabled and the upper and lower thresholds are set on an interface by using the **storm-constrain unicast kbps** *max-pps-values min-pps-values* command.

201608160221

- Symptom: Traffic cannot be forwarded.
- Condition: This symptom occurs if the following tasks are performed:
  - **a.** Use the **mirror-to interface** *interface-type interface-number* ***loopback*** *command to* configure an interface as a flow mirroring destination interface with the loopback feature.
  - **b.** Cancel the configuration.

201608040531

- Symptom: PBR-based forwarding fails on the VLAN interface of a super VLAN. Packets are forwarded through the previous forwarding route rather than the route specified by the PBR policy even though the next hop in the PBR policy is reachable.
- Condition: This symptom occurs if PBR is configured on the VLAN interface of the super VLAN.

201608100354/201607260156

- Symptom: The CLI hangs.
- Condition: This symptom occurs if a script including the **display clock** command is repeatedly executed.

201608080408

- Symptom: The **display system internal startup cache** command displays **None** after an IRF master/subordinate switchover, which indicates the .mdb binary configuration file on the device is lost.
- Condition: This symptom occurs if the following tasks are performed:
  - **a.** Save the running configuration and reboot the IRF fabric. A master/subordinate switchover occurs.
  - **b.** Display the file path of the .mdb binary configuration file used at the current startup by using the **display system internal startup cache** command.

201608050487

- Symptom: A checksum error occurs in an Efp_meter_table entry and the entry fails to be restored.
- Condition: This symptom occurs if a parity error exists in the Efp_meter_table entry.

201607190405

- Symptom: The number of multicast packets received by a multicast client is greater than or less than the expected number.
- Condition: This symptom occurs if the following tasks are performed:
  - **a.** An IRF fabric is connected a PE device.
  - **b.** The upstream interface and the RPF neighbor of the multicast tunnel interface are not the same.
  - **c.** A master/subordinate switchover occurs or multicast forwarding entries are cleared.

201607150396

- Symptom: The device reboots unexpectedly.
- Condition: This symptom occurs if the following tasks are performed:
  - **a.** Create multiple traffic classes by using the **traffic classifier** *classifier-name* [**operator** { **and** | **or** }] command.

b. Create multiple traffic behaviors by using the **traffic behavior** *behavior-name* command.
c. Create a QoS policy by using the **qos policy** *policy-name* command.
d. Associate traffic behaviors with the traffic classes in the QoS policy.
e. Apply the QoS policy to incoming and outgoing traffic of a VLAN by using the **qos vlan-policy** *policy-name* **vlan** *vlan-id-list* { **inbound | outbound** } command.
f. Remove the QoS policy applied to the incoming and outgoing traffic of the VLAN by using the **undo qos vlan-policy** *policy-name* **vlan** *vlan-id-list* { **inbound | outbound** } command.
g. Repeat tasks **e** to **f**.

201607110396

- Symptom: Some configuration of the device is lost after the device starts up.
- Condition: This symptom occurs if the following tasks are performed:
  a. Download a configuration file to the device through the HTTP server.
  b. Specify the configuration file as the next-startup configuration file.
  c. Save the running configuration and reboot the device.

201606280648

- Symptom: The description configured for an interface does not take effect.
- Condition: This symptom occurs if the description includes unsupported characters.

201608300525

- Symptom: The later-applied ACL on an interface cannot be used to filter outgoing packets.
- Condition: This symptom occurs if the following conditions exist:
  a. An interface is applied with an IPv4 advanced ACL and an IPv6 advanced ACL to filter outgoing packets.
  b. The number of rules in the IPv4 advanced ACL is in the range of 256 to 512.
  c. The IPv6 advanced ACL includes the following rules:
     - **rule** *rule-id* **permit icmpv6**.
     - **rule** *rule-id* **permit ipv6 source** *source-address.*
     - **rule** *rule-id* **permit tcp destination** *destination-address* **destination-port eq** *xx.*

201606060209

- Symptom: In an IRF fabric, traffic cannot be correctly forwarded after a patch is installed.
- Condition: This symptom occurs if the following conditions exist:
  a. The device has a hot patch installed to fix STP problems.
  b. The spanning tree protocol operates in PVST mode on the device.
  c. VLANs have been irregularly added and deleted on the device.

201607290021

- Symptom: CVE-2016-2177
- Condition: Fixed vulnerability in s3_srvr.c, ssl_sess.c, and t1_lib.c functions in OpenSSL through 1.0.2h that allows remote attackers to cause a denial of service (integer overflow and application crash), or possibly have an unspecified other impact by leveraging unexpected malloc behavior.

201607290007

- Symptom: CVE-2012-0036

- Condition: Fixed vulnerability in curl and libcurl 7.2x before 7.24.0 that allows remote attackers to conduct data-injection attacks via a crafted URL, as demonstrated by a CRLF injection attack on the (1) IMAP, (2) POP3, or (3) SMTP protocol.

201512280205

- Symptom: CVE-2015-3194
- Condition: Fixed vulnerability which can be exploited in a DoS attack, if device is presented with a specific ASN.1 signature using the RSA.
- Symptom: CVE-2015-3195
- Condition: Fixed vulnerability with malformed OpenSSL X509_ATTRIBUTE structure used by the PKCS#7 and CMS routines which may cause memory leak.
- Symptom: CVE-2015-3196
- Condition: Fixed vulnerability where a race condition can occur when specific PSK identity hints are received.
- Symptom: CVE-2015-1794
- Condition: Fixed vulnerability if a client receives a ServerKeyExchange for an anonymous Diffie-Hellman (DH) ciphersuite which can cause possible Denial of Service (DoS) attack.

201606160058

- Symptom: After an IRF fabric splits, the network ports on the Recovery-state IRF fabric stay in the down state for a long period of time.
- Condition: This symptom might occur if a MAD-enabled IRF fabric splits.

201606170104

- Symptom: After a QoS policy for flow mirroring is removed, new QoS policies cannot be applied to implement flow mirroring.
- Condition: This symptom might occur if the following conditions exist:
  - The number of mirroring destination ports of a mirroring group or a flow mirroring QoS policy exceeds the limit.
  - Application of a QoS policy for flow mirroring fails, and the QoS policy is removed.

201606160056

- Symptom: When multicast VPN or GRE tunneling is configured on an IRF fabric, outgoing traffic has an additional tag of VLAN 0.
- Condition: This symptom might occur if the following conditions exist:
  - Multicast VPN or GRE tunneling is configured on an IRF fabric.
  - The outgoing interface of the traffic is not on the same card as the ports in the service loopback group used for multicast VPN or GRE tunneling.

201606070629

- Symptom: PVST instances flap constantly when the network topology changes.
- Condition: This symptom might occur if the following conditions exist:
  - The number of PVST instances reaches 1 K.
  - sFlow is configured on the switch.
  - The network topology changes.

201605240067

- Symptom: The same MAC address is configured for two Layer 3 interfaces. When the MAC address of one interface is deleted, the other interface cannot forward traffic.
- Condition: This symptom might occur if the following operations are performed:

a. Configure the same MAC address for two Layer 3 interfaces.
b. Delete the MAC address of one Layer 3 interface.

201606120228

- Symptom: OSPF cannot establish a neighbor relationship through a sham link.
- Condition: This symptom might occur if the following operations are performed:
  a. Configure MD5 authentication multiple times for a sham link.
  b. Save the configuration and reboot the switch.

201606210535

- Symptom: A user-defined ACL cannot match packets with tunnel encapsulation by the inner IP header.
- Condition: This symptom might occur if a user-defined ACL is configured to match packets with tunnel encapsulation by the inner IP header.

201606230190

- Symptom: On an IRF fabric, the **display mac-address** command does not display the MAC addresses learned on an aggregate interface.
- Condition: This symptom might occur if the following conditions exist:
  - A multichassis aggregate interface is configured.
  - Traffic of the aggregate interface is forwarded by only one IRF member.

201606280429

- Symptom: When IPv4 IS-IS MTR and IPv6 IS-IS MTR are enabled, the switch cannot obtain routes from a Cisco NX9000 device.
- Condition: This symptom might occur if IPv4 IS-IS MTR and IPv6 IS-IS MTR are enabled, and the peer is a Cisco NX9000 device.

201606300317

- Symptom: When a Telnet user uses an overlength username, the switch might reboot for memory exhaustion.
- Condition: This symptom might occur if a Telnet user uses an overlength username.

201607040218

- Symptom: After certain operations, a directly connected device cannot ping the switch, and the switch cannot forward Layer 3 traffic.
- Condition: This symptom might occur if the following operations are performed:
  a. Create a VLAN interface and assign it an IP address.
  b. Associate the VLAN of the VLAN interface with a primary VLAN.
  c. Remove the association between the VLAN and the primary VLAN.

201607080232

- Symptom: When a management VLAN is configured for an aggregation group, the management VLAN cannot be pinged.
- Condition: This symptom might occur if the following operations are performed:
  a. Configure a management VLAN for an aggregation group.
  b. Remove ports from the aggregation group.

201607190025

- Symptom: When a large number of multicast entries are generated, available memory reaches the lower limit.

- Condition: This symptom might occur if a large number of multicast entries are generated.

201607010074

- Symptom: After an IRF master/subordinate switchover, multicast traffic forwarding is interrupted in one direction for a short period of time.
- Condition: This symptom might occur if the following operations are performed:
  - **a.** Configure multicast VPN for an IRF fabric, and enable the PIM-SSM mode for the public network.
  - **b.** Enable PIM NSR.
  - **c.** Configure the **default-group** command in MD view for a VPN instance.

201607010084

- Symptom: When certain conditions exist, some or all VPN instances on an IRF fabric cannot forward traffic.
- Condition: This symptom might occur if the following conditions exist:
  - Multicast VPN and PIM NSR are enabled for an IRF fabric.
  - The **data-group** command is configured in MD view for VPN instances.
  - Links for forwarding traffic are down during an IRF master/subordinate switchover.

201606210158

- Symptom: The unicast traffic statistics displayed by the **display interface** command are incorrect when a 40-GE interface receives unicast traffic at wire speed.
- Condition: This symptom might occur if a 40-GE interface receives unicast traffic at wire speed.

201605130329

- Symptom: When CCM sending is disabled on the local interface, the remote directly-connected interface is not shut down by CFD. The CFD continuity check function does not take effect.
- Condition: This symptom occurs if the following operations are performed:
  - **a.** Configure CFD on the directly-connected switches.
  - **b.** On the directly-connected interfaces, configure outward-facing MEPs without VLANs and enable CFD continuity check.
  - **c.** Execute the **undo cfd cc service-instance** *instance-id* **mep** *mep-id* **enable** command on the local interface.

201604280163

- Symptom: The dropped packet statistics cannot be cleared by using the **reset packet-drop interface** command for an interface.
- Condition: This symptom occurs if the interface drops packets because the data buffer is insufficient.

201604260478

- Symptom: When radar detection flow entries are issued to the switch, the display of interface-up and interface-down logs is delayed.
- Condition: This symptom occurs if radar detection flow entries are issued to the switch and interfaces on the switch are shut down or brought up.

201604250066/201308080141

- Symptom: In an IRF fabric configured with OpenFlow, delay occurs when you display flow table information for an OpenFlow instance.
- Condition: This symptom occurs if a large number of VLANs are associated with the OpenFlow instance.

201604220354

- Symptom: In an IRF fabric with multidevice link aggregation, OSPF log information cannot be displayed and OSPF configuration cannot be deleted.
- Condition: This symptom occurs if the following conditions exist:
    - Routing entries change frequently.
    - OSPF neighbors change frequently.
    - The **reset ospf process** command is executed repeatedly.

201604190259

- Symptom: The device enabled with CDP compatibility cannot recognize CDP packets and discards unrecognized CDP packets.
- Condition: This symptom occurs after the **lldp compliance admin-status cdp txrx** command is executed.

201604190234

- Symptom: In an IRF fabric with multidevice link aggregation, protocol flapping occurs on all link aggregation groups.
- Condition: This symptom occurs after the following operations are performed on an aggregation group:
    a. Configure the aggregate interface as a trunk port and assign it to all VLANs by using the **port trunk permit vlan all** command.
    b. Configure the aggregation group to operate in dynamic aggregation mode by using the **link-aggregation mode dynamic** command.
    c. Configure the aggregation group to operate in static aggregation mode by using the **undo link-aggregation mode** command**.**
    d. Configure the aggregation group to operate in dynamic aggregation mode by using the **link-aggregation mode dynamic** command.

201604150307/201510190119

- Symptom: A BGP peer of the device reboots exceptionally.
- Condition: This symptom occurs after the device is disabled to exchange labeled routes with the BGP peer by using the **undo peer label-route-capability** command.

201604140273

- Symptom: When an ENode receives RSCNs, it cannot timely obtain information about other ENodes in the same zone from the name server. As a result, ENodes in the same zone cannot access each other.
- Condition: This symptom occurs if the following conditions exists:
    - A large number of ENodes exist on the network.
    - A zone set is activated and distributed to the entire fabric by using the **zoneset activate** command.

201604120244

- Symptom: The switch cannot learn routes from two OSPF LSAs.
- Condition: This symptom might occur if two OSPF LSAs from a neighbor contain different information for the same transnet link.

201603220013

- Symptom: The device configured with OpenFlow cannot send packets out of the specified output port and cannot assign packets to the specified queue.

- Condition: This symptom occurs if an output port and a queue ID are specified in a flow entry issued by the controller.

201603170204

- Symptom: The device operating in the expert mode reboots exceptionally.
- Condition: This symptom occurs after the **undo flex10 enable** command is executed in Ethernet interface view.

201603120042

- Symptom: CLI does not respond to input commands after a client fails both 802.1X authentication and MAC authentication.
- Condition: This symptom occurs if the following conditions exist:
  - The device connects to a Cisco telephone through a port.
  - Both 802.1X authentication and MAC authentication are enabled on the port.
  - The device is configured to disable the port permanently upon detecting an illegal frame received on the port.

201603110240

- Symptom: On an MPLS L3 VPN network, the route between two PE devices which are interconnected through a P device is not reachable.
- Condition: This symptom occurs if a PE device connects to the P device through a Layer 3 Ethernet interface.

201602040439

- Symptom: The device fails to restart up by using the .cfg configuration file.
- Condition: This symptom occurs if spaces are included in the name of the NTP or SNTP server.

201511100575

- Symptom: A DHCPv6 client fails to obtain a static IPv6 address from the DHCPv6 server.
- Condition: This symptom occurs if no subnet is specified in the DHCPv6 address pool on the DHCPv6 server.

201508300025

- Symptom: STP status of a port is not correct.
- Condition: This symptom occurs after the following operations are performed:
  - **a.** Create an aggregation group.
  - **b.** Enable or disable STP globally on the local device.
  - **c.** Bring up or shut down an aggregation member port in the aggregation group on the peer device.

201604161225/201604161188

- Symptom: CVE-2016-0705
- Condition: Fixed vulnerability when OpenSSL parses malformed DSA private keys and could lead to a DoS attack or memory corruption for applications that receive DSA private keys from untrusted sources.
- Symptom: CVE-2016-0798
- Condition: Fixed vulnerability in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allows remote attackers to cause a denial of service (memory consumption) by providing an invalid username in a connection attempt.
- Symptom: CVE-2016-0797

- Condition: Fixed vulnerability in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allow remote attackers to cause a denial of service (heap memory corruption or NULL pointer dereference).
- Symptom: CVE-2016-0799
- Condition: Fixed vulnerability in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g improperly calculates string lengths, which allows remote attackers to cause a denial of service which could lead to memory allocation failure or memory leaks.
- Symptom: CVE-2016-0702
- Condition: Fixed vulnerability in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g which makes it easier for local users to discover RSA keys leveraging cache-bank conflicts, aka a "CacheBleed" attack.
- Symptom: CVE-2016-2842
- Condition: Fixed vulnerability in the doapr_outch function in crypto/bio/b_print.c, which allows remote attackers to cause a denial of service (out-of-bounds write or memory consumption) or possibly have unspecified other impact via a long string.

201605260046

- Symptom: The effective storm suppression threshold is 0 when the **broadcast-suppression/unicast-suppression/multicast-suppression pps** *1* command is executed in interface view.
- Condition: This symptom occurs if the **broadcast-suppression/unicast-suppression/multicast-suppression pps** *1* command is executed in interface view.

Resolved problems in F2428

201603230243/201605210012/201605030457

- Symptom: The switch reboots unexpectedly when an 802.1X user or DHCP client comes online after migration.
- Condition: This symptom might occur if an 802.1X user or DHCP client comes online after migration.

201602150629

- Symptom: In an IRF fabric, the BGP process exits abnormally after BGP NSR is configured.
- Condition: This symptom occurs if the following operations are performed:
  a. Start a BGP instance.
  b. Configure the **address-family ipv4 mdt** command.
  c. Configure the **non-stop-routing** command.

201511190281

- Symptom: The switch fails to establish a connection with the controller.
- Condition: This symptom occurs if the following operations are performed:
  a. Execute the **in-band management vlan** command in OpenFlow instance view to configure an inband management VLAN.
  b. Use the **network** command in OSPF area view to enable OSPF on the inband management VLAN interface.

201603280001

- Symptom: Two identical static routes in a device.
- Condition:

a. The preference of the DHCP automatically assigns a static route, which is the same as a user-defined static route.
b. Execute the display configuration command in the user view.

201604010506

- Symptom: IGMP packets are reported to the controller.
- Condition: This symptom occurs if the controller does not issue flow entries for IGMP packets.

201509020274

- Symptom: An aggregation group member port in Selected state might be blocked by STP.
- Condition: This symptom occurs if the following conditions exist:
  - LLDP, STP, and Ethernet link aggregation are configured in the network.
  - Loops exist in the network.

201512190244

- Symptom: The switch constantly outputs OpenFlow debugging information and delays outputting syslog messages.
- Condition: This symptom might occur if the OpenFlow-enabled switch receives a flood of packets that are to be transmitted in packet-in messages.

201603090358

- Symptom: The output from the **display process cpu | include lldp** command shows that the CPU usage of the LLDP process is high.
- Condition: This symptom might occur if the **lldp enable** command is executed.

201603140466

- Symptom: After MAC address move notifications are enabled, the switch does not generate notifications for MAC address move events.
- Condition: This symptom might occur if the **mac-address notification mac-move** command is executed, and MAC address move events occur.

201601210412

- Symptom: An IRF physical interface that uses a high power consumption transceiver module goes down unexpectedly after a switch reboot.
- Condition: This symptom might occur if the following conditions exist:
  - An IRF physical interface is installed with a high power consumption transceiver module.
  - The running configuration is saved, and the switch is rebooted.

201601080493

- Symptom: An OpenFlow instance cannot be activated if it is configured to perform QinQ tagging for double-tagged packets passing an extensibility flow table.
- Condition: This symptom might occur if an OpenFlow instance is configured to perform QinQ tagging for double-tagged packets passing an extensibility flow table.

201512280388

- Symptom: An online user on an interface receives an EAPOL-Start message and performs reauthentication.
- Condition: This symptom might occur if the following conditions exist:
  a. The 802.1X authentication feature and the keep-online feature for 802.1X users are enabled on an interface.
  b. The authentication server is unreachable.

201512180152/201512170260

- Symptom: After an IRF master/subordinate switchover, the management interface on the new master cannot obtain an IP address.
- Condition: This symptom might occur if the following conditions exist:
  - **a.** The **ip address dhcp-alloc** command is configured on the management interfaces of subordinate switches.
  - **b.** The master's management interface is down, and a master/subordinate switchover occurs.

201512180133

- Symptom: When two physical interfaces of the switch are connected, one interface is up and the other is down.
- Condition: This symptom might occur if the **link-delay delay-time** command is executed on one interface, and the speed of the other interface is modified.

201512150355

- Symptom: When the master switch of an IRF fabric is rebooted before a starting subordinate switch displays the "Cryptographic algorithms tests passed" message, the subordinate switch displays the "The board isn't ready for active and stand" message.
- Condition: This symptom might occur if the master switch of an IRF fabric is rebooted before a starting subordinate switch displays the "Cryptographic algorithms tests passed" message.

201603230128

- Symptom: The switch forwards received ARP packets out of the incoming interface and cannot ping remote devices.
- Condition: This symptom might occur if the controller issues a flow entry that contains a group entry, and the group entry contains an action with the output interface as the incoming interface of the ARP packets.

201603150263

- Symptom: On an IRF fabric, an Ethernet service instance still can match traffic after its frame match criterion is deleted.
- Condition: This symptom might occur if the following operations are performed:
  - **a.** Configure a site-facing Layer 2 aggregate interface.
  - **b.** Create an Ethernet service instance on the Layer 2 aggregate interface, and execute the **encapsulation s-vid** *vlan-id-list* command to configure a frame match criterion.
  - **c.** Execute the **undo encapsulation** command to delete the frame match criterion.

201602290172

- Symptom: An OpenFlow meter statistic collection action does not take effect.
- Condition: This symptom might occur if the controller issues an ACL flow entry with a meter statistic collection action.

201603170138

- Symptom: CVE-2016-0701
- Condition: Fixed vulnerability in the DH_check_pub_key function which makes it easier for remote attackers to discover a private DH (Diffie-Hellman) exponent by making multiple handshakes with a peer that chose an inappropriate number. This issue affects OpenSSL version 1.0.2. and addressed in 1.0.2f. OpenSSL 1.0.1 is not affected by this CVE.
- Symptom: CVE-2015-3197
- Condition: Fixed vulnerability when using SSLv2 which can be exploited in a man-in-the-middle attack, if device has disabled ciphers.

201505270316/201603300098

- Symptom: The switch cannot forward VPLS traffic if the interface that hosts an Ethernet service instance is not assigned to the VLANs that match the Ethernet service instance.
- Condition: This symptom might occur if the following conditions exist:
    - An Ethernet service instance is mapped to a VPLS VSI.
    - The interface that hosts the Ethernet service instance is not assigned to the VLANs that match the Ethernet service instance.

201509240266

- Symptom: When the MTU is set for a Layer 3 interface, the MTU setting is not synchronized to the OSPF and IS-IS modules. As a result:
    - After the **ospf mtu-enable** command is configured on the local interface and the peer interface, the two interfaces can establish OSPF neighborship in full state though the two ends have different MTU values.
    - IS-IS cannot establish neighborship.
- Condition: This symptom occurs if the MTU is set for a Layer 3 interface.

201604140100/201604070440

- Symptom: A user fails to come online.
- Condition: This symptom occurs if the RADIUS packets that the RADIUS server sends to the switch contain RADIUS attributes that the switch cannot recognize.

201604110116

- Symptom: When IPSG bindings are deleted from a Layer 3 subinterface or the VLAN interface with the same ID, underlying ACL configuration cannot be deleted completely.
- Condition: This symptom might occur if the following operations are performed:
    - Configure the **ip verify source** and **ip source binding** commands on a Layer 3 subinterface and the VLAN interface with the same ID.
    - Delete IPSG bindings from the Layer 3 subinterface or VLAN interface by performing one of the following operations:
        - Delete the Layer 3 subinterface.
        - Restore the default settings of the Layer 3 subinterface or VLAN interface.

201603100299/201512310465

- Symptom: The crosslink interfaces (not IRF physical interfaces) of HPE 6125XLG IRF member switches are not shut down as expected.
- Condition: This symptom might occur if one of the following operations is performed:
    - Modify an IRF member ID, reboot the member switch, and view the status of crosslink interfaces on the switch.
    - Set up an IRF fabric and view the status of crosslink interfaces on subordinate switches.

201603090041

- Symptom: Two aggregate interfaces are configured as PBB ACs to match customer traffic. Aggregate interface 1 uses the **encapsulation default** match criterion, and aggregate interface 2 uses the **encapsulation s-vid** match criterion. Aggregate interface 1 cannot forward traffic correctly if traffic is not received on its first member port. When aggregate interface 1 is deleted, aggregate interface 2 cannot forward traffic correctly.
- Condition: This symptom might occur if the following conditions exist:
    - Aggregate interface 1 and aggregate interface 2 are configured as PBB ACs to match customer traffic. The aggregate interfaces each have multiple member ports.

- Aggregate interface 1 uses the **encapsulation default** match criterion, and aggregate interface 2 uses the **encapsulation s-vid** match criterion.

201602180059

- Symptom: If the **ip ttl-expires enable** command is executed and the switch receives packets with a TTL of 0, the switch can neither forward traffic nor send ICMP error messages.
- Condition: This symptom might occur if the **ip ttl-expires enable** command is executed and the switch receives packets with a TTL of 0.

201602150276

- Symptom: After the switch is rebooted or the **display this** command is executed in queue scheduling profile view, the switch cannot display the configuration of a user-defined queue scheduling profile.
- Condition: This symptom might occur if the following operations are performed:
  - **a.** Use the **qos qmprofile** command to create a queue scheduling profile and enter its view.
  - **b.** Execute the **queue** *queue-id* **sp group** 1 **weight** *schedule-value* command.
  - **c.** Execute the **queue** *queue-id* **wfq group** 1 **byte-count** *schedule-value* command.

201602040154

- Symptom: The switch cannot ping a peer when the length of ping packets exceeds the MTU of the outgoing interface.
- Condition: This symptom might occur if the length of ping packets exceeds the MTU of the outgoing interface.

201601300194

- Symptom: The system reports mirroring resource insufficiency when mirroring group commands are executed multiple times.
- Condition: This symptom might occur if the following commands are executed in sequence multiple times.
  - **a.** **mirroring-group** *group-id* **mirroring-port** *interface-list* **inbound**.
  - **b.** **mirroring-group** *group-id* **monitor-port tunnel**.
  - **c.** **undo mirroring-group all**.

201601260421

- Symptom: When devices are connected through an aggregate link, packet loss occurs for about 1 second.
- Condition: This symptom occurs if the following operations are performed:
  - **a.** Enable BFD for the aggregate interface by using the **link-aggregation bfd ipv4** command.
  - **b.** Unplug the Rx optical fiber from the transceiver module of an aggregation group member interface on the peer device. The state of the member interface changes from inactive to active and then to inactive. As a result, packet loss occurs for a long period of time.

201601280089

- Symptom: An IRF fabric splits when a large number of entry parity errors occur.
- Condition: This symptom might occur if a large number of entry parity errors occur.

201603050089

- Symptom: On an IRF fabric, the routing process exits abnormally when certain conditions exist.
- Condition: This symptom might occur if the following conditions exist:

a. An IRF fabric has BGP peer relationships with other devices.
b. The **flush route-attribute bgp** command is executed in RIB IPv4 address family view.
c. A master/subordinate switchover occurs.

201602040580

- Symptom: Constant state flapping occurs on an DLDP-enabled interface that is connected to a Comware 3 device.
- Condition: This symptom might occur if DLDP is enabled on an interface that is connected to Comware 3 device.

201603030332

- Symptom: A user-defined queue scheduling profile uses byte-count WRR for a queue. After a reboot, weight-based WRR is used for the queue.
- Condition: This symptom might occur if the following operations are performed:
  a. Create a queue scheduling profile, and configure byte-count WRR for a queue.
  b. Delete the .mdb configuration file.
  c. Save the running configuration and reboot the switch.

201601300181

- Symptom: On an MSTP root bridge, an aggregate interface is in discarding state when the interface acts as a designated port.
- Condition: This symptom might occur if an aggregate interface is configured as a designated port on an MSTP root bridge.

201601280420

- Symptom: When a VLAN is deleted, the static MAC address entries of the VLAN are not deleted.
- Condition: This symptom might occur if static MAC address entries are created for a VLAN and the VLAN is deleted.

201603070215

- Symptom: The **lldp neighbor-protection aging block** command is executed on a Selected aggregation member port for the switch to block the port when the LLDP neighbor on the port ages out. The output from the **display link-aggregation verbose** command shows that the port is still in Selected state after its LLDP neighbor ages out.
- Condition: This symptom might occur if the following conditions exist:
  - The **lldp neighbor-protection aging block** command is executed on an aggregation member port.
  - The **display link-aggregation verbose** command is executed after the LLDP neighbor on the port ages out.

201511300051

- Symptom: An interface is configured to be blocked after the LLDP neighbor on the interface ages out. When the LLDP neighbor re-establishes a neighbor relationship with the interface, the interface cannot be restored to the forwarding state.
- Condition: This symptom might occur if an aged out LLDP neighbor re-establishes a neighbor relationship with an interface.

201512280232

- Symptom: An interface cannot generate a new MAC address entry for an IP phone after the old MAC address entry ages out.
- Condition: This symptom might occur if the following conditions exist:

- The IP phone is in the critical voice VLAN.
- The VLAN ID in the packets sent by the IP phone is different from the VLAN ID of the host connected to the IP phone.

201512310410

- Symptom: The switch has two configuration files **a.cfg** and **b.cfg**. The historical configuration file **a.cfg** contains monitor link group configuration and the **uplink up-port-threshold** command. The running configuration file **b.cfg** does not contain monitor link configuration. After the **configuration replace file** command is executed to replace the running configuration with the configuration in **a.cfg**, the **uplink up-port-threshold** setting is missing.
- Condition: This symptom might occur if the following conditions exist:
  - The historical configuration file **a.cfg** contains monitor link group configuration and the **uplink up-port-threshold** command. The running configuration file **b.cfg** does not contain monitor link configuration.
  - The **configuration replace file** command is executed to replace the running configuration with the configuration in **a.cfg**.

201512190270

- Symptom: The master switch of an IRF fabric does not display any prompts when a newly added subordinate switch fails to reboot with the software image downloaded from the master switch for flash memory shortage.
- Condition: This symptom might occur if a newly added subordinate switch fails to reboot with the software image downloaded from the master switch for flash memory shortage.

201602040025

- Symptom: The LLDP process exits abnormally if the **lldp notification med-topology-change enable** command is executed and the switch establishes an LLDP neighbor relationship with an IP phone.
- Condition: This symptom might occur if the **lldp notification med-topology-change enable** command is executed and the switch establishes an LLDP neighbor relationship with an IP phone.

201602260104

- Symptom: If two ACL rules are configured for an IPv6 ACL applied to a Layer 3 interface, the system reports ACL resource insufficiency and the second ACL rule does not take effect.
- Condition: This symptom might occur if the following operations are performed in the view of an IPv6 ACL:
  - **a.** Use the **rule** command to create a rule to match source IPv6 addresses with a prefix length of 128 bits.
  - **b.** Use the **rule** command to create another rule to match source IPv6 addresses with a prefix length of 64 bits.

201602040542

- Symptom: MAC address learning and protocol packet processing slow down on an interface that has 1024 secondary IP addresses when the interface receives a large number of ARP packets (for example, 2 K).
- Condition: This symptom might occur if 1024 secondary IP addresses are assigned to an interface, and a large number of ARP packets are sent to the interface.

201602160589

- Symptom: In an MPLS network, multiple PE devices are directly connected to a P device, and the **mpls label advertise explicit-null** command is executed on the PE devices. Some of the PE devices cannot ping one another.

- Condition: This symptom might occur if multiple PE devices are directly connected to a P device, and the **mpls label advertise explicit-null** command is executed on the PE devices.

201602040394

- Symptom: The switch does not detect an incoming label conflict when the **static-lsp egress** *lsp-name* **in-label** *in-label* command and the **static-cr-lsp egress** *lsp-name* **in-label** *in-label-value* command specify the same incoming label.
- Condition: This symptom might occur if the **static-lsp egress** *lsp-name* **in-label** *in-label* command and the **static-cr-lsp egress** *lsp-name* **in-label** *in-label-value* command specify the same incoming label.

201601160182/201601080571

- Symptom: The LDP-enabled switch reboots unexpectedly when it receives TCP packets that carry a length value of 0 in the header.
- Condition: This symptom might occur if the LDP-enabled switch receives TCP packets that carry a length value of 0 in the header.

201602190606

- Symptom: A Layer 2 Ethernet interface is assigned to VLAN 2 as an access port. After the link mode of the interface is set to Layer 3 and then switched back to Layer 2, the interface still can forward traffic of VLAN 2.
- Condition: This symptom might occur if the following operations are performed:
  - **a.** Execute the **port access vlan 2** command on a local Layer 2 Ethernet interface and its peer interface.
  - **b.** Execute the **port link-mode route** command on the local interface.
  - **c.** Execute the **port link-mode bridge** command on the local interface.

201601180120

- Symptom: After a master/subordinate switchover occurs on an IRF fabric that is configured with 1000 LDP VPN instances, the CLI stops responding for 3 minutes.
- Condition: This symptom might occur if 1000 LDP VPN instances are configured on an IRF fabric, and a master/subordinate switchover occurs.

201601130435

- Symptom: On an IRF fabric, the CPU usage is close to 100% on the member switch that hosts the active LDP process.
- Condition: This symptom might occur if the following conditions exist:
  - LDP NSR is enabled on an IRF fabric, and a master/subordinate switchover occurs after the LDP session is up.
  - The sent message count of the LDP session is incorrect.

Resolved problems in F2426

201601210131

- Symptom: The device fails to send messages in OpenFlow.
- Condition:
  - The device is configured with OpenFlow.
  - Execute the **stp enable** command.
  - Send messages to the controller.

201601080282

- Symptom: VPLS traffic cannot be processed between a Comware 7 device and a Comware 5 device.
- Condition: This symptom occurs if the Comware 7 device is connected to the Comware 5 device.

201601060247

- Symptom: An error message of "Configuration already exists" is displayed when a service loopback group is created and a port is assigned to the service loopback group by using NETCONF.
- Condition: This symptom occurs after a service loopback group is deleted.

201512250152

- Symptom: The device fails to roll back the configuration by using NETCONF.
- Condition: This symptom occurs if the following tasks have been performed:
  - **a.** Lock the device configuration by using NETCONF.
  - **b.** Deploy multiple configurations including incorrect configurations.

201512170149

- Symptom: Multicast packets are flooded to all ports in the VLANs to which the packets belong.
- Condition: This symptom occurs if the device operates in NLB multicast mode.

201512020082

- Symptom: The device fails to load the entropy file during startup.
- Condition: This symptom occurs if the device is configured with FIPS and enters FIPS mode through automatic reboot.

201512310465

- Symptom: Packet loss occurs in multi-chassis 6125XLG IRF fabrics.
- Condition: This symptom occurs if the following conditions exist:
  - Multiple C7000 enclosures exist.
  - In each enclosure, a 6125XLG device is installed in bay 1 and bay 2, separately.
  - All 6125XLG devices in bay 1 form an IRF fabric of ring topology. All 6125XLG devices in bay 2 form an IRF fabric of ring topology.

201601190167

- Symptom: TACACS authentication cannot be performed through the Web interface.
- Condition: This symptom occurs if authenticated is configured through the Web interface.

201403060134

- Symptom: The device fails to forward Layer 3 packets.
- Condition: This symptom occurs if the next hops of ECMP routes change.

201602020053

- Symptom: An ACL is applied to the NETCONF over SOAP over HTTP or HTTPs traffic. After the running configuration is saved and the switch is rebooted, the configuration does not take effect.
- Condition: This symptom might occur if the following operations are performed:
  - **a.** Apply an ACL to the NETCONF over SOAP over HTTP or HTTPs traffic.
  - **b.** Save the running configuration and reboot the switch.

201512010309

- Symptom: ARP suppression does not take effect.
- Condition: This symptom occurs if the following tasks have been performed:
  a. Create a multi-chassis aggregate interface.
  b. Execute the **encapsulation untagged** command on a service instance on the aggregate interface.
  c. Execute the **arp suppression enable** command on the VSI mapped to the aggregate interface.

201511110270

- Symptom: The packet statistic in the output from the **display interface** command is different from the value of the upSpeed field on the Portal page for the associated link.
- Condition: None.

201511130253

- Symptom: If non-existent scheduling rules are deleted by using ODL when NETCONF is deploying configuration to the switch, the system reports that XML has errors and configuration deployment fails.
- Condition: This symptom might occur if non-existent scheduling rules are deleted by using ODL when NETCONF is deploying configuration to the switch.

201511190354

- Symptom: After an IRF fabric splits, a terminal device cannot ping the directly connected IRF subordinate switch.
- Condition: This symptom might occur if an IRF fabric splits.

201509170208

- Symptom: MQC or packet filtering configuration fails if TRILL is enabled and then disabled.
- Condition: This symptom might occur if TRILL is enabled and then disabled.

201511180127

- Symptom: The switch reboots unexpectedly if the **l2protocol stp tunnel dot1q** command is executed on an aggregate interface that has a large number of Unselected member ports.
- Condition: This symptom might occur if the **l2protocol stp tunnel dot1q** command is executed on an aggregate interface that has a large number of Unselected member ports.

201511300121

- Symptom: NTP clock synchronization fails on the switch that acts as an NTP client if the precision of the NTP server is 2^{-32} second.
- Condition: This symptom might occur if the precision of the NTP server is 2^{-32} second.

201511200077

- Symptom: A Nuage VSC controller fails to issue IP addresses in the 0.136.x.x segment.
- Condition: This symptom might occur if a Nuage VSC controller issues IP addresses in the 0.136.x.x segment.

201511190081

- Symptom: The **undo loopback-detection global enable vlan all** command does not take effect if the running configuration is saved and then the switch is rebooted after this command is executed.
- Condition: This symptom might occur if the following operations are performed:
  a. Execute the **undo loopback-detection global enable vlan all** command.

b. Save the running configuration and reboot the switch.

201511110055

- Symptom: The output for the **boot-loader file filename all main** command does not include the prompt for the **ALL** option if an invalid value is entered for the "Please make a choice. [Y/N/A]:" message.
- Condition: This symptom might occur if the following operations are performed:
  a. Execute the **boot-loader file filename all main** command on an IRF fabric.
  b. Enter an invalid value when the **Please make a choice. [Y/N/A]:** message is displayed.

201508210207

- Symptom: When port security, 802.1X authentication, or MAC authentication is enabled, log messages are not generated in the following situations:
  - ACL resources are insufficient.
  - The 802.1X unicast trigger feature does not take effect.
  - SmartOn authentication fails.
  - 802.1X users fail authentication, pass authentication, or go offline.
  - MAC authentication users fail authentication, pass authentication, or go offline.
  - Port security fails to issue ACLs or user profiles to the driver.
  - Intrusion protection of port security is triggered.
  - Port security learns new secure MAC addresses.
- Condition: This symptom might occur if port security, 802.1X authentication, or MAC authentication is enabled.

201511260539

- Symptom: PBR configuration does not take effect if the next hop of packets is the local switch.
- Condition: This symptom might occur if PBR is configured and the next hop of packets is the local switch.

201511190389

- Symptom: The IUCT and ACLMGRD processes consume a large amount of CPU resource on an IRF member switch after the switch is rebooted.
- Condition: This symptom might occur if an IRF member switch is rebooted.

201506020183

- Symptom: More than 128 (the upper limit) IPv6 tunnels can be created. However, the excessive IPv6 tunnels cannot provide services.
- Condition: This symptom occurs if the number of IPv6 tunnels created exceeds the upper limit and the **display interface tunnel brief** command is executed to view whether the tunnel interfaces can go up.

201511040525

- Symptom: A phone attached to the switch cannot establish a connection with the voice server if the phone performs 802.1X authentication.
- Condition: This symptom might occur if the phone is capable of LLDP and 802.1X and performs 802.1X authentication.

201509160334

- Symptom: On an IRF fabric, the output from the **display lldp local-information** command is incorrect after a master/subordinate switchover.

- Condition: This symptom might occur if the **display lldp local-information** command is executed after a master/subordinate switchover.

201511270136

- Symptom: OSPF flapping occurs after an IRF fabric splits.
- Condition: This symptom might occur if BFD MAD is enabled for the IRF fabric, and the IRF split is caused by the shutdown of IRF physical interfaces.

201509250182

- Symptom: Two VPNs can communicate with each other. When a PC accesses a VPN through Telnet and SNMP separately, different ACLs are matched.
- Condition: This symptom might occur if a PC uses Telnet and SNMP to access a VPN separately.

201510210150

- Symptom: The switch sends RSCNs to nodes that do not have peer zone changes.
- Condition: This symptom might occur if the **smartsan enable fcoe** command is executed on the switch.

201511030428

- Symptom: The switch responds to NTP packets when NTP is disabled.
- Condition: This symptom occurs when NTP is disabled and SNTP is enabled.

201510300176

- Symptom: On a port, an Ethernet service instance is configured with the **encapsulation default** command, and another Ethernet service instance is configured with the **encapsulation s-vid** command. When packets with the specified outer 802.1Q VLAN ID arrive at the port, the packets match the Ethernet service instance configured with the **encapsulation default** command.
- Condition: This symptom occurs when PBB is used.

201511170528

- Symptom: Half of the broadcast traffic in the overlay management VLAN is lost if an IRF member switch is rebooted with configuration.
- Condition: This symptom might occur if the following operations have been performed:
    - **a.** Save the configuration.
    - **b.** Reboot the IRF member switch.

201512080300

- Symptom: Two storage devices cannot communicate with each other through an switch.
- Condition: This symptom might occur if two storage devices communicate through an switch.

201508040358

- Symptom: On an switch operating in FCF mode, the operating mode of a VSAN is displayed as FCF after the **fabric-name** command is executed in the view of the VSAN.
- Condition: This symptom might occur if the following operations have been performed:
    - **a.** Set the operating mode to FCF for the switch.
    - **b.** Execute the **fabric-name** command in the view of the VSAN.

201510300068/201510300207

- Symptom: The switch cannot establish an OVSDB connection with the VCF controller if the VCF controller is in a private network and OpenFlow is also enabled on the switch.

- Condition: This symptom might occur if the VCF controller is in a private network and OpenFlow is also enabled on the switch.

201509070220

- Symptom: A TCL script used to configure a VSAN to operate in FCF mode is terminated unexpectedly.
- Condition: This symptom occurs if the TCL script is executed on a switch operating in FCF-NPV mode.

201504280282

- Symptom: In an IRF fabric, a table-miss flow entry configured to count traffic in packets and in bytes at the same time fails to be deployed.
- Condition: This symptom occurs if the controller removes the flags parameter when deploying the flow entry.

201506110097

- Symptom: In an IRF fabric, when the switch is connected to a controller, the statistics collected by using the **send_stat_table** instruction are incorrect.
- Condition: This symptom occurs if the switch receives packets that match the flow entries and the packets that do not match the flow entries at the same time.

201506260236

- Symptom: After the controller deploys an OpenFlow flow entry for mirroring packets to a GRE tunnel interface, the matching packets cannot be forwarded out of the interface.
- Condition: This symptom occurs if OpenFlow is configured on the switch and the default
- table-miss flow entry, which drops packets, is used.

201508190171

- Symptom: A flow entry with the MAC address of a multiport MAC address entry fails to be deployed.
- Condition: This symptom occurs if the following conditions exist:
    - The global mode is enabled for the OpenFlow instance.
    - The **default table-miss permit** command is configured.
    - Multiport MAC address entries are configured.

201507290144

- Symptom: OSPF routes are incorrect. As a result, devices cannot communicate with each other.
- Condition: This symptom occurs if the following conditions exist:
    - A server running OSPF establishes OSPF neighborship with a Layer 3 virtual interface of the switch.
    - The switch receives Type-2 LSAs with the same network segment from the server and a neighbor switch.

Resolved problems in R2423

201509070220

- Symptom: A TCL script used to configure a VSAN to operate in FCF mode is terminated unexpectedly.
- Condition: This symptom occurs if the TCL script is executed on a switch operating in FCF-NPV mode.

201504280282

- Symptom: In an IRF fabric, a table-miss flow entry configured to count traffic in packets and in bytes at the same time fails to be deployed.
- Condition: This symptom occurs if the controller removes the flags parameter when deploying the flow entry.

201506110097

- Symptom: In an IRF fabric, when the switch is connected to a controller, the statistics collected by using the **send_stat_table** instruction are incorrect.
- Condition: This symptom occurs if the switch receives packets that match the flow entries and the packets that do not match the flow entries at the same time.

201506260236

- Symptom: After the controller deploys an OpenFlow flow entry for mirroring packets to a GRE tunnel interface, the matching packets cannot be forwarded out of the interface.
- Condition: This symptom occurs if OpenFlow is configured on the switch and the default
- table-miss flow entry, which drops packets, is used.

201508190171

- Symptom: A flow entry with the MAC address of a multiport MAC address entry fails to be deployed.
- Condition: This symptom occurs if the following conditions exist:
  - The global mode is enabled for the OpenFlow instance.
  - The **default table-miss permit** command is configured.
  - Multiport MAC address entries are configured.

Resolved problems in R2422P02

201508110063

- Symptom: IRF physical interfaces go down.
- Condition: This symptom occurs if the following conditions exist:
  - Two switches are connected through 40G_BASE_SR_BD_QSFP_PLUS or 40G_BASE_BD_WDM1310_QSFP_PLUS transceiver modules.
  - The interconnecting interfaces are used as IRF physical interfaces.
  - The subordinate IRF member switch automatically reboots and joins the IRF fabric.

201512070381

- Symptom: OpenFlow configuration fails for memory leaks if the OpenFlow instance contains flow entries with Experimenter match fields.
- Condition: This symptom might occur if the OpenFlow instance contains flow entries with Experimenter match fields.

201512091527/201605120175

- Symptom: The CLI does not respond.
- Condition: This symptom occurs if the following tasks are performed:
  a. Log in to the device through SSH.
  b. Enter the **tclsh** command.
  c. Enter any command.

201512210288

- Symptom: A switch fails to send sFlow packets when the management Ethernet interface acts as an sFlow agent and uses a DHCP-assigned IP address.
- Condition: This symptom might occur if the management Ethernet interface acts as an sFlow agent and uses a DHCP-assigned IP address.

201512250139

- Symptom: The system fails to write sFlow data statistics in a two-chassis IRF fabric.
- Condition: This symptom occurs if the following operations have been performed:
  a. Execute the **sflow collector** *collector-id* **vpn-instance** *vpn-instance-name* command in system view.
  b. Reboot the device or update the software.

201601120467

- Symptom: The system fails to obtain the value of MIB node entphysicalvendortype for a transceiver module.
- Condition: This symptom occurs if a 40G_BASE_SR_BD_QSFP_PLUS transceiver module is installed in the device.

201601180429

- Symptom: The software of an IRF fabric is upgraded from R2418P06 to R2422P01 through an ISSU. After the upgrade, interfaces cannot establish LLDP neighbor relationships.
- Condition: This symptom might occur if an ISSU is performed to upgrade the software from R2418P06 to R2422P01 for an IRF fabric.

201602180362

- Symptom: When multiple SSH clients simultaneously log in to the switch that acts as an SSH server and constantly create and delete files, the switch cannot respond to commands and reboots for memory exhaustion.
- Condition: This symptom might occur if multiple SSH clients simultaneously log in to the switch that acts as an SSH server and constantly create and delete files.

201604140036

- Symptom: When an SFP+ AOC module is removed and reinstalled on an IRF physical interface, the interface goes down unexpectedly.
- Condition: This symptom might occur if an SFP+ AOC module is removed and reinstalled on an IRF physical interface.

201605100323/201605120216

- Symptom: An IRF fabric is rebooted when endless loops are detected.
- Condition: This symptom occurs if parity errors occur to the l2_entries of the switch.

201606010234

- Symptom: The switch reboots exceptionally.
- Condition: This symptom occurs if the following operations are performed:
  a. Use the IMC server to monitor interface A of the switch.
  b. Apply a QoS policy to interface A.
  c. Use the **undo classifier** *classifier-name* command to delete all traffic classes of the QoS policy.

201606010533

- Symptom: The switch reboots unexpectedly when OpenFlow configuration is rolled back.

- Condition: This symptom might occur if OpenFlow configuration is rolled back.

201606200288

- Symptom: ARP requests are broadcasted on Layer 3 interfaces.
- Condition: This symptom might occur if a Layer 3 interface receives an ARP request with an all-0s source MAC address.

201510120304

- Symptom: After a user remotely logs in to the device, the console port does not respond.
- Condition: This symptom occurs if the following tasks are performed:
  - **a.** Configure RADIUS authentication on the device. The RADIUS server does not authorize any roles.
  - **b.** The device is not configured with the default user role assignment function.

201510220079

- Symptom: Packet loss occurs when a user pings an IRF fabric from a virtual machine.
- Condition: This symptom occurs if a user pings an IRF fabric from a virtual machine.

201608200139

- Symptom: The memory of the device slowly leaks.
- Condition: This symptom occurs if L2VPN is enabled by using the **l2vpn enable** command in system view.

201606030317

- Symptom: CVE-2016-2105
- Condition: Fixed vulnerability in “EVP Encode” in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of binary data.
- Symptom: CVE-2016-2106
- Condition: Fixed vulnerability in “EVP Encrypt” in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of binary data.
- Symptom: CVE-2016-2107
- Condition: Fixed vulnerability in OpenSSL before 1.0.1t and 1.02h allows remote attackers to obtain sensitive cleartext information via a padding-oracle attack against an AES CBC session.
- Symptom: CVE-2016-2108
- Condition: Fixed vulnerability in OpenSSL before 1.0.1o and 1.0.2 before 1.0.2c allows remote attackers to execute arbitrary code or cause a denial of service (buffer underflow and memory corruption).
- Symptom: CVE-2016-2109
- Condition: Fixed vulnerability in “asn” before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (memory consumption) via a short invalid encoding.
- Symptom: CVE-2016-2176
- Condition: Fixed vulnerability in “X509” in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to obtain sensitive information from memory or cause a denial of service

201511200516/20160427040

- Symptom: CVE-2015-7871
- Condition: Cause ntpd to accept time from unauthenticated peers.

* Symptom: CVE-2015-7704
* Condition: An ntpd client forged by a DDoS attacker located anywhere on the Internet, that can exploit NTP's to disable NTP at a victim client or it may also trigger a firewall block for packets from the target machine.
* Symptom: CVE-2015-7705
* Condition: The DDoS attacker can send a device a high volume of ntpd queries that are spoofed to look like they come from the client. The servers then start rate-limiting the client.
* Symptom: CVE-2015-7855
* Condition: Ntpd mode 6 or mode 7 packet containing an unusually long data value could possibly use cause NTP to crash, resulting in a denial of service.

201605090023/201605090022/TB201605040255

* Symptom: CVE-2015-8138
* Condition: Fixed vulnerability in ntpd which attackers may be able to disable time synchronization by sending a crafted NTP packet to the NTP client.
* Symptom: CVE-2015-7979
* Condition: Fixed vulnerability in ntpd allows attackers to send special crafted broadcast packets to broadcast clients, which may cause the affected NTP clients to become out of sync over a longer period of time.
* 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.
* 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.

201605160326

* Symptom: CVE-2016-1547
* Condition: Fixed vulnerability where an off-path attacker can deny service to ntpd clients by demobilizing preemptable associations using spoofed crypto-NAK packets.
* Symptom: CVE-2016-1548
* Condition: Fixed vulnerability where an attacker can change the time of an ntpd client or deny service to an ntpd client by forcing it to change from basic client/server mode to interleaved symmetric mode.
* 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.
* 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.
* Symptom: CVE-2016-2519
* Condition: Fixed vulnerability in ntpd will abort if an attempt is made to read an oversized value.
* Symptom: CVE-2015-7704
* Condition: Fixed vulnerability in ntpd that a remote attacker could use, to send a packet to an ntpd client that would increase the client's polling interval value, and effectively disable synchronization with the server.

201607040265

- Symptom: CVE-2016-4953
- Condition: Fixed vulnerability in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service by sending a spoofed packet with incorrect authentication data at a certain time.
- 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.
- Symptom: CVE-2016-4956
- Condition: Fixed vulnerability in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service via a spoofed broadcast packet.

Resolved problems in R2422P01

201510190093

- Symptom: After an FCF switch is rebooted, the peer zone type fails to be restored in a zone set.
- Condition: This symptom occurs if the following operations are performed:
    - **a.** Create a peer zone on the FCF switch according to the configuration on the storage device.
    - **b.** Save the configuration, and delete the .mdb configuration file.
    - **c.** Restore the configuration by using the .cfg configuration file.

201511280147

- Symptom: An 10GE interface on an switch cannot come up after an optical transceiver module is installed or removed for the interface.
- Condition: This symptom might occur if an optical transceiver module is installed or removed for an 10GE interface of an switch.

201511260190

- Symptom: MPLS cannot be enabled on VLAN interfaces if the total number of Layer 3 interfaces and subinterfaces exceeds 512 on the switch.
- Condition: This symptom might occur if the total number of Layer 3 interfaces and subinterfaces exceeds 512 on the switch.

201512070290

- Symptom: A server cannot recognize a storage device.
- Condition: This symptom occurs if the following conditions exist:
    - o An FCF switch is connected to the server, and a VSAN is created on the switch.
    - o When the software is upgrade, the BootROM version changes, and the configuration of the switch is restored by using the .cfg configuration file.

Resolved problems in R2422

201510280327

- Symptom: The system displays "Invalid version" if the **boot-loader file** *ipe-filename* **all main command is executed on an IRF fabric.**
- Condition: This symptom might occur if the **boot-loader file** *ipe-filename* **all main command is executed in user view.**

201506170119

- Symptom: FCoE packets are out of order.
- Condition: This symptom might occur if FIP snooping is enabled on Transit switches, and STP flapping occurs.

201508190332

- Symptom: The interfaces in the output from the **tracert trill –v** command are identified by their circuit IDs instead of physical port numbers.
- Condition: This symptom might occur if the **tracert trill –v** command is executed.

201509010033

- Symptom: The switch can receive Path messages from a Juniper device but cannot establish a CRLSP with the device.
- Condition: This symptom might occur if the switch works with a Juniper device.

201509020039

- Symptom: Users fail authentication if the switch uses an ACS5.6 server to perform TACACS authentication.
- Condition: This symptom might occur if the switch uses an ACS5.6 server to perform TACACS authentication.

201509240030

- Symptom: The member switches in an IRF fabric do not operate correctly if link aggregation has multiple management VLANs.
- Condition: This symptom might occur if multiple management VLANs are configured for link aggregation by using the **link-aggregation management-vlan** command.

201508280352

- Symptom: When the **display openflow flow-table** command is executed to display the extensibility flow table, the byte count for the table-miss flow entry is incorrect in the command output
- Condition: This symptom occurs if the following conditions exist:
  - The OpenFlow instance is configured to operate in global mode.
  - The OpenFlow instance receives Layer 2 traffic.

201510090358

- Symptom: The CLI does not respond when the **display ospf peer** command is executed.
- Condition: This symptom occurs if the **placement program default** command and then the **affinity location-type paired default** command are repeatedly executed.

201508180376

- Symptom: VTY login to a multichassis IRF fabric fails.
- Condition: This symptom might occur if master/subordinate switchovers occur frequently.

201508210176

- Symptom: The **display interface M-GigabitEthernet0/0/0** command does not display the IP address of the management Ethernet interface on an IRF member switch.
- Condition: This symptom might occur if the following operations have been performed:
  a. Use the **ip address irf-member** command to assign an IP address to the management Ethernet interface of an IRF member switch.
  b. Execute the **display interface M-GigabitEthernet0/0/0** command to view management Ethernet interface configuration.

201506260237

- Symptom: A Comware 5 switch and a Comware 7 switch cannot set up a TCP connection for BGP.
- Condition: This symptom might occur if the following conditions exist:
  - SYN Cookie is enabled on the Comware 7 switch.
  - BGP MD5 authentication is enabled on both switches.
  - The Comware 7 switch acts as a TCP server, and the Comware 5 switch acts as a TCP client to set up a TCP connection.

201508210119

- Symptom: The ACL for a Layer 3 aggregate subinterface is not deleted when the subinterface is deleted.
- Condition: This symptom might occur if the following operations have been performed:
  - **a.** Create a Layer 3 aggregate subinterface.
  - **b.** Use the **undo interface route-aggregation** command to delete the Layer 3 aggregate subinterface.
  - **c.** Execute the **debug qacl show acl-resc slot** *slot-number* **chip** *chip-number* command.

201508210119

- Symptom: The default ACL rules based on a Layer 3 interface still exist after the interface's link mode is set to bridge or the interface is deleted.
- Condition: This symptom might occur if the link mode of an Ethernet interface is switched from route to bridge, or a Layer 3 Ethernet subinterface, Layer 3 aggregate interface, or Layer 3 aggregate subinterface is deleted.

201509300450

- Symptom: In a VPLS network, packet loss occurs on an aggregation group member port.
- Condition: This symptom occurs if the following operations are performed:
  - **a.** Configure the link type of the aggregation group member port as access.
  - **b.** Remove the port from the aggregation group.
  - **c.** Create a service instance on the port, and execute the **encapsulation default** command for the service instance.
  - **d.** Remove the port from the service instance.
  - **e.** Assign the port to the aggregation group again.

201508120257

- Symptom: The **display qos policy control-plane management pre-defined** command displays nothing.
- Condition: This symptom might occur if the **display qos policy control-plane management pre-defined** command is executed in user view.

201508180448

- Symptom: Users cannot access the network through the switch enabled with ARP attack detection.
- Condition: This symptom might occur if the following conditions exist:
  - ARP attack detection is enabled, and trusted interfaces are excluded from ARP attack detection.
  - A trusted interface receives ARP packets sent at a rate higher than 100 pps.

201506020169

- Symptom: An interface on an IRF member switch does not forward voice packets in the interface's voice VLAN. As a result, the priority of the voice packets is not modified according to the priority settings for the voice VLAN.
- Condition: This symptom might occur if the interface is assigned to the voice VLAN and receives untagged packets that use an OUI address as the source MAC address.

201505200264

- Symptom: One VPN instance can receive and forward packets destined for another VPN instance.
- Condition: This symptom might occur if two MPLS L3VPN instances are configured on the switch.

201508060056

- Symptom: The OpenFlow process restarts unexpectedly after the switch receives flow entries from the controller.
- Condition: This symptom might occur if the flow entries contain the experimenter field.

201505040217

- Symptom: The **display lldp local-information** command displays the model of the original IRF master switch after an IRF master/subordinate switchover.
- Condition: This symptom might occur if the **display lldp local-information** command is executed after an IRF master/subordinate switchover.

201508030032

- Symptom: The switch sends the controller the ARP packets received in inband management VLANs.
- Condition: This symptom might occur if inband management VLANs are configured on the switch.

201508170165

- Symptom: In a single-ring RRPP network, the secondary port on the master node is up.
- Condition: This symptom might occur if the secondary port is a Layer 2 aggregate interface, and a member port of the aggregation group is replaced.

201505150213

- Symptom: Unexpected memory leaks cause all interfaces on the switch to go down and interrupt services.
- Condition: This symptom might occur if the switch processes packets that need to be sent to the CPU.

201507220169

- Symptom: The switch displays **The service BGP status failed : abnormal exit!** after certain operations are performed.
- Condition: This symptom might occur if the following operations have been performed:
    - **a.** Enable OSPF and BGP on the switch and its peer, and configure routing policies on the switch.
    - **b.** Delete the routing policies, and reconfigure the routing policies after OSPF processes are re-optimized.
    - **c.** Configure the same routing policy on the outbound and inbound directions of the peer.

201507170310

- Symptom: When the switch works with a Comware V5 device, IPsec authentication fails and packet loss occurs on the switch.
- Condition: This symptom might occur if the following operations have been performed on the switch:
  - Enable IKE negotiation for IPsec.
  - Enable PFS.
  - Use the **ipsec sa global-duration traffic-based** command to set a small traffic-based SA lifetime.

201508100310

- Symptom: The switch cannot establish OSPFv3 neighbor relationship with a peer.
- Condition: This symptom might occur if the following operations have been performed:
  a. Set the authentication mode to keychain on the interface connected to the peer.
  b. Add the switch to an IRF fabric.

201507220244

- Symptom: It takes a long time period to clear the packet statistics on interfaces through NETCONF.
- Condition: This symptom might occur if packet statistics on interfaces are cleared through NETCONF.

201506110236

- Symptom: NTP cannot synchronize the clock of the switch in an MPLS L3VPN network.
- Condition: This symptom might occur if the switch is in a VPN, and the **ntp-service peer acl** *acl-number* command is executed on the switch.

201507030050/TB201507170231

- Symptom: BGP flapping occurs on the switch.
- Condition: This symptom occurs if the following conditions exist:
  - The switch runs an sFlow agent.
  - sFlow is enabled on an interface.
  - The outgoing interface for sFlow packets is a Layer 3 aggregate interface or subinterface.

201507160185

- Symptom: The match rule configured for a DHCP user class cannot be successfully deleted.
- Condition: This symptom occurs if the **if-match rule** *rule-number* command and then the **undo if-match rule** *rule-number* command are executed in DHCP user class view.

201507290223

- Symptom: In a TRILL network, the **ping trill** command, which is used to identity whether an RB is reachable, outputs information after a delay.
- Condition: This symptom occurs if the **ping trill** command is executed in any view.

201505140078

- Symptom: When devices are connected through aggregate interfaces, the state of an interface cannot automatically recover after it changes.
- Condition: This symptom occurs if the following operations have been performed:
  a. Cross-connect the optical fibers.
  b. Swap the Tx and Rx fibers.

c. Restore the swap.

201505200478

- Symptom: A valid user fails to pass MAC authentication.
- Condition: This symptom occurs if the MAC authentication server is configured to bind the user IPv6 addresses for authentication.

201505250285

- Symptom: On an IRF fabric, some ARP entries and route entries still exist after Layer 3 flow entries are successfully deleted in batch.
- Condition: This symptom occurs if a master/subordinate switchover is performed for the IRF fabric.

201506030153

- Symptom: Traffic cannot be forwarded between transit nodes in an RRPP network.
- Condition: This symptom occurs if the following conditions exist:
  - Transit nodes are connected through aggregate interfaces.
  - The aggregation group member ports are shut down and brought up.

201506100433

- Symptom: Continuous loops appear in the network.
- Condition: This symptom occurs if the following conditions exist:
  - Devices are connected through aggregate interfaces.
  - The spanning tree protocol is enabled on the devices.
  - Some member ports are removed from the aggregation group.

201506150158

- Symptom: When switches are connected through aggregate interfaces, the spanning tree protocol packets cannot be correctly exchanged.
- Condition: This symptom occurs if RSTP is enabled and VRRP is configured to operate in non-preemptive mode on the devices.

201506260038

- Symptom: A user fails to be logged out.
- Condition: This symptom occurs if the following operations have been performed:
  a. The user passes 802.1X authentication and logs in.
  b. The FreeRADIUS server issues a command carrying the NAS-IP-Address attribute to forcibly log out the user.

201506290052

- Symptom: ARP packets cannot be forwarded between the switch and the controller.
- Condition: This symptom occurs if the switch sends ARP packets to the controller in an SDN network.

201506290068

- Symptom: A user cannot connect to the public network through Portal authentication.
- Condition: This symptom occurs if a large number of log in and log out and continuously access the external network.

201506290195

- Symptom: A user fails to remotely log in to the switch through a VTY line.

- Condition: This symptom occurs if the following operations have been performed:
  a. Configure the **authentication-mode none** command in VTY line view, and save the configuration.
  b. Reboot the switch.

201508180154

- Symptom: A transceiver module is started correctly. However, the QSFP+ interface state might frequently switch between up and down.
- Condition: This symptom occurs if the switch has a QSFP-40G-LR4-WDM1300 transceiver module (the model is H4C1QE1C-H3C) installed.

201508050374

- Symptom: The interfaces at both ends of a link bounce up and down.
- Condition: This symptom occurs if a local interface is split into four breakout interfaces and these interfaces are connected to the peer device.

201507140229/201507140225

- Symptom: Known multicast packets with TTL 1 are dropped.
- Condition: This symptom occurs if the following conditions exist:
  - IGMP snooping is enabled on the switch.
  - The multicast packets with TTL 1 are forwarded within a VLAN.

201507220065/201508050136/201507170127

- Symptom: The switch authorizes a user that uses an incorrect password to initiate authentication.
- Condition: This symptom might occur if the user uses NETCONF and HWTACACS authentication when it logs in to the switch.

201507160037

- Symptom: The switch drops a gratuitous ARP packet and does not update the ARP table if the target IP address of the packet is 0.0.0.0, 255.255.255.255, or a directed broadcast address.
- Condition: This symptom might occur if the switch receives a gratuitous ARP packet with the target IP address as 0.0.0.0, 255.255.255.255, or a directed broadcast address.

201508170121

- Symptom: A VPLS VSI cannot forward traffic if another VPLS VSI is up.
- Condition: This symptom might occur if the VSIs generate the same label.

201508300024

- Symptom: The aggregation member ports on an IRF subordinate switch cannot forward traffic after the switch is rebooted.
- Condition: This symptom might occur if the ports are in a cross-chassis aggregation group.

201507270359

- Symptom: The ARP blackhole route for an interface is deleted 25 seconds after the interface goes down. As a result, the FIB table is not updated within this period.
- Condition: This symptom might occur if an IP packet matches a network route for the interface after the corresponding ARP entry is already deleted. The switch will send an ARP request and issue an ARP blackhole route.

201509230128

- Symptom: The serial interfaces of an IRF fabric do not respond if configuration of the management interface is displayed or the interface is shut down.
- Condition: This symptom might occur if the following operations have been performed:
  a. Execute the **ping trill** or **tracert trill** command.
  b. Reboot an IRF member switch.

201504100150

- Symptom: The DBM memory leaks when the **display this** command is executed in VSI view.
- Condition: This symptom occurs if selective flood is enabled for a MAC address on the VSI.

201504100143

- Symptom: The DBM memory is not released.
- Condition: This symptom occurs if the switch is rebooted after the **ip address** *ip-address* **vpn-instance** *vpn-instance-name* command is configured.

201506180198

- Symptom: The memory of the switch is occupied.
- Condition: This symptom occurs if the following conditions exist:
  - Static routes are redistributed on two devices configured with OSPF. These static routes have the same destination address. The outgoing interfaces of the static routes are enabled with OSPF and their network type is broadcast.
  - The network flaps.

201412050511

- Symptom: After DHCP Snooping is enabled, the terminals in a secondary VLAN of the private VLAN cannot obtain IP addresses through DHCP.
- Condition: This symptom occurs if DHCP snooping is enabled and secondary VLANs of the private VLAN are configured.

201502160178

- Symptom: OpenFlow packets cannot be forwarded by using a MAC-IP flow table after a master/subordinate switchover on an IRF fabric.
- Condition: This symptom occurs if the ARP table is modified during the master/subordinate switchover.

201505090053

- Symptom: In an OpenFlow network, the CPU usage of the syslogd process is high when a large number of ARP packets match flow entries and are sent to the controller.
- Condition: This symptom occurs if a large number of ARP packets match flow entries in the OpenFlow network.

201504200089

- Symptom: In a basic MPLS L3VPN, the switch prints the COPP stack information.
- Condition: This symptom occurs if the basic MPLS L3VPN functions are configured and traffic is forwarded correctly.

201505140415

- Symptom: The LACP MAD state flaps repeatedly.
- Condition: This symptom occurs if LACP MAD is configured.

201503060016

- Symptom: During the flow entry deployment process, the switch is disconnected from the OpenFlow controller and reconnects to the OpenFlow controller.
- Condition: This symptom occurs if a large number of flow entries are deployed.

201504090145

- Symptom: The switch is disconnected from the OpenFlow controller and reconnects to the OpenFlow controller.
- Condition: This symptom occurs if the switch is in an IRF fabric and the master member switch of the IRF fabric is rebooted.

201504150070

- Symptom: The duration of the flow entry in the Flow-Removed message that the switch sends to the OpenFlow controller is 1 second longer than the hard_timeout value in the flow entry when the flow entry is deployed.
- Condition: This symptom occurs if the switch is connected to an OpenFlow controller.

201412080352

- Symptom: After the **ipv6 address dhcp-alloc** and **ipv6 dhcp client duid mac** commands are executed on the management interface, the interface successfully obtains an IPv6 address prefix and a default route. The switch cannot obtain an IPv6 address after the switch is rebooted even if the configuration has been saved.
- Condition: This symptom might occur if the following operations have been performed:
  - **a.** Execute the **ipv6 address dhcp-alloc** and **ipv6 dhcp client duid mac** commands on the management interface.
  - **b.** Save the configuration and reboot the switch.

201502060453

- Symptom: An interface cannot forward traffic if the **trill evb-support** and **evb enable** commands are executed on the interface.
- Condition: This symptom might occur if the **trill evb-support** and **evb enable** commands are executed on the interface.

201503300339

- Symptom: The switch does not prompt for incorrect operations when non-existent VLANs are replaced through NETCONF.
- Condition: This symptom might occur if non-existent VLANs are replaced through NETCONF.

201504230156

- Symptom: Residual BFD session information exists if the **tunnel bfd enable destination-mac** and **undo tunnel bfd enable** commands are repeatedly executed.
- Condition: This symptom might occur if the **tunnel bfd enable destination-mac** and **undo tunnel bfd enable** commands are repeatedly executed.

201505180103

- Symptom: An NMS retrieves an incorrect hh3cEntityExtErrorStatus value for a copper transceiver module installed on the switch.
- Condition: This symptom might occur if the NMS retrieves the hh3cEntityExtErrorStatus value for a copper transceiver module installed on the switch.

201506050167

- Symptom: NQA operations fail if they are performed frequently.

- Condition: This symptom might occur if NQA operations are performed frequently.

201504140260

- Symptom: Information for the **display mac-address mac-move** command is not included in the output from the **display diagnostic-information** command.
- Condition: This symptom might occur if the **display diagnostic-information** command is executed.

201507140337

- Symptom: Tracert operation fails if the route to the destination host is unknown.
- Condition: This symptom might occur if the route to the destination host is unknown.

201501060627

- Symptom: The driver of an IRF subordinate switch does not support portal rule assignment.
- Condition: This symptom might occur if the following conditions exist.
  - **a.** A large number of portal users come online through an interface on the IRF master switch.
  - **b.** A master/subordinate switchover is performed.

201501260549

- Symptom: AAA memory leak occurs if LDAP authentication is repeatedly performed.
- Condition: This symptom might occur if LDAP authentication is repeatedly performed.

201504080051/201504080056/201504080046/201501260561

- Symptom: Read and write permissions for some files do not meet the requirements of the system.
- Condition: This symptom might occur if the switch starts properly, and read and write permissions for some files do not meet the requirements of the system.

201502030659

- Symptom: Handle leak occurs if the **display ipv6 netstream cache** command is repeatedly executed.
- Condition: This symptom might occur if the **display ipv6 netstream cache** command is repeatedly executed.

201502030665

- Symptom: Handle leak occurs if the **display ip netstream cache** command is repeatedly executed
- Condition: This symptom might occur if the **display ip netstream cache** command is repeatedly executed.

201504150067

- Symptom: The switch does not return an error message when the Groupmod message for a group entry contains invalid weight values and the group type of the group entry is not **select**.
- Condition: This symptom occurs when the following conditions exist:
  - The Groupmod message for a group entry contains invalid weight values.
  - The group type of the group entry is not **select**.

201505070194

- Symptom: An IRF fabric does not update the ARP entry for a MAC address when the MAC address moves between member switches in an IRF fabric.
- Condition: This symptom occurs if the MAC address learned on one member switch moves to another member switch in the IRF fabric.

201410100191

- Symptom: The iMC BIMS component does not delete user logs and configuration file when restoring the factory default configuration for the switch.
- Condition: This symptom occurs if the factory default configuration is restored through the iMC BIMS component.

201503240442

- Symptom: The **Permission denied** message is displayed when a user issues the **undo interface Bridge-Aggregation1** command without entering a space between the interface type and the interface number.
- Condition: This symptom occurs if the user role is permitted to use all read, write, and execute commands of the LACP feature.

201409230444

- Symptom: An switch continuously sends pause frames to the uplink switch.
- Condition: This symptom occurs if the server attached to the switch continuously sends pause frames to the switch.

201506250315

- Symptom: An S-channel interface receives packets with the VLAN ID as 0.
- Condition: This symptom occurs if the following operations are performed:
    - **a.** Enable EVB on the Layer 2 Ethernet interface where the S-channel interface is created.
    - **b.** Send untagged packets to the S-channel interface.

201506050282

- Symptom: An LSU containing an LSA with a length of 264 fails to be sent out.
- Condition: This symptom occurs if the OSPF NSR is enabled.

201412190247

- Symptom: The time zones for MAC address move time are incorrect.
- Condition: This symptom occurs if the **clock timezone** command is used to set the local time zone.

201507090470

- Symptom: The VCF controller fails to authenticate to its connected switch through TACACS.
- Condition: This symptom occurs if the TACACS authentication is configured on the switch through NETCONF.

201503030448

- Symptom: A card on the EVB switch reboots because of memory leaks.
- Condition: This symptom occurs if the EVB switch communicates with an EVB server on that card.

201503300341/201503300336

- Symptom: An interface still operates in Layer 3 mode after NETCONF is used to roll back the configuration.
- Condition: This symptom occurs if the interface operates in Layer 2 mode before the rollback point.

201504150066

- Symptom: When the OpenFlow switch receives a SET_CONFIG message with an invalid flag value, the OpenFlow switch does not report an error to the controller.

- Condition: This symptom occurs if the controller sends messages with invalid flag values in an OpenFlow network.

201504160118

- Symptom: When the bridge MAC address is added as a blackhole MAC address entry for the first time, the system displays that the entry already exists.
- Condition: This symptom might occur if the **mac-address blackhole** *mac-address* **vlan** *vlan-id* command is executed to add the bridge MAC address as a blackhole MAC address entry.

201503180401

- Symptom: The switch fails to output information for the **display ip load-sharing path** command.
- Condition: This symptom might occur if the following operations have been performed:
  - **a.** Execute the **ip load-sharing mode per-flow dest-ip src-ip dest-port src-port** command.
  - **b.** Execute the **display ip load-sharing path** command.

201505190278

- Symptom: In a TRILL network, an egress RB cannot forward TRILL broadcast traffics out of the outgoing interface.
- Condition: This symptom might occur if TRILL is globally enabled on the RB, and the outgoing interface is assigned to a VLAN.

201506030299

- Symptom: A DHCP server cannot ping DHCP clients if many-to-one VLAN mappings are configured on the intermediate device between them.
- Condition: This symptom might occur if the following conditions exist:
  - The DHCP server is connected to the DHCP clients through the intermediate device.
  - The DHCP server and clients are in different VLANs. Many-to-one VLAN mappings are configured on the intermediate device's interface connected to the DHCP clients.
  - The **dhcp snooping trust**, **arp detection enable**, and **vlan-mapping nni** commands are executed on the intermediate device's interface connected to the DHCP server.

201503300139

- Symptom: Though 32 Selected ports exist in an aggregation group, only 16 of them forward traffic.
- Condition: This symptom might occur if unicast traffic is sent to the aggregation group

201506030342

- Symptom: The forwarding path in the output from the **display link-aggregation load-sharing path** command is not the actual forwarding path.
- Condition: This symptom might occur if an aggregation group receives unicast traffic.

201505110081

- Symptom: Packets forwarded out of S-channel interfaces have only one VLAN tag.
- Condition: This symptom might occur if the switch is operating in FCoE mode and receives traffic.

201507020134

- Symptom: The switch does not remove the customer VLAN tag from FCoE packets when it forwards the packets out of an S-channel interface.
- Condition: This symptom might occur if the PVID of the S-channel interface matches the customer VLAN tag of the FCoE packets.

201507030086

- Symptom: After the **encapsulation default** command is executed on an Ethernet service instance, frame match criteria on other Ethernet service instances no longer take effect.
- Condition: This symptom might occur if the **encapsulation default** command is executed on one of the Ethernet service instances on the switch.

201506120267

- Symptom: Execution of the **mac-address static source-check enable** command fails on a Layer 3 aggregate interface.
- Condition: This symptom might occur if the **mac-address static source-check enable** command is executed on the Layer 3 aggregate interface.

201504130020/201504130191

- 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.
- Symptom: CVE-2015-0286
- Condition: DoS vulnerability in certificate verification operation. Any application which performs certificate verification is vulnerable including OpenSSL clients and servers which enable client authentication.
- 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.
- Symptom: CVE-2015-0288
- Condition: The function X509_to_X509_REQ will crash with a NULL pointer dereference if the certificate key is invalid.
- Symptoms: 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.

TB201504140268

- Symptom: CVE-2015-1799
- Condition: Authentication doesn’t protect symmetric associations against DoS attacks.

201506030144（CVE-2015-5434）

- Symptoms: When an interface without MPLS enabled receives MPLS-labeled packets, the interface incorrectly forwards the MPLS-labeled packets to the next LSR by LFIB entry.
- Condition: This symptom occurs when the interface does not have MPLS enabled and the interface receives MPLS-labeled packet that match the FIB entries.

201507310040

- Symptom: CVE-2015-3143
- Condition: cURL and libcurl 7.10.6 through 7.41.0 does not properly re-use NTLM connections, which allows remote attackers to connect as other users via an unauthenticated request.
- Symptom: CVE-2015-3148
- Condition: cURL and libcurl 7.10.6 through 7.41.0 does not properly re-use authenticated Negotiate connections, which allows remote attackers to connect as other users via a request.

201507160287

- Symptom: CVE-2014-8176
- Condition: If a DTLS peer receives application data between the ChangeCipherSpec and Finished messages. May result in a segmentation fault or potentially, memory corruption.
- 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.
- 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.
- 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.
- Symptom: CVE-2015-1791
- Condition: If a NewSessionTicket is received by a multi-threaded client when attempting to reuse a previous ticket then a race condition can occur potentially leading to a double free of the ticket data.
- Symptom: CVE-2015-1792
- Condition: When verifying a signedData message the CMS code can enter an infinite loop. This can be used to perform denial of service against any system which verifies signedData

201505210464

- Symptom: Inbound packet capture does not take effect.
- Condition: This symptom might occur if the following operations have been performed:
  a. Install the packet capture software package.
  b. Execute the **packet-capture** command to enable inbound packet capture.

Resolved problems in R2418P01

201502120368

- 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.
- Symptom: CVE-2014-3571
- Condition: A carefully crafted DTLS message can cause a segmentation fault in OpenSSL due to a NULL pointer dereference. This could lead to a Denial Of Service attack.
- Symptom: CVE-2015-0206
- Condition: A memory leak can occur in the dtls1_buffer_record function under certain conditions. In particular this could occur if an attacker sent repeated DTLS records with the same sequence number but for the next epoch. The memory leak could be exploited by an attacker in a Denial of Service attack through memory exhaustion.
- 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.

- 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.
- 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.
- 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.
- 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.
- 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.

201412300447

- Symptom: A device cannot be pinged when it is directly connected to an aggregate interface.
- Condition: This symptom occurs if TRILL is enabled (**trill enable**) and then disabled (**undo trill enable**) on the aggregate interface.

201504250083

- Symptom: Some IRF member switches print the message "OVERLAYMACD ha upgrade failed" and these switches enter kdb.
- Condition: This symptom occurs when the following conditions exist:
  - A large number of known unicast packets with changing source MAC addresses are sent to the IRF fabric.
  - Master/subordinate switchover occurs in the IRF fabric.

201504160288

- Symptom: The console port displays garbled characters. This problem is solved after you log out and then log in through the console port again.
- Condition: This symptom occurs when the VLANs to which a port belongs are modified.

201504090111

- Symptom: Serious packet loss occurs to Layer 3 packets forwarded by the switch,
- Condition: This symptom occurs when the following conditions exist:
  - The number of route entries exceed 8K.
  - uRPF is enabled and then disabled.

201502050608

- Symptom: A QoS policy fails to be applied to some VLANs because of insufficient ACL resources when ACL resources are sufficient.
- Condition: This symptom occurs if the following conditions exist:
    - A traffic class in the QoS policy includes both IPv4 and IPv6 ACLs as match criteria.
    - IPv4 ACLs are removed from the traffic class after the system displays a message that indicates insufficient ACL resources.

201503130390

- Symptom: An aggregate interface forwards packets received on a member port out of another member port in the aggregation group.
- Condition: This symptom occurs if the following operations are performed:
    a. Configure an aggregation group on an IRF fabric with its member ports on different IRF member devices.
    b. Configure two Ethernet service instances on the aggregate interface, and map them to one VSI.

201503260342

- Symptom: A member port of an aggregation group cannot establish a micro BFD session with the peer port.
- Condition: This symptom occurs if the member port establishes a micro BFD session for multihop detection.

201504150256

- Symptom: An interface prints MAC address change information repeatedly for a previously learned MAC address when no MAC address is added.
- Condition: This symptom occurs if the following operations are performed:
    - The **mac-address information mode syslog** command is configured.
    - The **mac-address information enable** command is configured in system view.
    - The **mac-address information enable added** command is configured on an interface after the interface learns a MAC address.

201502160178

- Symptom: OpenFlow packets cannot be forwarded by using a MAC-IP flow table after a master/subordinate switchover on an IRF fabric.
- Condition: This symptom occurs if the ARP table is modified during the master/subordinate switchover.

201409180122

- Symptom: Layer 3 traffic is broadcast on an access switch.
- Condition: This symptom occurs if the following conditions exist:
    - The access switch does not support TRILL.
    - TRILL VRs are configured on the distribution switches.

201502160108

- Symptom: iMC cannot connect to a managed switch and generates an ICMP no response alarm for the switch.
- Condition: This symptom occurs if the switch suffers from attacks on the ipForwarding and ipDefaultTTL nodes.

201412190247

- Symptom: The time zones for MAC address move time are incorrect.
- Condition: This symptom occurs if the **display mac-address mac-move** command is executed.

201503020059

- Symptom: Modifying or deleting an OpenFlow MAC-IP flow entry results in a memory leak.
- Condition: This symptom occurs if the output port of a MAC-IP flow entry is modified or a MAC-IP flow entry with an output port is deleted.

201502070165

- Symptom: An IS-IS primary route cannot be installed into the routing table.
- Condition: This symptom occurs if the following conditions exist:
  - The primary route is learned from a neighbor.
  - IS-IS FRR is enabled, but the backup next hop is unavailable.

201502040503

- Symptom: The state of the BFD session in an IRF fabric toggles between down and init for 10 minutes after the IRF fabric splits.
- Condition: This symptom occurs if BFD MAD and uRPF are configured on the IRF fabric.

201412200068

- Symptom: The **jumboframe enable 1536** or **undo jumboframe enable** command does not take effect.
- Condition: This symptom occurs if the **undo jumboframe enable** or **jumboframe enable 1536** command has been configured.

201501280247

- Symptom: The switch forwards some IP traffic to incorrect VPNs.
- Condition: This symptom occurs if two ARP entries exist for one IP address because the output interface of an ARP entry changes.

201502160110

- Symptom: The switch acting as an access device in a portal system logs out a portal client after the client reboots.
- Condition: This symptom occurs if the following conditions exist:
  - Portal roaming is enabled.
  - DHCP server or DHCP relay agent is enabled on the interface connected to the portal client.
  - The interface connected to the portal client changes during the reboot of the portal client.

201503100015

- Symptom: The member ports in an aggregation group on the master switch in an IRF fabric cannot be selected.
- Condition: This symptom might occur after the entire IRF fabric is rebooted.

201501270115

- Symptom: A walk on the hh3cVsiStatistics node times out.
- Condition: This symptom occurs if the following operations are performed:
  - **a.** Configure 4095 VSIs (the upper limit).
  - **b.** Perform a walk on the hh3cVsiStatistics node by using a MIB tool.

201502090577

- Symptom: Tunnels established by using ENDP in an IRF fabric have tunnel interface views.
- Condition: This symptom occurs if master election occurs multiple times.

201503130204

- Symptom: In a non-default MSTI, all the four 10 GE breakout interfaces split from a 40 GE interface are in incorrect port states and cannot forward packets.
- Condition: This symptom occurs when the following conditions exist:
  - MSTP is disabled globally.
  - VLAN 1 is mapped to the non-default MSTI.

201501130302

- Symptom: The class-based accounting action does not take effect on a Layer 3 aggregate subinterface.
- Condition: This symptom occurs if a QoS policy containing the class-based accounting action is applied to a Layer 3 aggregate subinterface.

201502120452

- Symptom: The minimum guaranteed bandwidth setting does not take effect.
- Condition: This symptom occurs if you assign a queue to the WRR group and set the minimum guaranteed bandwidth for the queue in a queue scheduling profile.

201502120422

- Symptom: The **display qos qmprofile configuration** command displays the value previously set for the minimum guaranteed bandwidth after the **undo bandwidth queue** command is executed.
- Condition: This symptom occurs if the following operations are performed:
  - **a.** Set the minimum guaranteed bandwidth in a queue scheduling profile.
  - **b.** Execute the undo bandwidth queue command to delete the minimum guaranteed bandwidth setting.

201503120210

- Symptom: An interface enabled with the DHCP relay agent drops DHCP packets.
- Condition: This symptom occurs if the interface is configured with secondary VLANs.

201501130340

- Symptom: The information format of the **display trill interface** command output is incorrect.
- Condition: This symptom occurs when the **display trill interface** command is executed.

201502090087

- Symptom: A Layer 3 Ethernet interface with subinterfaces leaves its interface range.
- Condition: This symptom occurs when the Layer 3 Ethernet interface is configured as a Layer 2 Ethernet interface.

201501290469

- Symptom: A 10 GE copper port cannot communicate with the connected 100 Mbps NIC on a PC.
- Condition: This symptom occurs if the 10 GE copper port is configured to negotiate a speed with its peer.

201501280230

- Symptom: An aggregate interface is in an incorrect STP port state.
- Condition: This symptom occurs if the following operations are performed:
  a. Create a large number of S-channels on the aggregate interface.
  b. Shut down and bring up each member port in the aggregation group repeatedly.

201501130051

- Symptom: An aggregate interface is not in the same VLAN as its member ports and cannot forward packets.
- Condition: This symptom occurs if the following operations are performed:
  a. Create an aggregation group and assign interfaces with continuous numbers to the aggregation group.
  b. Create an interface range and assign all member ports in the aggregation group to the interface range.
  c. Copy the configuration in interface range view.
  d. Delete the configuration in interface range view by using the default command and quickly apply the copied configuration to the interface range.

201503200087

- Symptom: An interface connected to a server in a slot of an C3000 or C7000 enclosure goes down and comes up.
- Condition: This symptom occurs when a different server is installed into or removed from another slot in the C3000 or C7000 enclosure.

Resolved problems in R2417

201504270026

- Symptom: Loops occur after two directly connected aggregate interfaces are assigned to the same VLANs as trunk ports.
- Condition: This symptom occurs if the following conditions exist:
  - TRILL is enabled on the two aggregate interfaces.
  - The link type of each aggregate interface is set to access.

201410220620

- Symptom: The CLI might be halted and not respond for tens of minutes. After the **port link-mode** command is executed on an interface to change its link mode, the **display interface** command cannot display the interface.
- Condition: This symptom occurs when the following conditions exist:
  - The switch is in an IRF fabric and is connected to other devices through aggregate interfaces to form an RRPP network. About 40 RRPP domains are created.
  - The **shutdown** and then **undo shutdown** commands are repeatedly executed on the aggregate interfaces.
  - The **port link-mode** command is repeatedly executed on the interface to change its link mode.

201410280446

- Symptom: After the switch is rebooted, the operation of canceling SPBM-related configurations does not take effect.
- Condition: This symptom occurs after the following procedure is performed:

a. The switch is enabled with SPBM and configured with some SPBM features.
b. The configuration is saved.
c. The switch is rebooted.

201412230343

- Symptom: IPv6 routes do not take effect. Some unknown Layer 3 unicast packets cannot trigger ARP entry learning.
- Condition: This symptom occurs after the switch is changed to the switch-mode 4 mode.

201412180455

- Symptom: An IRF fabric cannot be rebooted.
- Condition: This symptom occurs after the following procedure is performed:
  a. Execute the mac-address notification mac-move suppression command on the IRF fabric.
  b. Save the configuration and reboot the entire IRF fabric.

201412090452

- Symptom: When multicast traffic is forwarded between sub VLANs, the forwarding entries still exist after sub VLANs are dissociated from its super VLAN.
- Condition: This symptom occurs after the following procedure is performed:
  a. Configure a super VLAN and associate it with sub VLANs.
  b. After sub VLANs receive multicast traffic, the debug ipmc show entry all command shows that forwarding entries have been set up.
  c. Dissociate the sub VLANs from the super VLAN.
  d. The display multicast forwarding-table command shows that the forwarding entries for the sub VLANs have been deleted. The debug ipmc show entry all command shows that the forwarding entries still exist.

201409260342

- Symptom: The automatic configuration feature in HTTP Python method cannot be used.
- Condition: This symptom occurs if the following conditions exist when you configure the DHCP server on the switch:
  - The DHCP server address pool has the address of the TFTP server.
  - The DHCP server has an automatic configuration file in the HTTP Python method.

201412170483

- Symptom: After the master/subordinate switchover in an IRF fabric, aggregation group member ports cannot become Selected.
- Condition: This symptom occurs after the following procedure is performed:
  a. In the IRF fabric, configure link aggregation to collaborate with BFD on all aggregate interfaces.
  b. Perform a master/subordinate switchover in the IRF fabric.

201412230215

- Symptom: The Tcl script cannot be executed correctly on the switch.
- Condition: This symptom occurs when the Tcl script to be executed contains two or more continuous new lines.

201412260153

- Symptom: The track status of a TRILL port is different from the status of the associated track entry.

- Condition: This symptom occurs after the following procedure is performed:
  a. Associate the TRILL port with a track entry.
  b. Restart the TRILL protocol.

201409180268

- Symptom: Incomplete greeting (MOTD) banner is displayed when a console user logs in an IRF fabric through a console port.
- Condition: This symptom occurs if you perform the following steps:
  a. Use the header motd command to configure a greeting banner after logging in through the console port.
  b. Log off the console port.
  c. Log in again through the console port.

201411040009

- Symptom: The UID LED on an IRF subordinate device cannot blink.
- Condition: This symptom occurs if the subordinate device is upgraded with the software images of the master device by using the **boot-loader update** command.

201412310012

- Symptom: The value read from the hh3cifPktBufFree MIB object is not the same as the remaining buffer size displayed by using the **display buffer usage** command.
- Condition: This symptom occurs if you use the **display buffer usage** command and a MIB tool to obtain the remaining buffer size.

201412020354

- Symptom: Hosts cannot ping the gateway when primary and secondary VLANs are configured.
- Condition: This symptom might occur if the following steps are performed:
  a. Configure the VLAN interface for the primary VLAN, and bind the interface to a VPN instance.
  b. Associate the primary VLAN with a list of secondary VLANs by using the private-vlan command.

201501040129

- Symptom: The packet filter on a VLAN interface filters Layer 2 traffic.
- Condition: This symptom might in either of the following situations:
  - The **packet-filter filter route** command, and then the packet filtering rules are configured when the VLAN interface is up.
  - The **packet-filter filter route** command, and then the packet filtering rules are configured when the VLAN interface is down. Then, the VLAN interface is brought up.

201501300449

- Symptom: The device does not forward spanning tree protocol BPDUs without processing them when the spanning tree feature is disabled.
- Condition: This symptom occurs when the spanning tree feature is globally disabled.

201412200068

- Symptom: The **display interface** command shows that the maximum frame length setting is 1536. However, the maximum length of frames that can pass through is only 1518.
- Condition: This symptom occurs if the command is used in Layer 2 interface view to prevent jumbo frames to pass through.

201412190083

- Symptom: The QoS priority set for voice traffic by using the voice-vlan qos command does not take effect.
- Condition: This symptom occurs if the lldp tlv-enable med-tlv network-policy vlan-id command has been configured to advertise voice information through LLDP/CDP.

201412230382

- Symptom: The packet statistics feature cannot work correctly for Ethernet service instances created on a Layer 2 aggregate interface that uses multichassis aggregation on the IRF fabric.
- Condition: This symptom occurs if a subordinate device reboots. The packet statistics feature will be unable to count the traffic that pass through the member links on the subordinate device.

Resolved problems in R2406P02

CVE-2014-3567

- Symptom: CVE-2014-3567.
- Condition: When an OpenSSL SSL/TLS/DTLS server receives a session ticket the integrity of that ticket is first verified. In the event of a session ticket integrity check failing, OpenSSL will fail to free memory causing a memory leak. By sending a large number of invalid session tickets an attacker could exploit this issue in a Denial of Service attack.

SSL 3.0 Fallback protection

- 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).

CVE-2014-3568

- Symptom: CVE-2014-3568.
- Condition: When OpenSSL is configured with "no-ssl3" as a build option, servers could accept and complete a SSL 3.0 handshake, and clients could be configured to send them.

201411280162

- Symptom: The switch cannot respond to a multi reply message, and it is disconnected from the controller.
- Condition: This symptom occurs when the following conditions exist:
  - The controller deploys two flow entries. The table-miss flow entry is not the default (by default, a table-miss flow entry drops packets).
  - The controller queries information about flow entries.

201410130397

- Symptom: BGP routes are learned very slowly.
- Condition: This symptom occurs when a large number of routes with changed AS path attributes are injected to the switch.

201412090206

- Symptom: When you Telnet to a switch and view the memory usage for the Telnet process, no information is displayed.

- Condition: This symptom occurs when the following procedure is performed:
    - Telnet to the switch.
    - Use the display process memory heap command to view the memory usage for the Telnet process.

201411280348

- Symptom: After mirroring packets to a CPU is configured, the packets mirrored to the CPU are incorrectly encapsulated.
- Condition: This symptom occurs when the following conditions exist:
    - Configure mirroring packets to a CPU.
    - View the contents of packets mirrored to the CPU.

201411110152

- Symptom: LLDP information for a 40-GE interface is incorrectly displayed.
- Condition: This symptom occurs when the following conditions exist:
    - LLDP is enabled globally and on the 40-GE interface.
    - The **display lldp neighbor-information verbose** command is used to display the detailed LLDP information for the 40-GE interface.

201410150732

- Symptom: When Layer 3 traffic passes through a network management interface, the network management interface operates incorrectly.
- Condition: This symptom occurs when the following conditions exist:
    - The network management interface operates at 100 Mbps and at half duplex mode through autonegotiation.
    - Incoming packets and outgoing packets appear on the network management interface at the same time.

201411070472

- Symptom: When a link-down event occurs to an aggregation group member port, the link down SNMP traps are not sent as expected.
- Condition: This symptom occurs when the following conditions exist:
    - The switches form an IRF fabric. One interface on the master member switch and one interface on the subordinate member switch are assigned to an Layer 2 aggregate interface.
    - When the member port on the master member switch is shut down, the member port on the subordinate member switch does not send link down SNMP traps carrying ifAdminstatus and IfOperStatus. When the member port on the subordinate member switch is shut down, the link down traps can be sent.

201411130364

- Symptom: Static routes fail to be issued.
- Condition: This symptom occurs when the following conditions exist:
    - NETCONF is used to issue static routes.
    - The value of <NexthopVrfIndex></NexthopVrfIndex> is different from the value of <DestVrfIndex></DestVrfIndex>.

201410240289

- Symptom: Flow mirroring cannot obtain the destination MAC address for an ARP entry, and the destination MAC address is displays as all-Fs.
- Condition: This symptom occurs when the following conditions exist:

- Configure the destination IP address of remote flow mirroring as a directly-connected IP address.
- Shut down and then bring up the VLAN interface identified by the destination IP address.

201410150536

- Symptom: The switch displays errors in logs showing that "The driver does not support rule assignment."
- Condition: This symptom occurs when the following conditions exist:
  - Cross-subnet portal authentication is enabled in an IRF fabric.
  - A user logs in successfully and traffic can be transmitted.

201410220398

- Symptom: A special configuration file name causes the configuration file comparison feature to fail.
- Condition: This symptom occurs when a configuration file with a name containing "%s" is specified as the startup configuration file.

201412130015

- Symptom: In an IRF fabric, the system fails to allocate memory for sending packets on the subordinate.
- Condition: This symptom occurs when the interfaces on the subordinate are repeatedly brought up and shut down.

201412120208

- Symptom: After a packet is forwarded through MPLS, the DSCP precedence information in the original IP packet is lost.
- Condition: This symptom occurs when the following conditions exist:
  - The switch is configured with an MPLS L3VPN.
  - The switch receives an MPLS packet. The original IP packet of the MPLS packet contains the DSCP precedence information.

201410140570

- Symptom: A downlink aggregation group member port of a monitor link group is down.
- Condition: This symptom occurs when the uplink ports of the monitor link group are shut down.

201410110066

- Symptom: The **ipv6 dhcp client duid mac** command might still exist on a VLAN interface.
- Condition: This symptom occurs when the following procedure is performed:
  - Configure the ipv6 dhcp client duid mac command in VLAN interface view.
  - Delete the VLAN interface.
  - Create the VLAN interface.

201412090054

- Symptom: The BFD session on a tunnel interface is always down.
- Condition: This symptom occurs when the following procedure is performed:
  - Create a tunnel interface, and configure the tunnel mode of the interface as GRE over IPv4.
  - Configure OSPF BFD on the tunnel interface.

201411270333

- Symptom: When the table-miss flow entry is restored to the default, it does not support collecting packet statistics.

- Condition: This symptom occurs when the following conditions exist:
  - The ACL table-miss flow entry configured for the OpenFlow instance is activated.
  - The ACL table-miss entry is deleted manually or aged.

201411170127

- Symptom: An aggregation group member port cannot get the LLDP neighbor information.
- Condition: This symptom occurs when the following procedure is performed:
  - Shut down the aggregate interface.
  - Bring up the aggregate interface when the member port is physically up.

201411280337

- Symptom: An SSH client fails to log in to the switch.
- Condition: This symptom occurs when the following conditions exist:
  - The switch acts as the SSH server and is configured with RSA and DSA key pairs.
  - The SSH client uses the RSA public key algorithm.

201411070457

- Symptom: The **display mac-address** command does not display any MAC address entries.
- Condition: This symptom occurs when private VLAN is configured on the switch and traffic arrives at the switch.

201411060615

- Symptom: The system displays an error message showing that "The service OFP status failed: abnormal exit!"
- Condition: This symptom occurs when OFP instances are activated in an IRF fabric.

201412050065

- Symptom: The switch displays a message showing that "incompatible with hardware." The **boot-loader file** command fails to be executed.
- Condition: This symptom occurs when the **boot-loader file** command is used to specify the startup software package or .IPE file.

201409100557

- Symptom: The output from the **display stp brief** command executed on an IRF fabric shows information about ports that are not enabled with STP.
- Condition: This symptom can be seen if the following procedure is performed:
  - Enable global STP on an IRF fabric and enable STP on ports of the master and subordinate.
  - Save the configuration and reboot the IRF fabric.
  - Execute the display stp brief command.

201409090165

- Symptom: The switch reboots unexpectedly.
- Condition: This symptom occurs when about 4K DHCP users come online or renew leases.

201409050316

- Symptom: The NTP process exits unexpectedly on the switch.
- Condition: This symptom occurs when the following procedure is performed:
  - **a.** The switch is configured with NTP.
  - **b.** The configuration is saved and then the switch is restarted.
  - **c.** The switch receives private packets in NTP mode 7 after it is started.

201408220191

- Symptom: After the switch is patched or the aggregation process is restarted, the member ports in Individual state in an aggregation group leave the aggregation group and cannot be assigned to the aggregation group.
- Condition: This symptom occurs when aggregation group member ports in Individual state exist on subordinate member switches of an IRF fabric.

201409260401

- Symptom: When the actions in an OpenFlow flow entry include sending packets to the controller and directing packets to a meter, the packets matching the flow entry cannot be sent to the controller.
- Condition: This symptom occurs when the actions in an OpenFlow flow entry include sending packets to the controller and directing packets to a meter.

201409260353

- Symptom: The system displays a message showing "`The service OFP status failed : abnormal exit!`".
- Condition: This symptom occurs when the following conditions exist:
  - OpenFlow deploys a meter associated with the table-miss flow entry and then deletes the meter.
  - Traffic to be processed by the table-miss flow entry arrives at the switch.

201410090209

- Symptom: A subordinate IRF member switch might reboot twice.
- Condition: This symptom occurs when the following procedure is performed:
  - Use 40-G transceiver modules and fibers to connect switches to form an IRF fabric.
  - Reboot the IRF fabric.

201409050328

- Symptom: When a command is used on the peer end to display the neighbor's LLDP information, the output shows that the rate and duplex mode of the local interface connected to the peer is as follows:
  - The speed is 0.
  - The duplex mode is unknown.
- Condition: This symptom occurs when the following conditions exist:
  - LLDP is enabled globally and on all ports on the local switch.
  - The local switch is connected to the peer end through 40G QSFP+ transceiver modules of the CSR4 type.

201404140063

- Symptom: When the **display transceiver manuinfo** command is used to display electronic label information about a transceiver module, the system displays a message showing that "The transceiver does not support this function."
- Condition: This symptom occurs when a DWDM SFP+ transceiver module for which the electronic label information has been written is installed.

201408130322

- Symptom: After a 40-GE interface is split into four 10-GE breakout interfaces and a QSFP+ transceiver module with the code of 0231A2E4 produced by INNOLIGHT is installed in the 40-GE interface, the interface cannot recognize the transceiver module, and it repeatedly goes up and down.

- Condition: This symptom occurs when the following procedure is performed:
  - Use the using tengige command to split the 40-GE interface into four 10-GE breakout interfaces.
  - Install a 40-GE QSFP+ transceiver module with the code of 0231A2E4 produced by INNOLIGHT in the 40-GE interface.

201406130208

- Symptom: The duration_sec value (which indicates the lifetime of a flow entry) in the flow removed message that the OpenFlow switch sends to the controller might be one second longer than the hard_timeout value set in the flow entry that the controller deploys.
- Condition: This symptom occurs when the following procedure is performed:
  - Deploy a flow entry configured with only hard_timeout.
  - View the duration_sec value in the flow removed message sent to the controller after the flow entry times out.

201409160439

- Symptom: When the software image is downloaded, **chassis** appears in the message that appears.
- Condition: This symptom occurs when the IRF software auto-update feature is used to download the software image.

201408260460

- Symptom: The entPhysicalVendorType value for an LR4 transceiver module obtained in MIB is incorrect.
- Condition: This symptom occurs when the following procedure is performed:
  - Install an LR4 transceiver module in a port of the switch.
  - Use the MIB browser tool to read the entPhysicalVendorType value for the port.

201409010368

- Symptom: When the switch receives a Hello message of an unknown Hello element type, the switch does not ignore the message as defined in the standard, and the switch returns an error message.
- Condition: This symptom occurs when the switch receives a Hello message of an unknown Hello element type in an OpenFlow network.

201311180209

- Symptom: The memory usage reaches the alarm threshold. The flow entries do not age out when traffic does exist in the network.
- Condition: This symptom occurs when plenty of flow entries configured with idle time are deployed.

201408250565

- Symptom: The system displays a message showing that "`System is busy or this command can't be executed because of no such privilege!`"
- Condition: This symptom occurs when you log in to the switch through SSH and issue commands in batches.

201407040500

- Symptom: The switch reboots unexpectedly or operates abnormally.
- Condition: This symptom occurs when the following conditions exist:
  - Portal authentication is enabled on interfaces of the switch.
  - Plenty of users access the external network through the switch.

201408060484

- Symptom: When two users sharing an account log in after passing Layer 3 portal authentication in the Web interface, the user that first logs in is logged out 12 minutes after the login.
- Condition: This symptom occurs when portal authentication is enabled and the two users are configured to use the same account on the IMC authentication server.

201407250412

- Symptom: The switch directly returns a hello packet received from a client, and then returns the hello packet of the server.
- Condition: This symptom occurs when NETCONF operations are performed for the switch through NETCONF over SSH and the client immediately sends a hello packet after the SSH connection is established.

201408220480

- 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.

201409240323

- Symptom: Long delay is detected when Vmotion is carried out, and **mac-address mac-move fast-update** does not help the problem.
- Condition: Vmotion is carried out on bridge aggregation.

Resolved problems in R2406P01

201407210092

- Symptom: A Telnet or SSH user fails to log in to the switch without any prompt information when the upper limit for Telnet or SSH users has been reached.
- Condition: This symptom can be seen if a Telnet or SSH user logs in to the switch when the upper limit for Telnet or SSH users has been reached.

201406230420

- Symptom: After an IRF fabric and a controller complete TCP handshake, the controller sends an OFP hello packet, but the IRF fabric returns a RST packet, resetting the TCP connection.
- Condition: This symptom can be seen if the following conditions exist:
  - The controller connects to an IRF subordinate switch.
  - Repeated **shutdown** and **undo shutdown** operations are performed on the port that connects to the controller.

201407150514

- Symptom: When dynamic link aggregation uses LACP to negotiate selected ports, it is not the device with the smallest device ID (containing the system LACP priority and the system MAC address) that determines the Selected ports.
- Condition: This symptom occurs when the following conditions exist:
  - The peer end of an aggregate link contains two devices. One of the two devices has a smaller device ID, which means a higher priority.
  - On the local end, the interface connecting to the higher-priority peer device has a greater index than the interface connecting to the lower-priority peer device.

201404250257

- Symptom: Some packets forwarded through an SPBM network get lost.
- Condition: This symptom can be seen if the following procedure is performed:
  - Configure graceful-restart on the SPBM network.
  - Execute the reset spbm database graceful-restart command or perform an SPBM active/standby switchover.

201407040601

- Symptom: An aggregate interface fails to forward TRILL traffic.
- Condition: This symptom can be seen if the following conditions exist:
  - Two RBs connected through Layer 2 Ethernet ports establish a neighbor relationship.
  - The ports between the two RBs are added to an aggregation group.

201408260578

- Symptom: CRC error packet statistics exist on the local 40GE port or the peer port.
- Condition: This symptom can be seen if the local 40GE port is installed with a QSFP+ transceiver module that supports a maximum transmit distance of 300 meters.

201407180277

- Symptom: An IRF fabric on a TRILL network splits.
- Condition: This symptom can be seen if the following conditions exist:
  - Rapidly enable and disable TRILL on a port.
  - A loop exists on the TRILL network, resulting TRILL loop storm.

201408140216

- Symptom: TRILL traffic is interrupted for up to 40 seconds.
- Condition: This symptom can be seen if the following conditions exist:
  - An RB with the highest DRB priority joins a broadcast network.
  - The new RB has the lowest MAC address among non-DRBs.
  - Two DRBs (the new RB and the original DRB) appoint AVFs for VLANs on the broadcast network.

201409010235

- Symptom: A switch takes a long time to start up.
- Condition: This symptom can be seen if the following procedure is performed:
  - Enable global STP or enable STP on a port.
  - Delete a dbm file.
  - Reboot the switch.

201408130356

- Symptom: The **port link-aggregation group** settings get lost on some member ports in an aggregation group after an IRF master/subordinate switchover.
- Condition: This symptom can be seen if the following procedure is performed:
  - Configure a multi-chassis link aggregation group on an IRF fabric.
  - Perform an IRF master/subordinate switchover.

201408080140

- Symptom: After a NETCONF <get-config> operation is performed to get the content of the data field, the system prompts "Unexpected element", which is unclear.

- Condition: This symptom can be seen after a NETCONF <get-config> operation is performed to get the content of the data field.

201407040588

- Symptom: The portal redirect function fails to direct the user to the portal authentication page.
- Condition: This symptom can be seen when a portal user accesses the network by using a browser.

201408060485

- Symptom: A portal user that first comes online is logged off after it has been online for 12 minutes.
- Condition: This symptom can be seen if the following conditions exist:
    - A user account configured on the IMC authentication server is used by two portal users.
    - The two portal users come online using the same user account.

201409060011

- Symptom: The output from the **display version** command executed on a TAA device does not show TAA information.
- Condition: This symptom can be seen if the **display version** command is executed on a TAA device.

201409010025

- Symptom: After the **restore factory-default** command is executed, the system prompts "The device might not support this operation. Please restore the factory default configuration manually."
- Condition: This symptom can be seen after the **restore factory-default** command is executed.

201408150284

- Symptom: The CLI might not respond for four minutes after the **reboot** command is executed.
- Condition: This symptom might be seen after the **reboot** command is executed.

201408200531/201408190278/201408190284

- Symptom: Some up 10GE ports split from a 40GE port might go down and up.
- Condition: This symptom can be seen if the 40GE port split into four 10GE ports is installed with a QSFP+ transceiver module and some 10GE ports are up.

201408190271

- Symptom: A 10GE or 40GE port installed with a transceiver module that is not connected to any fiber goes up and down, or is always up.
- Condition: This symptom can be seen if a 10GE or 40GE port is installed with a transceiver module that is not connected to any fiber.

201408130187

- Symptom: When the switch is configured with system LACP priority 0, a dynamic aggregation group on the switch chooses member ports with greater port IDs as Selected ports.
- Condition: This symptom might occur when the system LACP priority of the switch is set to 0.

201408190237

- Symptom: Using a MIB tool to get the manufacture date of a transceiver module on a port fails.
- Condition: This symptom can be seen if the following procedure is performed:
    - Install a transceiver module whose electric label contains manufacture date to a port.
    - Use a MIB tool to get the value of entPhysicalMfgDate on the port.

Resolved problems in R2406

201407180522

- Symptom: The output from the **display current-configuration** command does not show information about a VPLS PW configured using the **peer** command in VSI view. In addition, using the **save** command fails to save the VPLS PW configuration.
- Condition: This symptom can be seen after a VPLS PW is configured using the **peer** command in VSI view.

201406240010

- Symptom: The switch fails to perform local authentication for an administrator user (as configured) after remote HWTACACS authentication fails.
- Condition: This symptom can be seen if the switch cannot exchange packets with the remote HWTACACS server after they establish a TCP connection.

201407020210

- Symptom: If an STP edge port goes down and up, all MAC entries on the switch are deleted.
- Condition: This symptom can be seen if the following conditions exist:
    - STP is globally enabled.
    - An STP edge port goes down and up.

201407040601

- Symptom: If a TRILL port is added to an aggregation group, the switch fails to forward traffic due to miscalculation of multicast distribution trees.
- Condition: This symptom can be seen if the following conditions exist:
    - A TRILL port is in an aggregation group.
    - The TRILL neighbor of the port is the peer of the port's aggregation group.

201407080486

- Symptom: The **info-center loghost** command is configured on a switch to specify two or more log hosts by IP address. However, the specified log hosts cannot receive logs from the switch.
- Condition: This symptom can be seen if the following conditions exist:
    - The switch runs on Release 2405 and is restarted or a master/subordinate switchover is performed after the log host configuration is saved.
    - The switch runs on Release 2403 or earlier and is upgraded to Release 2405 after the log host configuration is saved.

201403290139

- Symptom: The system prompts insufficient ACL resources when the default command is executed on a port.
- Condition: This symptom can be seen if a VLAN interface is configured with packet-filter that contains large numbers of ACLs, some of which are not assigned due to shortage of ACL resources.

201405130409

- Symptom: The output from the ls or dir command shows incorrect file time.
- Condition: This symptom can be seen if SFTP or FTP is used to log in to the switch.

201406090639

- Symptom: IMC considers the deployment of a configuration file to a switch fails if the switch takes a long time to execute the configuration file.

- Condition: This symptom can be seen if a switch takes a long time to execute a configuration file assigned from IMC.

201406110412

- Symptom: The **display transceiver interface** command shows transceiver type exception information for a port.
- Condition: This symptom might be seen if the port is inserted with a 40GE QSFP+ transceiver module.

201407100333

- Symptom: The output from the debug qacl show acl-resc command shows incomplete information.
- Condition: This symptom can be seen if ACLs are configured on a Layer 3 Ethernet subinterface.

201406240602

- Symptom: The SSH server can use DSA to authenticate clients when the switch is in FIPS mode.
- Condition: This symptom can be seen if the SSH server uses RSA and then DSA to authenticate clients.

201407170071

- Symptom: An IRF fabric sends RSCN packets to the connected servers.
- Condition: This symptom can be seen if the following conditions exist:
  - Only the subordinate switch is configured with FCoE.
  - A master/subordinate switchover is performed.

201406070113

- Symptom: An SNMP walk on hh3cifMulSuppression MIB of an interface returns a value of 1 when the multicast-suppression pps 0 command has been configured on the interface.
- Condition: This symptom can be seen after an SNMP walk on hh3cifMulSuppression MIB of an interface where the multicast-suppression pps 0 command has been configured.

201407030128

- Symptom: An IRF member switch unexpectedly reboots due to handshake timeout.
- Condition: This symptom can be seen if the following conditions exist:
  - There is a layer 2 loop that comprises two or more IRF member switches.
  - Enable and disable TRILL on a port that has been configured with **qos trust dot1p**.

201407110459

- Symptom: After an IRF member switch is rebooted, it stays in loading state and cannot be rebooted at the CLI.
- Condition: This symptom can be seen if the IRF auto-update function is disabled on IRF member switches.

201407080145

- Symptom: Memory usage continually increases when users repeatedly log in to the switch through an AUX or VTY user line.
- Condition: This symptom can be seen if the following procedure is performed:
  - The **idle-timeout 0** command is configured on the user line.
  - Telnet, SSH, and FTP users repeatedly log in to the switch through the user line.

201407090176

- Symptom: After a switch completes software upgrade by using a python POAP script obtained through auto-configuration, it does not release the temporary IP address assigned by DHCP.
- Condition: This symptom can be seen if the reboot time in the python POAP script is earlier than the address release time.

201406170371

- Symptom: After an IRF member switch is rebooted, it continually reboots.
- Condition: This symptom can be seen if the following conditions exist:
  - HPE 6125XLG switches form an IRF fabric.
  - The **irf link-delay 0** command is configured.
  - An IRF member switch is rebooted.

201406090268

- Symptom: Flow control does not take effect when an Ethernet interface receives pause frames.
- Condition: This symptom can be seen when the following procedure is performed:
  - Restore a physical IRF port to a common Ethernet interface.
  - Enable flow control on the Ethernet interface by using the flow-control command.

201406160440

- Symptom: After a switch is rebooted, a VPN instance might fail to establish sessions to its BGP peers.
- Condition: This symptom might be seen if the following conditions exist:
  - BGP settings include IP addresses for the VPN instance but do not include any public IP addresses.
  - The global router ID is not configured and no router ID is configured for the VPN instance.
  - The configuration is saved and the switch is rebooted.

201406090115

- Symptom: After an IRF fabric is rebooted, the ports in a VLAN are up, but the corresponding VLAN interface cannot come up.
- Condition: This symptom might be seen if the following conditions exist:
  - The IRF fabric is connected to downstream devices through a multi-chassis Layer 2 aggregate interface.
  - The Layer 2 aggregate interface is a trunk port that permits more than 512 VLANs whose VLAN interfaces are created.

201403200509

- Symptom: A user who is authorized access permission to the interface feature cannot execute the mdix-mode and undo mdix-mode commands in interface view.
- Condition: This symptom occurs when the user executes the commands in the following conditions:
  - The user has user role rules that can access the **interface** feature.
  - The user does not have user role rules configured for the commands individually.

201404010200

- Symptom: RBAC fails to control a user's access to specific interfaces when the interface numbers specified in the user role resource access policies contain leading digits.

- Condition: This symptom occurs when the interface numbers specified in the user's user role resource access policies contain leading digits. For example, Ten-GigabitEthernet 02/0/1, Ten-GigabitEthernet 2/00/1, and Ten-GigabitEthernet 2/0/01 contain leading digit 0.

201406190088

- Symptom: CVE-2014-0224.
- Condition: This symptom can be seen when Open SSL Server is used.

201403200475

- Symptom: A user who has access permission to the **device** feature cannot execute the **password-recovery enable** or **undo password-recovery enable** command.
- Condition: This symptom occurs when the user executes the **password-recovery enable** and **undo password-recovery enable** commands in the following conditions:
  - The user has access permission to the **device** feature.
  - No permit command rule is configured for the commands.

201406040553

- Symptom: The output from the **display transceiver alarm** command sometimes does not show alarm information for a 40GE transceiver module. After the 40GE interface is split into four 10GE interfaces, the output shows RX signal loss, which should be RX loss of signal.
- Condition: This symptom can be seen when a 40GE fiber port is inserted with a 40GE transceiver module.

201406160009

- Symptom: When ARP packets are sent to the ingress port of an OpenFlow instance, twice as many ARP packets are received on the output port.
- Condition: This symptom can be seen if the following procedure is performed:
  - Create an OpenFlow instance that contains one ingress port and one output port.
  - Create a flow entry with the output port as All. Then the ingress port receives ARP packets.

201405260353

- Symptom: After a reboot, the system enables SNMP v3, which is not enabled in the configuration file.
- Condition: This symptom can be seen if the following procedure is performed:
  - Configure the SNMP version as v1 or v2c by using the snmp-agent sys-info version command.
  - Save the configuration.
  - Delete the .mdb file.
  - Reboot the switch.

201405120458

- Symptom: After a Layer 3 aggregate interface is deleted using the **undo interface route-aggregation** command, corresponding ACL resources might not be deleted.
- Condition: This symptom might be seen if the following procedure is performed:
  - A configuration rollback is performed to load a configuration file in which at least one Layer 3 aggregate interface has Layer 3 aggregate sub interfaces that reach the maximum number.
  - Use the undo interface route-aggregation command to delete such a Layer 3 aggregate interface.

201406090159

- Symptom: The switch cannot correctly identify a transceiver module.

- Condition: This symptom can be seen if the transceiver module is HPE 10GbE 100m SFP+ XCVR (PN#: H6Z42A) , specifically:
  - Vendor PN# 5697-2671.
  - Part labeled Made in CHINA.

201406110376

- Symptom: The system cannot display electronic label information for some SFP-GE modules.
- Condition: This symptom can be seen if the following procedure is performed:
  - Insert one of the following modules: JD113A, JD114A, JD115A, JD116A, JD109A, JD110A, JD111A, JD112A, JF829A, JF830A, and JF831A. The output from the display transceiver interface command does not display J# for these modules.
  - Execute the display transceiver manuinfo command to display transceiver manufacture information.

201406030245

- Symptom: Multicast data is cleared from hh3cIgmpSnoopingClearStats MIB.
- Condition: This symptom can be seen if the hh3cIgmpSnoopingClearStats is set to 1 when hh3cIgmpSnoopingStatsObjects has multicast data.

201405120011

- Symptom: An OpenFlow instance cannot forward incoming VRRP packets to the controller.
- Condition: This symptom can be seen if the following conditions exist:
  - Interfaces 1 and 2 are connected through a cable.
  - Interface 1 belongs to VLAN 1 where VRRP is enabled.
  - Interface 2 belongs to VLAN 2 that is configured as an OpenFlow VLAN.

201404300077

- Symptom: When an OpenFlow instance contains VLAN 1, tunneled traffic on the member ports of a service loopback group is discarded.
- Condition: This symptom can be seen when an OpenFlow instance contains VLAN 1.

201406170025

- Symptom: After the **undo shutdown** command is executed on a fiber port, the port takes a certain time to come up. Or displaying diagnostics/alarm information on the fiber port responds slowly.
- Condition: This symptom can be seen if the following conditions exist:
  - The fiber port connects to another device's fiber port.
  - The **shutdown** and **undo shutdown** commands are executed on the fiber port. Or the diagnostics/alarm information is displayed for the fiber port.

201406170371

- Symptom: When two 6125XLG switches form an IRF fabric through cross-link ports, the subordinate switch continually reboots.
- Condition: This symptom can be seen when two 6125XLG switches form an IRF fabric through cross-link ports.

201406200497

- Symptom: The switch has an exception or a watchdog reboot occurs upon receiving packets that match IRF packet type from a user port.
- Condition: This symptom can be seen when the switch receives packets that match IRF packet type from a user port.

201404300194

- Symptom: After an IRF master/subordinate switchover, MPLS TE settings in tunnel-policy fail to be restored.
- Condition: This symptom can be seen after an IRF master/subordinate switchover.

201405080449

- Symptom: An exception occurs to portal authentication, resulting in a system reboot.
- Condition: This symptom can be seen if one of the following conditions exists:
  - Users frequently come online and go offline.
  - Portal packets have multiple attributes.
  - Portal packets that have illegal attributes exist.
  - Press **CTRL+C** when the **display portal user** command is executed.

201406050329

- Symptom: The IRF port repeatedly goes up and down, resulting in repeated system reboots.
- Condition: This symptom can be seen if the following conditions exist:
  - Two 6125XLG switches form a chain IRF through a 40G cable.
  - An IRF master/subordinate switchover is performed.

201405230102

- Symptom: The **display power** command does not output any information.
- Condition: This symptom can be seen after the switch is started up.

201405060360

- Symptom: Settings on the AUX port of an HPE 6125XLG switch get lost.
- Condition: This symptom can be seen if the following conditions exist:
  - The **authentication-mode none** and **user-role network-admin** commands are configured on the AUX port.
  - Modify the slot number of the HPE 6125XLG switch, or use multiple HPE 6125XLG switch to form an IRF.

201405060344

- Symptom: The monitor-link state of an HPE 6125XLG switch is abnormal.
- Condition: This symptom can be seen if the following conditions exist:
  - The downstream port of the HPE 6125XLG switch is set to a monitor-link downstream port and connects to the 10G NIC of a blade server on c7000.
  - Remove and insert the blade server.

201403200271

- Symptom: Identical MAC entries exist on an IRF fabric.
- Condition: This symptom can be seen if the following conditions exist:
  - Multiple switches form the IRF fabric.
  - An aggregate S channel is created through EVB. MAC and VLAN are used to identify traffic.
  - An IRF master/subordinate switchover is performed.

201405160142

- Symptom: The CLI responds slowly on an HPE 6125XLG switch.
- Condition: This symptom can be seen if the following conditions exist:
  - The switch has a transceiver module inserted in a 40G port.

- Traffic is delivered to the CPU.

201404250050

- Symptom: An FCoE switch fails to communicate with the connected server's NIC.
- Condition: This symptom can be seen if the NIC continuously sends two FDISC packets.

201404140465

- Symptom: After a reboot, the four 10GE ports split from a 40GE QSFP+ port might fail to identify the transceiver module.
- Condition: This symptom can be seen if the following procedure is performed:
  - Insert a transceiver module into a 40GE QSFP+ port.
  - Split the 40GE QSFP+ port into four 10GE ports.
  - Reboot the switch.

201405120151

- Symptom: The sequence number of a transceiver module obtained from IMC is incorrect.
- Condition: This symptom can be seen when you use IMC to view the sequence number of a transceiver module.

201405140359/201405120461

- Symptom: After a member port is added to an aggregation interface, the member port might fail to forward multicast traffic.
- Condition: This symptom might be seen after a member port is added to an aggregation interface that acts as an egress port for multicast forwarding.

201405140076

- Symptom: The output from the **display diagnostic-information** command is incomplete.
- Condition: This symptom can be seen in the output from the **display diagnostic-information** command.

201405060082

- Symptom: A walk on hh3cevtPortSw-SFP-8GFC-SW or hh3cevtPortSw-SFP-8GFC-LW MIB returns incorrect information.
- Condition: This symptom can be seen during a walk on hh3cevtPortSw-SFP-8GFC-SW or hh3cevtPortSw-SFP-8GFC-LW MIB.

201312260147

- 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.

201404090038

- Symptom: A walk on a 10G copper port's LswportType MIB returns incorrect information.
- Condition: This symptom can be seen during a walk on a 10G copper port's LswportType MIB.

201405080391

- Symptom: The CPU usage of an IRF fabric increases, delaying access from other devices to the IRF fabric.
- Condition: This symptom can be seen if the following conditions exist:
  - Multiple IRF member switches send packets that have the same 5-tuple at the same time.

- The sent packets match ECMP routing, and all egress ports are Layer 3 ports.
- Each slot has at least one egress port.

201405150545

- Symptom: The switch might fail to forward TRILL broadcast traffic.
- Condition: This symptom might be seen if the following conditions exist:
  - A TRILL access port's link type is set to trunk and it permits multiple VLANs.
  - Repeated **shutdown** and **undo shutdown** operations are performed on another TRILL trunk port.

201405140297

- Symptom: IGMP snooping entries cannot be established for TRILL, resulting in multicast forwarding failure.
- Condition: This symptom can be seen if the following procedure is performed:
  - A port enabled with TRILL is added to a multicast entry.
  - The VLAN enabled with IGMP snooping is configured with **igmp-snooping drop-unknown**.
  - The **reset trill** command is repeatedly executed.

201405120392

- Symptom: After the **broadcast-suppression**, **multicast-suppression**, or **unicast-suppression** command (that sets a non-zero percent or kbps value) is executed, the system prompts that the command does not take effect.
- Condition: This symptom can be seen if the following procedure is performed:
  - Use the broadcast-suppression, multicast-suppression, or unicast-suppression command to set a pps value of 0, and then restore the default.
  - Use the broadcast-suppression, multicast-suppression, or unicast-suppression command to set a percent or kbps value of 0.
  - Use a different command to set a non-zero percent or kbps value. For example, if the previous step uses broadcast-suppression, this step uses multicast-suppression or unicast-suppression.

201404280244

- Symptom: The switch fails to forward OpenFlow traffic.
- Condition: This symptom can be seen during batch assignment of flow entries.

201405140158

- Symptom: The **dis evb summary** command displays incorrect information.
- Condition: This symptom can be seen if the **dis evb summary** command is executed when the S channel of a VSI (not the last one) is being deleted.

201406050920

- Symptom: A walk on snmpIfInDiscards MIB returns statistics for pause frames.
- Condition: This symptom can be seen if the port is configured with **flow-control** or **flow-control receive enable**, and received pause frames.

201312310451

- Symptom: The OSPF neighbor relationship between two IRF fabrics goes down.
- Condition: This symptom can be seen if the following conditions exist:
  - The two IRF fabrics are connected through an aggregate link.
  - An MSTP instance-to-VLAN mapping is configured on both ends of the aggregate link.

201401220221

- Symptom: The MAC address moving suppression function does not take effect in an IRF fabric.
- Condition: This symptom occurs when the two member devices of the IRF fabric successively receive broadcast traffic with the same source MAC address.

201402250548

- Symptom: The VLAN interface of a primary VLAN cannot forward traffic at Layer 3.
- Condition: This symptom occurs when the following procedure is performed:
  a. Configure a private VLAN.
  b. Bind the VLAN interface of the primary VLAN to a VPN instance.
  c. Remove the binding.

201403120408

- Symptom: When all nodes are logged out, the output from the **display fip-snooping rules enode** command shows that no ENode FIP snooping rules exist. However, the output from the **display qos-acl resource** command shows that the number of ACL rules used is more than that in the initial state.
- Condition: This symptom occurs when the following conditions exist:
  - The switch is operating in Transit mode.
  - A large number of nodes are logged in and logged out repeatedly.
  - The following tasks are repeatedly performed on the switch:
    - Shutting down and bringing up ports.
    - Adding and deleting VLANs.
    - Assigning ports to and removing ports from VLANs.

201403190173

- Symptom: In the output from the **display qos-acl resource** command, the VFP ACL or IFP ACL usage might exceed 100%.
- Condition: This symptom might occur when the following procedure is performed:
  - Use the system-working-mode command to configure the system working mode as advanced.
  - Configure the private VLAN feature.
  - Configure local QoS ID marking actions or flow-based VLAN marking actions in QoS policies to occupy all VFP resources, or configure QoS policies or packet filtering to occupy all IFP resources.

201404280257

- Symptom: Some OpenFlow flow tables might fail to forward traffic.
- Condition: This symptom might occur when a large number of OpenFlow flow tables are deployed in batch.

201403240344

- Symptom: The switch fails to forward traffic for multiple multicast groups.
- Condition: This symptom occurs when the switch has large numbers of multicast forwarding entries.

201403270410

- Symptom: After a VLAN interface is shutdown, the multicast forwarding entries that use the VLAN interface are not deleted.

- Condition: This symptom occurs if the VLAN of the shutdown VLAN interface contains a multicast member port that is also a member port of an aggregation group.

201403240159

- Symptom: The MAC addresses learned by UNI ports involved in many-to-one VLAN mapping cannot be displayed on a per-port basis.
- Condition: This symptom occurs when the **display mac-address interface** command is used to display the MAC addresses learned by an UNI port involved in many-to-one VLAN mapping.

201403250492

- Symptom: If static bindings are configured by using the **ip source bind** or **ipv6 source bind** command in Layer 2 Ethernet port view when ACL resources are insufficient, the system does not provide prompt information. The output from the **display current-configuration** command in system view or the **display this** command in port view shows the configured static bindings.
- Condition: This symptom occurs if static bindings are configured by using the **ip source bind** or **ipv6 source bind** command in Layer 2 Ethernet port view when ACL resources are insufficient.

201403130262

- Symptom: A host fails to ping its gateway, although the MAC address of the gateway can be obtained through ARP.
- Condition: This symptom occurs if the following procedure is performed:
  - Configure a private VLAN and its secondary VLAN.
  - Bind a VPN instance to the VLAN interface of the private VLAN, and configure private VLAN-secondary VLAN mapping.

201402270049

- Symptom: An IRF member switch stops running during startup.
- Condition: This symptom occurs if continual IRF master/subordinate switchovers and reboots are performed.

201403200085

- Symptom: After the switch has run a scheduled task, the system log shows that the IRF port fails to receive IRF packets from the neighbor. A system reboot might occur.
- Condition: This symptom might occur when the following conditions exist:
  - IRF continually processes traffic.
  - The scheduled task executes the **display diagnostic-information** command.

201401170243

- Symptom: When the link mode is changed in interface range view, the link mode configuration fails, and the system exits the interface range view.
- Condition: This symptom occurs when the following procedure is performed:
  - Use the interface range interface-list command to enter interface range view.
  - Change the link mode in interface range view.

201401170113

- Symptom: After a master/subordinate switchover occurs to an IRF fabric, packets that match the static IPv6 routes deployed by an OpenFlow controller cannot be correctly forwarded.
- Condition: This symptom might occur when the following procedure is performed:
  - Configure OpenFlow, and deploy IPv6 static routes and the corresponding ND entries.
  - Perform a master/subordinate switchover for the IRF fabric.

201404080286

- Symptom: The **display ospfv3 peer** command fails to be executed in FIPS mode.
- Condition: This symptom occurs if the **display ospfv3 peer** command is executed in FIPS mode.

201403010153

- Symptom: The effective value of the port status detection timer is 5 seconds greater than the configured value.
- Condition: This symptom might occur when the following conditions exist:
  - The port status detection timer is configured.
  - Ports are shut down by STP or DLDP.

201312270486

- Symptom: In an IRF fabric, the dynamic flow table ages out after 60 seconds, and then traffic cannot be forwarded.
- Condition: This symptom might occur when the following conditions exist:
  - In an IRF fabric, an OpenFlow port is a multichassis aggregate interface.
  - The packet count is -- (which means that the packet count is not collected) in the flow table deployed.
  - Some of the aggregation group member ports receive traffic.

201403130400

- Symptom: If a process unexpectedly quits and a core file is generated, the switch unexpectedly reboots.
- Condition: This symptom occurs if a process unexpectedly quits and a core file is generated.

201403120423

- Symptom: The CPU usage of the FCSD process is higher than expected.
- Condition: This symptom occurs after the switch is started.

201403120229

- Symptom: The ports on a disk device are down.
- Condition: This symptom occurs when a disk device is connected to an FCoE-capable switch through a Nexus 5000 switch.

201403120101

- Symptom: The output from the **display port-security mac-address security** command shows that the remaining lifetime of some secure MAC addresses is 2 minutes when the aging timer for secure MAC addresses is set to 2 minutes by using the **port-security timer autolearn aging** command.
- Condition: This symptom occurs when the aging timer for secure MAC addresses is set to 2 minutes in autolearn mode by using the **port-security timer autolearn aging** command.

201403240356

- Symptom: The PTP interface information displayed on an IRF fabric that comprises two switches shows that time is not synchronized.
- Condition: This symptom can be seen when PTP is configured on an IRF fabric that comprises two switches.

201401020078

- Symptom: A HPE 6125XLG switch sends a corrupted HTTP packet to IMC. IMC fails to detect that a VSI went offline.

- Condition: This symptom occurs when the following procedure is performed:
    - Bind the NIC of a VM to a dvportgroup on VMware vCenter. The VSI for the VM comes online.
    - Configure the VM to log off the VSI.
    - Configure the debugging evb event command on the switch.

201404010472

- Symptom: A switch in a PBB network fails to forward traffic that matches **encapsulation-default** over the downstream port. The **shutdown** and **undo shutdown** command must be executed on the port to bring it up.
- Condition: This symptom occurs if TRILL is enabled and then disabled on the downstream port.

201403310220

- Symptom: When VFC interface A is bound to a Layer 2 aggregate interface, VFC interface A goes down. Then, when VFC interface B is bound to the Layer 2 aggregate interface, VFC interface B goes up, but VFC interface A is still down.
- Condition: This symptom might occur when the following procedure is performed:
    - Bind VFC interfaces A and B to an Ethernet interface Port 1.
    - Create a Layer 2 aggregate interface, and assign Port 1 to the Layer 2 aggregate interface.

201403200111

- Symptom: Aggregation group member ports in Individual state might not learn MAC addresses, even after they leave the aggregation group.
- Condition: This symptom might occur when the following procedure is performed:
    - Configure the aggregate interface as an edge aggregate interface.
    - Configure the edge aggregate interface to operate in dynamic mode, and then configure it to operate in static mode.

201311050110

- Symptom: SPBM cannot perform optimal path selection based on link costs because the costs calculated by SPBM for all interfaces (including 1G, 10G, and aggregate interfaces) are 1.
- Condition: This symptom occurs when SPBM automatically calculates link costs.

201403180423

- Symptom: The TRILL link cost for an aggregate interface is the automatically calculated link cost when automatic link cost calculation is disabled for TRILL ports.
- Condition: This symptom might occur when the following procedure is performed:
    - Use the auto-cost enable command to enable automatic link cost calculation for TRILL ports. In this example, the automatically calculated link cost is 666.
    - Use the undo auto-cost enable command to disable automatic link cost calculation for TRILL ports. Then, the link cost is restored to 2000 for TRILL ports.
    - Use the shutdown command and then the undo shutdown command to re-enable the aggregate interface. Unexpectedly, the link cost for the aggregate interface becomes 666.

201404040543

- Symptom: On switches of some models, the 10-GE fiber ports can stay up only after they go down and come up multiple times, or the 10-GE fiber ports cannot go up.
- Condition: This symptom occurs when 1000-Mbps copper transceiver modules are installed in 10-GE fiber ports.

201404250221

- Symptom: The CPU usage seriously increases when an aggregation group member port is repeatedly shut down and brought up.
- Condition: This symptom occurs when an aggregation group member port is repeatedly shut down and brought up and its state changes between Selected and Unselected.

201208210014

- Symptom: A 40-GE interface without an external PHY might fail to go up.
- Condition: This symptom might occur when the following procedure is performed:
  - Connect a cable to a 40-GE interface without an external PHY.
  - Reboot the switch or use the shutdown command and then the undo shutdown command on the interface.

201404110133

- Symptom: A grammatical error exists in the following error message:

  "Do you want to change the system working mode? [Y/N]:y

  Failed to set the system working mode, please tocheck hard resource. ”
- Condition: This symptom occurs when the following procedure is performed:
  - When the system working mode is standard, configure ACLs to reach the maximum number of ACLs allowed.
  - Use the system-working-mode advance command to configure the system working mode as advanced.

201403140267

- Symptom: After a rule that denies ICMP and TCP packets is applied to switch through a QoS policy, ICMP and TCP packets can still pass through.
- Condition: This symptom occurs when a rule that denies ICMP and TCP packets is applied to the incoming traffic of a port through a QoS policy.

201403120389

- Symptom: When the **display fcs database** command to display the FCS database information, the **Attached port wwns** displayed for a VFC interface are incorrect.
- Condition: This symptom might occur when the following procedure is performed:
  - Assign the VFC interface to multiple VSANs as trunk ports.
  - Log in one node to the VFC interface in each VSAN. Log in multiple nodes to the VFC interfaces simultaneously.

201403120360

- Symptom: When the members in the default zone are denied from accessing each other, displaying the active zone set information will cause a memory leakage.
- Condition: This symptom might occur when the following procedure is performed:
  - Configure and activate a zone set in a VSAN.
  - Use the undo zone default-zone permit command to deny members in the default zone from accessing each other in the VSAN when logged-in nodes exist in the default zone.
  - User the display zoneset active command to display information about the active zone set.

201405040350

- Symptom: The switch reboots unexpectedly.
- Condition: This symptom occurs when the QoS configurations are frequently, dynamically modified for the QoS policies applied to the switch.

201403260176

- Symptom: When an aggregate interface is in down state, the output from the **display interface** command still shows packet statistics for that interface.
- Condition: This symptom can be seen when the following conditions exist:
  - Physical connections exist between the aggregate interface and a terminal.
  - The member ports of the aggregate interface are in Individual state.

201403290121

- Symptom: Downloading a large file through FTP fails.
- Condition: This symptom occurs if the FTP download operation is performed in Python shell view by executing the **transfer** command.

201403060184

- Symptom: When the loop detection feature detects a loop on a port, the port cannot automatically go up after the port status detection interval configured by using the **shutdown-interval** command.
- Condition: This symptom might occur when the following procedure is performed:
  - Use the loopback-detection action shutdown command to configure the loop protection action as shutdown.
  - Use the shutdown-interval command to configure the port status detection interval.

LSV7D007841

- Symptom: After an unexpectedly reboot, the system does not record anomaly information for the reboot. The output from the **display version** command shows "Watchdog timeout reboot."
- Condition: This symptom can be seen after an unexpectedly reboot.

201312180312

- Symptom: The disk device that connects to a subordinate device cannot be registered.
- Condition: This symptom occurs when the following conditions exist:
  - An IRF fabric acts as an FCF switch.
  - The domain ID is modified for the IRF fabric.

201405120151

- Symptom: The serial number that IMC reads from a transceiver module is incorrect.
- Condition: This symptom occurs when IMC reads the serial number of a transceiver module.

201403210223

- Symptom: The **stp global enable** or **undo stp global enable** command takes effect several minutes after the command is executed.
- Condition: This symptom occurs when the spanning tree protocol mode is PVST.

201403240117

- Symptom: VFC interfaces go down unexpectedly.
- Condition: This symptom occurs when MST regions are deleted and then MSTIs are configured in an FCoE network.

201403270570

- Symptom: The system prompts "unsuccessfully" when MAC entries are added or deleted on an EVB S-channel aggregate interface.
- Condition: This symptom occurs when MAC entries are added or deleted on an EVB S-channel aggregate interface.

201403260407

- Symptom: Disabling MAC address learning for B-VLAN fails.
- Condition: This symptom occurs if the following procedure is performed:
  - Enable SPBM and configure B-VLAN.
  - Disable MAC address learning for B-VLAN.
  - Disable SPBM.

201402210125

- Symptom: ACLs can be successfully deployed to a switch when the ACL resource usage is 100%.
- Condition: This symptom might occur when the following procedure is performed:
  - Deploy ACLs to a port of the switch to make the ACL usage reach 100%.
  - Deploy ACLs to another port of the switch.

201405050496

- Symptom: The **display transceiver interface** command might fail to display the information about an FC transceiver module.
- Condition: This symptom might occur when the following procedure is performed:
  - Install an FC transceiver module in an interface.
  - Execute the display transceiver interface command on the switch.

201403120404

- Symptom: Soft zoning stays enabled, and hard zoning is not enabled even when the hardware resources are sufficient.
- Condition: This symptom might occur when the following procedure is performed:
  - After FCoE links are successfully configured, configure ACLs to occupy all ACL resources.
  - Use the undo zone default-zone permit command to deny members in the default zone from accessing each other for effective VLANs. In this case, soft zoning is enabled.
  - Release ACL resources.

201403120385

- Symptom: The downlink interfaces of an NPV switch take a long time to detect the physical state changes (up or down) of the uplink interface.
- Condition: This symptom might occur when the following procedure is performed:
  - Configure a large number of VSANs and VFC interfaces in the FCoE fabric.
  - Shut down an uplink interface of the NPV switch.
  - Bring up the uplink interface.

201404170112

- Symptom: The console port stops responding and the switch reboots during a walk on ARP MIB.
- Condition: This symptom occurs when the following conditions exist:
  - More than 5000 ARP entries exist.
  - A walk on 1.3.6.1.2.1.3.1.1.3 ARP MIB is performed, and at the same time, the **reset arp all** command is executed.

201403190452

- Symptom: After a VRID is deleted, the configuration is saved, and the switch is rebooted, the output from the **display vrrp** command shows the VRID still exists.

- Condition: This symptom can be seen after the following procedure is performed:
    - Execute the undo vrrp vrid virtual-router-id [virtual-ip [virtual-address]] or undo vrrp vrid virtual-router-id track [track-entry-number] command.
    - Save the configuration and reboot the switch.

201405150314

- Symptom: When you log in to the switch through a console port, the CLI might be stuck when you enter commands at the CLI.
- Condition: This symptom might occur when a custom transceiver module is installed in an interface that can be split into four breakout interfaces and does not have an external PHY.

201403210219

- Symptom: When the function of discarding unknown multicast packets is enabled for a VLAN in a TRILL+IGMP snooping scenario, unknown multicast packets in the VLAN are not discarded.
- Condition: This symptom occurs when the function of discarding unknown multicast packets is enabled for a VLAN in a TRILL+IGMP snooping scenario.

201403240370

- Symptom: Layer 2 traffic in a TRILL network fails to be forwarded between two RBs.
- Condition: This symptom occurs when the following conditions exist:
    - One RB acts as the AVF, and the other RB acts as a non-AVF. The two RBs connect through TRILL access ports.
    - The access ports on the AVF and the non-AVF are configured as TRILL trunk ports.

201404010465

- Symptom: The SFTP client on Switch B fails to download a file from Switch A after the SFTP client on Switch A downloads that file from a Linux server.
- Condition: This symptom can be seen when the SFTP client on Switch B downloads a file from Switch A after the SFTP client on Switch A downloads that file from a Linux server.

201403260454

- Symptom: The keyword STRING appears after the **save** command.
- Condition: This symptom can be seen if TAB is pressed multiple times after the **save** command is input.

201403180283

- Symptom: OpenFlow fails to deploy MAC address entries to overwrite existing multiport unicast MAC address entries.
- Condition: This symptom occurs when the following procedure is performed:
    - Configure multiport unicast MAC address entries.
    - Configure OpenFlow to deploy MAC address entries to overwrite these multiport unicast MAC address entries.

201403240270

- Symptom: A non-administrator user can bypass RBAC check and use unauthorized functions and resources.
- Condition: This symptom occurs if the user performs the following procedure:
    - Upload a new configuration file that contains the rights for managing the functions and resources.
    - Set the configuration file as the next startup configuration file.
    - Reboot the switch.

201404040471

- Symptom: Device will tear down TCP connection in established state when receives wrong TCP packet.
- Condition: Only for those TCP connections in established state. When they receive TCP SYN packet which is carrying a sequence number falling into the connection receiving window, a RST packet will be sent and the connection will be dropped immediately.

201403210195

- Symptom: After the configurations occupying ACL resources are canceled, the output from the **display qos-acl resource** command shows that some ACL resources are not retrieved.
- Condition: This symptom occurs when the following procedure is performed:
  - Configure private VLAN and IGMP snooping on the switch.
  - Configure private VLAN to occupy all ACL resources.
  - Repeatedly configure and cancel the private VLAN configuration.
  - Cancel the private VLAN and IGMP snooping configuration on the switch.

201404010188

- Symptom: EVB fails to be enabled on a port.
- Condition: This symptom occurs if the following procedure is performed:
  - Enable and then disable TRILL on a port.
  - Enable EVB on the port.

201404150058

- Symptom: When the **zone default-zone permit** command is not configured on a switch, the attached nodes in the default zone can access each other.
- Condition: This symptom occurs when the following procedure is performed:
  - Enable FCoE on the switch.
  - Attach ENode 1 and ENode 2 in the same VSAN to the switch.

201404080316

- Symptom: When an attached node that has not been logged in sends an FKA packet to a switch, the switch does not respond with an FIP Clear Virtual Links packet.
- Condition: This symptom occurs when the following procedure is performed:
  - Enable FCoE on the switch.
  - An attached node that has not been logged in sends an FKA packet to the switch.

201401270147

- Symptom: Zone distribution cannot be completed.
- Condition: This symptom occurs when a large number of zones and zones sets are configured and zone distribution is triggered.

201403210200

- Symptom: The switch ignores the cases of VRF names.
- Condition: This symptom occurs when the **controller address** command is used to specify a controller by its IP address and specify a VRF by its name for the controller.

201311190312

- Symptom: The broadcast storm suppression threshold and the multicast storm suppression threshold are configured as 0 in an IRF fabric. After the IRF fabric is rebooted, these storm suppression configurations do not take effect.

- Condition: This symptom occurs when the following procedure is performed:
    - In an IRF fabric, use the broadcast-suppression and multicast-suppression command in Ethernet interface view to configure the broadcast storm suppression threshold and the multicast storm suppression threshold as 0.
    - Reboot the IRF fabric.

201404220072

- Symptom: The rate-limit parameter deployed by OpenFlow is different from that displayed on the switch.
- Condition: This symptom occurs when the following procedure is performed:
    - On the controller, configure the rate-limit parameter burst size.
    - Use the display openflow instance command on the switch to display the OpenFlow configuration.

201312120164

- Symptom: After a user goes offline from a port and then comes online through another port, the output from the **display ip source binding** command still shows the IP source guard binding created for the user at the first time.
- Condition: This symptom occurs if the following procedure is performed:
    - The user comes online through a port, and obtains an IP address from the DHCP server.
    - The switch creates an IP source guard binding for the user.
    - The user abnormally goes offline and then comes online through another port.
    - The user normally goes offline.

201311290366

- Symptom: The auto-configuration result information shows that the switch successfully obtained a configuration file, although the switch actually failed to obtain that configuration file.
- Condition: This symptom can be seen if the following conditions exist:
    - The switch connects to a DHCP server on another switch. The configuration file path specified on the DHCP server is valid but it does not contain any configuration file.
    - The switch starts up without loading any configuration file.

201312040262

- Symptom: A Layer 3 interface on an IRF subordinate switch does not learn ARP entries and IPCIM entries get lost on the switch.
- Condition: This symptom occurs when the following conditions exist:
    - The Layer 3 interface on the IRF subordinate switch connects to a DHCP server.
    - The IRF subordinate switch is rebooted.

201312170465

- Symptom: When the SCP client on the switch uploads a file that does not exist to a remote SCP server, the system shows that the upload operation is successful.
- Condition: This symptom can be seen when the SCP client on the switch uploads a file that does not exist to a remote SCP server.

201312060432

- Symptom: The many-to-one VLAN mapping configuration does not take effect.
- Condition: This symptom occurs when the following procedure is performed:
    - Use two switches to form an IRF fabric.

- Configure the dhcp snooping binding record command and configure many-to-one VLAN mapping on a port of IRF member switch 1.
- Reboot IRF member switch 2.

201403070417

- Symptom: A switch running Comware v5 can get a file from a switch running Comware v7 by executing an SCP command. The switch running Comware v7 cannot put a file to the switch running Comware v5 through an SCP command.
- Condition: This symptom can be seen between a switch running Comware v5 and a switch running Comware v7.

201312260147

- Symptom: A DHCP client takes a very long time to complete address acquisition from the DHCP server on the switch.
- Condition: This symptom occurs if the DHCP request from the DHCP client contains an IP address that is not on the same network as the IP address of the DHCP server's receiving interface.

201310220394

- Symptom: After FCoE mode is changed to none, FIP snooping driver entries still exist, and FCoE mode is still FCF mode.
- Condition: This symptom can be seen if the following procedure is performed:
  - Create 100 VFC interfaces and bind them to the same Layer 2 aggregate interface on an FCF switch.
  - 100 nodes log in through the 100 VFC interfaces.
  - Create static routes that reach the software specification. Some static routes are in inactive state because of exceeding the driver specification.
  - Bind another VFC interface to a member port of the Layer 2 aggregate interface.
  - Change FCoE mode to none.

201401060010

- Symptom: After more than 10 non-contiguous VSANs are configured using the **port trunk vsan** command on a VFC interface, the output from the **display current-configuration** command shows that the VSANs configurations failed.
- Condition: This symptom can be seen after more than 10 non-contiguous VSANs are configured using the **port trunk vsan** command on a VFC interface.

201403060232

- Symptom: Assigning QoS policies in batches to virtual nodes from IMC fails.
- Condition: This symptom can be seen when you use IMC to batch assign QoS policies to virtual nodes.

201311050393

- Symptom: The output from the **display spbm multicast-fib** command has a redundant space.
- Condition: This symptom can be seen in the output from the **display spbm multicast-fib** command.

201405190183

- Symptom: An IRF fabric that comprises an HPE 6125XLG switch fails to be created.
- Condition: This symptom occurs if the two switches are connected through a 40G cable, and then the 40G cable is replaced with QSFP+ modules and a fiber cable.

201403070232

- Symptom: A port in MDIX mode can go up when it connects to a peer port in MDIX mode. A port in MDI mode cannot go up when it connects to a peer port in MDIX mode. The mode of a port that is up cannot be changed using the **mdix-mode** command.
- Condition: This symptom can be seen when you use the **mdix-mode** command to switch the mode of an Ethernet port between MDIX and MDI.

201402250494

- Symptom: A Layer 2 ACL for matching outbound LSAP packets on an interface actually matches all packets.
- Condition: This symptom can be seen when a Layer 2 ACL for matching outbound LSAP packets is applied to an interface.

201403030079

- Symptom: When a QoS policy fails to be assigned using the **qos policy** command, the prompt information is incorrect.
- Condition: This symptom can be seen when a QoS policy fails to be assigned using the **qos policy** command.

Resolved problems in R2403

SSH with TACACS

- Symptom: When logging into the switch using SSH with TACACS remote authentication, after the user passes authentication, the system may display "login: unrecognized option `--level'" and log the user off.
- Condition: Cannot log into the switch using SSH with TACACS remote authentication

Bootware output on OA port

- Symptom: Bootware output did not appear when connected to the switch via OA serial port connection
- Condition: Cannot see boot output on console during switch startup when connected through OA.

File deletion failure

- Symptom: Attempting to delete files in the flash directory may fail with the message “permission denied” when files are downloaded from a system where they were stored with insufficient permissions.
- Condition: Files downloaded to flash sometimes could not be deleted.

201401200047

- Symptom: When you log in to a switch through an AUX port, you are directly led into user view. However, no prompt is displayed.
- Condition: This symptom occurs when you log in to the switch through an AUX port.

201402070236

- Symptom: The result of walking the entPhysicalName node is incorrect.
- Condition: This symptom occurs when you use the MIB browser to walk the entPhysicalName node on the switch.

201401150494

- Symptom: The output from the display buffer usage command is incorrect.

- Condition: This symptom occurs when you use the display buffer usage command after configuring the burst-mode by using the **burst-mode enable** or **undo burst-mode enable** command.

201401200303

- Symptom: The device returns an error message with the OFPET_FLOW_MOD_FAILED type and the OFPFMFC_UNKNOWN code.
- Condition: This symptom occurs when the following conditions exist:
  - The switch is enabled with OpenFlow.
  - The controller sends a FlowMod(ADD/goto Group) entry after sending a GroupMod(MODIFY) entry to the switch.

201401150404

- Symptom: Device fails to re-authenticate with the Windows 2003 RADIUS Server.
- Condition: This symptom occurs when the following conditions exist:
  - Device connects to the Windows 2003 RADIUS Server for authentication.
  - Device initiates an authentication again after the re-auth period.

201312250142

- Symptom: When EVB is configured in an IRF fabric, a VSI aggregate interface goes down and then goes up.
- Condition: This symptom occurs if a master/subordinate switchover occurs when the VSI aggregate interface is up.

201312300276

- Symptom: A legal transceiver module is identified as an illegal one.
- Condition: This symptom occurs when you insert a legal SFP transceiver module into the switch.

201401140101

- Symptom: When you use the **undo ip address dhcp-alloc** command to release the IP address of a switch acting as a DHCP client, the switch might fail to send a DHCP-RELEASE packet.
- Condition: This symptom occurs when the following conditions exist:
  - The switch acts as a DHCP client, and obtains dynamically assigned IP addresses.
  - After the switch obtains an IP address, the **undo ip address dhcp-alloc** command is used to release the obtained IP address on the interface where the DHCP client resides.

201401220208

- Symptom: An error prompt appears when you configure an IPv4 portal authentication source subnet.
- Condition: This symptom occurs when you use the **portal layer3 source** command to configure the IPv4 portal authentication source subnet as 0.0.0.0 255.255.255.0.

201401220382

- Symptom: The switch might fail to upload or download files.
- Condition: This symptom might occur when the following procedure is performed:
  a. Configure the switch as an FTP client.
  b. Use the **get** or **put** command to download or upload files multiple times.

201312300294

- Symptom: The FTP service is unexpectedly disabled on a switch.

- Condition: The symptom occurs when you use FTP to exchange files between the switch and another switch multiple times.

201312170314

- Symptom: When you use the **display link-aggregation verbose bridge-aggregation** *interface-number* command to display aggregate interface information, the state of an aggregation group member port is incorrectly displayed.
- Condition: This symptom occurs when the following conditions exist:
  - Layer 2 aggregate interfaces are created at both ends of a link.
  - The number of member ports at each end exceeds the maximum number of Selected ports allowed.

201401270240

- Symptom: When you upgrade the software through the Boot ROM menu, the software image file might fail to be loaded.
- Condition: This symptom might occur when you upgrade the software through the Boot ROM menu.

201401150527

- Symptom: When the VM of a VSI interface is migrated from an aggregate interface to another aggregate interface of a switch, the VSI interface frequently goes up and down, and the VM cannot successfully log in.
- Condition: This symptom occurs when the following procedure is performed:
  - **a.** Enable EVB on the target aggregate interface.
  - **b.** Migrate the VM of the VSI interface from an aggregate interface to the target aggregate interface.
  - **c.** Disable and then enable EVB on the target aggregate interface.

201402170152

- Symptom: The switch does not reboot as configured in the **scheduler reboot at** or **scheduler reboot delay** command.
- Condition: This symptom occurs when you use the **scheduler reboot at** or **scheduler reboot delay** command in user view.

201401100305

- Symptom: When the switch is an OpenFlow switch, it cannot communicate with an IXIA controller running the IXIA ANVL test suite.
- Condition: This symptom occurs when the following conditions exist:
  - The switch acts an OpenFlow switch.
  - The IXIA test device acts as a controller.
  - The IXIA test device runs the IXIA ANVL test suite.

201402170350

- Symptom: The number of VLANs supported for PVST on a switch is less than that defined in specifications.
- Condition: This symptom occurs when the following procedure is performed:
  - **a.** Enable the spanning tree protocol globally.
  - **b.** Configure the spanning tree protocol to operate in MSTP mode.
  - **c.** Disable the spanning tree protocol globally.
  - **d.** Configure the spanning tree protocol to operate in PVST mode.
  - **e.** Enable the spanning tree protocol globally.

201402170013

- Symptom: The console port of a switch might fail to respond to Telnet operations.
- Condition: This symptom might occur when you frequently operate the switch through Telnet and the console port.

201402080060

- Symptom: On a switch with both MAC-IP flow entries and extensibility flow entries, after a packet is matched against MAC-IP flow entries, the packet matches the table-miss flow entry and is sent to the controller, rather than matched against an extensibility flow entry with the metadata configured.
- Condition: This symptom occurs when the following conditions exist:
  - Configure MAC-IP flow tables and extensibility flow tables.
  - Use a controller to deploy a flow entry to an extensibility flow table on the switch. The match fields of the flow entry contain metadata 0x01.

201401260259

- Symptom: On a switch, packets that do not match the highest-priority flow entry temporarily match the flow entry.
- Condition: This symptom occurs when you use an OpenFlow controller to deploy multiple flow entries to the switch.

201311260144

- Symptom: The iNode authentication failure reasons are not prompted.
- Condition: This symptom occurs when the following procedure is performed:
  a. Enable 802.1X globally and in port view.
  b. Enter an incorrect password when logging in through the iNode client.

201312300323

- Symptom: Multichassis PFC does not take effect.
- Condition: This symptom occurs when the following conditions exist:
  - Two switches form an IRF fabric through 10-GE SFP+ fiber ports. Interfaces A and B are located on different IRF member switches.
  - Traffic enters the IRF fabric through interface A and leaves through interface B. The same PFC configuration is used on all interfaces that the traffic passes through.

201312170023

- Symptom: A VM exchanges login packets with the aggregation group member ports on the subordinate member switch of an IRF fabric. The VM cannot successfully log in.
- Condition: This symptom occurs when the following conditions exist:
  - In an IRF fabric, enable EVB and create S-channels on a multichassis Layer 2 aggregate interface.
  - Aggregation group member ports on the subordinate member switch receive the login packets from the VM.

201312230472

- Symptom: After a master/subordinate switchover occurs to an IRF fabric, the previous master switch cannot correctly start for a long time, and it prompts that the EVB process fails to start.
- Condition: This symptom occurs when the following conditions exist:
  - In an IRF fabric, enable EVB and create S-channels on a Layer 2 aggregate interface.
  - Master/subordinate switchover occurs to the IRF fabric.

- The aggregation group member ports on the subordinate member switch receive a large amount of EVB protocol packets and data packets.
- The NPV switch is configured to operate in FCF mode.

201401240231

- Symptom: Traffic statistics are collected for traffic in only one direction.
- Condition: This symptom occurs when you use a controller to deploy bidirectional extensibility flow entries to the switch and the switch receives and sends traffic.

201402100406

- Symptom: A switch does not display the MAC addresses learned by the UNI and NNI ports involved in many-to-one VLAN mapping.
- Condition: This symptom occurs when you configure many-to-one VLAN mapping on the switch.

Resolved problems in R2402

201312030126

- 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.

201311040104

- Symptom: IRF fails to forward Bidir PIM traffic between slots.
- Condition: This symptom occurs when IRF performs inter-slot Bidir PIM traffic forwarding.

201311040132

- Symptom: When TC Snooping is enabled using the **stp tc-snooping** command, the switch continually deletes MAC entries, affecting MAC update and aging.
- Condition: This symptom can be seen when TC Snooping is enabled using the **stp tc-snooping** command.

201311040138

- Symptom: When STP is disabled on a port, traffic is blocked on the port due to STP block.
- Condition: This symptom occurs if the following procedure is performed:
  - **a.** Disable TRILL on a port.
  - **b.** Configure the port as an IRF port.
  - **c.** Change the IRF port to a common port.
  - **d.** Enable TRILL on the port.

201311060199

- Symptom: The **display mac-address** command cannot display MAC address table information for a specified nickname.
- Condition: This symptom can be seen when the **display mac-address** command is executed to display MAC address table information for a specified nickname.

201311040237

- Symptom: Broadcast traffic is flooded through the first 16 selected ports (in ascending order of port numbers) in an aggregation group that has 32 selected ports.

- Condition: This symptom can be seen when broadcast traffic passes an aggregation group that has 32 selected ports.

201311190518

- Symptom: Type 3 LSAs for servers in different NSSA areas still exist after the servers become unreachable.
- Condition: This symptom can be seen when the following conditions exist:
  - The NSSA areas have a common ABR, which provides equal-cost routes to the servers.
  - The ABR advertises Type 3 LSAs for the servers in different NSSA areas.
  - The servers become unreachable.

201311090008

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

201311040393

- Symptom: The 10-GE breakout interface information displayed in IMC is disordered.
- Condition: This symptom occurs after the first 40-GE interface of the switch is split into four 10-GE breakout interfaces.

201311290364

- Symptom: On a ring-topology IRF fabric, an IRF port is blocked after its physical ports are removed, and then bound to the IRF port again.
- Condition: This symptom occurs if the following procedure is performed:
  - **a.** Shut down all the physical ports of the IRF port.
  - **b.** Use the **undo irf-port** command to remove the physical ports from the IRF port.
  - **c.** Bind the physical ports to the IRF port again.

201311220152

- Symptom: After a port is bound to an IRF port and then is removed from the IRF port, the port is blocked by STP, and it cannot forward any traffic, although STP is globally disabled.
- Condition: This symptom occurs if the following procedure is performed when STP is globally disabled:
  - **a.** Configure an IRF port, and use the **port group interface Ten-GigabitEthernet** command to bind the IRF port to a port that is shut down.
  - **b.** Use the **undo irf-port** command to remove all port bindings on the IRF port.

201312060311

- Symptom: The state of a BFD session to an OSPF neighbor continually goes up and down.
- Condition: This symptom occur when the following conditions exist:
  - The OSPF neighbor is an IRF fabric.
  - FRR is enabled using the **fast-reroute lfa** command.
  - BFD is used for FRR.

201311040163

- Symptom: When a member port in a Layer 3 aggregation group is changed to a Layer 2 Ethernet interface and then assigned to a VLAN, the VLAN interface for that VLAN cannot ping the directly connected device.
- Condition: The symptom occurs when the following procedure is performed:

a. Configure a Layer 3 aggregate interface, and assign member ports to the Layer 3 aggregation group.
b. Use the **port link-mode bridge** command to change a member port in the Layer 3 aggregation group to a Layer 2 Ethernet interface, and assign the port to a VLAN.

201311200449

- Symptom: BFD MAD does not take effect when it is configured on a VLAN interface of an IRF fabric.
- Condition: This symptom occurs when BFD MAD is configured on a VLAN interface of an IRF fabric.

201311140447

- Symptom: The switch fails to download a file from a TFTP server after **tftp x.x.x.x get xxx.xxx** is executed.
- Condition: This symptom can be seen if the TFTP server is TFTPD32.

201310220122

- Symptom: After an IRF master/subordinate switchover, the system prompts that ARP rate-limit fails to be assigned.
- Condition: This symptom can be seen if the following procedure is performed:
  a. Configure ARP rate-limit on an IRF fabric.
  b. Reboot the master to perform a master/subordinate switchover.

201312010016

- Symptom: When a switch starts up with factory defaults and the configuration is rolled back, all OpenFlow instances are inactive. To activate these OpenFlow instances, activate them one by one or reboot the switch.
- Condition: This symptom occurs when the following procedure is performed:
  a. Configure OpenFlow instances and save the configuration.
  b. Start the switch with factory defaults, and roll back the configuration.

201311280415

- Symptom: The **format** and **fixdisk** commands do not take effect.
- Condition: This symptom can be seen when you use the **format** or **fixdisk** command to format or fix the flash.

201311040427

- Symptom: After multiple PW switchovers between PEs, the PEs have inconsistent PW entries, resulting in forwarding failures.
- Condition: This symptom occurs if the following conditions exist:
  - The two PEs establish both local and remote LDP peer relationships.
  - Multiple PW switchovers are performed between PEs

201312060429

- Symptom: When the maximum number of Selected ports allowed in an aggregation group is reached, the newly assigned member ports are in the Unselected state. However, they can forward traffic.
- Condition: This symptom occurs when the number of member ports in an aggregation group exceeds the maximum number of Selected ports allowed in the aggregation group.

201312030470

- Symptom: On a two-chassis IRF fabric, the peer IRF port of the subordinate device is up. However, the port cannot receive packets while the subordinate device is rebooting.
- Condition: This symptom occurs when you reboot the subordinate device of a two-chassis IRF fabric.

201311140161

- Symptom: BFD flapping occurs.
- Condition: This symptom can be seen when the following conditions exist:
  - The **bfd min-transmit-interval** and **bfd min-receive-interval** are both set to 250 ms.
  - The **bfd detect-multiplier** is set to 3.
  - The CPU is attacked by TTL=1 IP packets or other packets.

201311040504

- Symptom: No trap message is output after the configuration file is saved.
- Condition: This symptom can be seen after the configuration file is saved.

201311040423

- Symptom: The switch might fail to forward traffic over a PW.
- Condition: This symptom might be seen after the IP address of the public interface is changed.

201311040308

- Symptom: STP state error occurs on an IRF fabric, resulting in a loop.
- Condition: This symptom can be seen if the following procedure is performed:
  - **a.** Enable STP on the IRF fabric and configure multi-chassis link aggregation.
  - **b.** Reboot the IRF fabric.

201311040137

- Symptom: The RTM policy quits when an RTM action is executing a python script.
- Condition: This symptom can be seen if the python script contains multiple Binary Right Shift Operators ">>".

201311040128

- Symptom: The SPBM process abnormally exits.
- Condition: This symptom occurs when the following procedure is performed:
  - **a.** Enable SPBM.
  - **b.** Configure an MST region as follows:
    ```
    stp region-configuration
    region-name spbm
    instance 4092 vlan 1001 to 2023
    active region-configuration
    ```
  - **c.** Continuously configure and cancel the mapping between MSTI 2 and VLANs.

201311040155

- Symptom: A TRILL port configured as an access port with the alone attribute can still process LSPs. As a result, an invalid bridge might be elected as a TRILL distribution tree root, and TRILL cannot forward broadcast traffic.
- Condition: This symptom occurs when you configure a hybrid TRILL port as an access TRILL port with the alone attribute.

201311040164

- Symptom: After an RB reboots, the configured nickname does not take effect. Instead, a nickname is randomly generated for the RB.
- Condition: This symptom occurs when the following procedure is performed:
  a. Configure the nickname for an RB and save the configuration.
  b. Disable TRILL globally, and reboot the RB without saving the configurations.

201311060490

- Symptom: When packets are dropped due to Fast Filter Processor (FFP) or STP non-forwarding state exist, the dropped packet count is always 0 in the output from the **display packet-drop summary** or **display packet-drop interface** command.
- Condition: This symptom occurs when packets are dropped due to the existing of Fast Filter Process or (FFP) or STP non-forwarding state.

201311280471

- Symptom: The buffer settings in the output from the **display buffer queue** command are different from the actual buffer settings.
- Condition: This symptom occurs when the following procedure is performed:
  a. Use the **buffer egress cell queue** command to configure the fixed area space or shared area space of cell resources in the egress buffer.
  b. Use the **buffer apply** command to apply the manually configured data buffer settings.

201311260519

- Symptom: A routed subinterface on the IRF fabric cannot be pinged from its directly connected device after a master/subordinate switchover occurs on the IRF fabric.
- Condition: This symptom occurs when a master/subordinate switchover occurs.

201312060432

- Symptom: Many-to-one VLAN mapping fails to replace the SVLAN tag with CVLAN tags for the downlink traffic.
- Condition: This symptom occurs when the following procedure is performed:
  a. Configure many-to-one VLAN mapping on an IRF fabric. Many-to-one VLAN mapping should replace the SVLAN tag with the CVLAN tags for the downlink traffic according to the DHCP snooping entries.
  b. Reboot an IRF member device which does not host the incoming interface of the traffic, and shut down the incoming interface, so that the traffic enters the IRF fabric through the rebooted IRF member device.

201312010009

- Symptom: BGP/OSPF neighbor flapping occurs after **ip redirects enable** and then **undo ip redirects enable** are executed.
- Condition: This symptom occurs after **ip redirects enable** and then **undo ip redirects enable** are executed.

201311040117

- Symptom: EVE does not work after an IRF fabric is manually rebooted.
- Condition: This symptom can be seen if the IRF fabric has large numbers of EVB VSIs.

201311190051

- Symptom: After **shutdown** and then **undo shutdown** are performed on an EVB-enabled aggregate interface, the VMs (in keepalive state) connected to the aggregate interface cannot get online.

- Condition: This symptom occurs after **shutdown** and then **undo shutdown** are performed on an EVB-enabled aggregate interface.

201311040118

- Symptom: The **lock** command can be successfully executed if you press **Enter** at the prompt "Please input password<1 to 16> to lock current line:" without inputting a password.
- Condition: This symptom can be seen if you press **Enter** at the prompt "Please input password<1 to 16> to lock current line:" without inputting a password.

201311040093/201312040162

- Symptom: When a port joins or leaves a link aggregation group, the device hosting the port reboots abnormally. If you continue injecting CDCP packets and VSI packets during the operation, the standby member device of the IRF fabric keeps rebooting.
- Condition: This symptom occurs when the following procedure is performed:
  a. Plenty of EVB configurations exist on the aggregate interface of an IRF fabric.
  b. Assign ports to or remove member ports from the aggregation group.

201311040101

- Symptom: The L2VPN process unexpectedly quits during an IRF master/subordinate switchover.
- Condition: This symptom might be seen if the IRF fabric has large number of L2VPN peers.

201311040139

- Symptom: If the egress interface of a CCC connection that is configured with the **nexthop** keyword is changed, L2VPN updates the LSP, and the MPLS entry becomes incorrect.
- Condition: This symptom can be seen if the egress interface of a CCC connection that is configured with the **nexthop** keyword is changed.

201312030399

- Symptom: The CLI does not respond.
- Condition: This symptom occurs if the following procedure is performed:
  a. Divide a 40 GE interface into four 10 GE interfaces.
  b. Configure the 10 GE interfaces as IRF physical interfaces.

201311040141

- Symptom: The **display vrrp** or **display vrrp ipv6** command continually outputs VRRP group information.
- Condition: This symptom can be seen if more than seven VRRPv2 or VRRPv3 groups are configured on a VLAN interface.

201311040166

- Symptom: In a TRILL network, a non-AVF port forwards IGMP packets.
- Condition: This symptom occurs when the following procedure is performed:
  a. Set up a TRILL network, and a Layer 2 switch is elected as an AVF.
  b. Transmit IGMP packets in the TRILL network.

201311260189

- Symptom: A port cannot be assigned to a static VLAN.
- Condition: This symptom occurs when the following procedure is performed:
  a. Enable MVRP globally and on a port. The port learns a VLAN dynamically.

b. Use the **undo port trunk permit vlan** command to remove the port from the dynamic VLAN.
c. Manually create the same VLAN. Use the **port trunk permit vlan** command to assign the port to the VLAN.

201312060371

- Symptom: On two IRF fabrics that are connected through a Layer 2 aggregate interface, DLDP flapping might occur when the CPU usage is high.
- Condition: This symptom might occur when the following conditions exist:
    - Two IRF fabrics are connected through a Layer 2 aggregate interface.
    - The member interfaces of the aggregate interface are enabled with DLDP.

201311180003

- Symptom: An SSH user fails to log in to the switch.
- Condition: This symptom can be seen when the following conditions exist:
    - The ACS server is configured.
    - The login-service is set to Telnet.

201311040317

- Symptom: After online users reach the limit configured using the **access-limit** command, are set to blocked state by using the **state block** command, and then log out, the output from the **display local-user** command shows that the number of online users is not reduced, and the logged-out users cannot log in to the switch.
- Condition: This symptom can be seen after online users reach the limit configured using the **access-limit** command and then are logged out using the **state block** command.

201311040112

- Symptom: After an IRF member switch is rebooted, the routes over a tunnel interface might become invalid.
- Condition: This symptom might occur after an IRF member switch is rebooted.

201312250142

- Symptom: After an IRF master/subordinate switchover, the VSIs on an S-channel aggregate interface of the original subordinate switch get offline and then online.
- Condition: This symptom occurs when the following conditions exist:
    - An S-channel aggregate interface is created on the subordinate switch.
    - An IRF master/subordinate switchover is performed.

201401090199

- Symptom: When a port of a VLAN receives a packet destined for the MAC address of the VLAN interface of another VLAN, the port discards the packet.
- Condition: This symptom can be seen when a port of a VLAN receives a packet destined for the MAC address of the VLAN interface of another VLAN.

201311040158

- Symptom: Switches directly connected through a Layer 3 aggregate interface cannot ping each other.
- Condition: This symptom occurs if a VPN instance is bound to the member interfaces of the Layer 3 aggregate interface but is not bound to the Layer 3 aggregate interface.

Resolved problems in E2402

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

- HPE 6125XLG Blade Switch Installation Guide
- About the HPE 6125XLG Blade Configuration Guides-R242x
- HPE 6125XLG Blade Switch Series ACL and QoS Configuration Guide-R242x
- HPE 6125XLG Blade Switch Series Configuration Guides Index-R242x
- HPE 6125XLG Blade Switch Series EVB Configuration Guide-R242x
- HPE 6125XLG Blade Switch Series FCoE Configuration Guide-R242x
- HPE 6125XLG Blade Switch Series Fundamentals Configuration Guide-R242x
- HPE 6125XLG Blade Switch Series High Availability Configuration Guide-R242x
- HPE 6125XLG Blade Switch Series IP Multicast Configuration Guide-R242x

- HPE 6125XLG Blade Switch Series IRF Configuration Guide-R242x
- HPE 6125XLG Blade Switch Series Layer 2 - LAN Switching Configuration Guide-R242x
- HPE 6125XLG Blade Switch Series Layer 3 - IP Routing Configuration Guide-R242x
- HPE 6125XLG Blade Switch Series Layer 3 - IP Services Configuration Guide-R242x
- HPE 6125XLG Blade Switch Series MPLS Configration Guide-R242x
- HPE 6125XLG Blade Switch Series Network Management and Monitoring Configuration Guide-R242x
- HPE 6125XLG Blade Switch Series OpenFlow Configuration Guide-R242x
- HPE 6125XLG Blade Switch Series Security Configuration Guide-R242x
- HPE 6125XLG Blade Switch Series SPB Configuration Guide-R242x
- HPE 6125XLG Blade Switch Series TRILL Configuration Guide-R242x
- About the HPE 6125XLG Blade Command References-R242x
- HPE 6125XLG Blade Switch Series ACL and QoS Command Reference-R242x
- HPE 6125XLG Blade Switch Series EVB Command Referencee-R242x
- HPE 6125XLG Blade Switch Series FCoE Command Reference-R242x
- HPE 6125XLG Blade Switch Series Fundamentals Command Reference-R242x
- HPE 6125XLG Blade Switch Series High Availability Command Reference-R242x
- HPE 6125XLG Blade Switch Series IP Multicast Command Reference-R242x
- HPE 6125XLG Blade Switch Series IRF Command Reference-R242x
- HPE 6125XLG Blade Switch Series Layer 2 - LAN Switching Command Reference-R242x
- HPE 6125XLG Blade Switch Series Layer 3 - IP Routing Command Reference-R242x
- HPE 6125XLG Blade Switch Series Layer 3 - IP Services Command Reference-R242x
- HPE 6125XLG Blade Switch Series MPLS Command Reference-R242x
- HPE 6125XLG Blade Switch Series Network Management and Monitoring Command Reference-R242x
- HPE 6125XLG Blade Switch Series Security Command Reference-R242x
- HPE 6125XLG Blade Switch Series TRILL Command Reference-R242x
- HPE 6125XLG Blade Switch Series OpenFlow Command Referencee-R242x
- HPE 6125XLG Blade Switch Series SPB Command Reference-R242x

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 5 hardware features

Item	Specification
Dimensions (H × W × D) (excluding feet and rack-mounting brackets)	27.9 × 192.8 × 267.7 mm (1.1 × 7.59 × 10.54 in)
Weight	≤ 2 kg (4.41 lb)
Input AC voltage	90V to 264V, 47/63Hz
Max. power consumption	95W
Operating temperature	10°C to 35°C (50°F to 95°F)
Relative humidity (noncondensing)	10% to 90%

Software features

Table 6 Software features

Category	Features
Full duplex Wire speed L2 switching capacity	1280Gbps
Whole system Wire speed L2 switching Packet forwarding rate	Up to 893Mpps
Forwarding mode	Store-forward and cut-through
IRF	• Ring topology • Daisy chain topology • LACP MAD • ARP MAD • ND MAD • BFD MAD • IRF comprised of different models
Link aggregation	• Aggregation of 10-GE ports • Aggregation of 40-GE ports • Static link aggregation • Dynamic link aggregation • When stacked, supports up to 1024 aggregation groups, each supporting up to 32 ports

Category	Features
Data center	• PFC • DCBX • FcoE(FCF/Transit/NPV) • TRILL • EVB • SPBM • PBB
OpenFlow	• Supported
Flow control	• IEEE 802.3x flow control and back pressure
Jumbo Frame	Supports maximum frame size of 10000
MAC address table	• 128K MAC addresses • 1K static MAC addresses • Blackhole MAC addresses • MAC address learning limit on a port
VLAN	• Port-based VLANs (4094 VLANs) • Private VLAN • Super VLAN • MVRP • QinQ and selective QinQ
VLAN mapping	• One-to-one VLAN mapping • Many-to-one VLAN mapping • Two-to-two VLAN mapping
ARP	• 16K entries • 1K static entries • Gratuitous ARP • Standard proxy ARP and local proxy ARP • ARP source suppression • ARP black hole • ARP detection (based on DHCP snooping entries/802.1x security entries/static IP-to-MAC bindings) • Multicast ARP • ARP logging • IRDP • ARP proxy
ND	• 8K entries • 1K static entries • ND proxy
VLAN virtual interface	• 1K
Router port	• Supported • Router port aggregation

Category	Features
DHCP	• DHCP client • DHCP snooping • DHCP relay agent • DHCP server • DHCPv6 snooping • DHCPv6 rlay agent • DHCPv6 server
UDP helper	• Supported
DNS	• Dynamic domain name resolution • Dynamic domain name resolution client • IPv4/IPv6 addresses
IPv4 routing	• 1K static routes • RIP (Routing Information Protocol) v1/v2; up to 2K IPv4 routes • OSPF (Open Shortest Path First) v1/v2; up to 16K IPv4 routes • BGP (Border Gateway Protocol); up to 16K IPv4 routes • IS-IS (Intermediate System-to-Intermediate System); up to 16K IPv4 routes • Configurable maximum number of equal-cost routes; up to 4K equal-cost routes • VRRP • PBR • GR • NSR
IPv6 routing	• 1K static routes • RIPng: Supports up to 2K IPv6 routes • OSPF v3: Supports up to 8K IPv6 routes • ISISv6: Supports up to 8K IPv6 routes • Up to 4K ECMP routes; each ECMP route supports up to 32 next hops • Routing policy • VRRP • PBR • GR • NSR
URPF	• Reverse route check strict mode and loose mode
MCE	• Supported
BFD	• OSPF/OSPFv3 • BGP/BGP4 • IS-IS/IS-ISv6 • PIM/IPM for IPv6 • Static route • MAD

Category	Features
Tunnel	• IPv4 over IPv4 tunnel • IPv4 over IPv6 tunnel • IPv6 over IPv4 manual tunnel • IPv6 over IPv4 6to4 tunnel • IPv6 over IPv4 ISATAP tunnel • IPv6 over IPv6 tunnel • GRE tunnel
MPLS	• MPLS • VPLS
IPv4 multicast	• IGMP snooping v1/v2/v3 • IGMP report suppression • Multicast VLAN • IGMP v1/v2/v3 • PIM-DM • PIM-SM • PIM-SSM • PIM-BIDIR • MSDP • PIM snooping • Multicast VPN
IPv6 multicast	• MLD snooping v1/v2 • MLD report suppression • IPv6 multicast VLAN • Ipv6 PIM snooping • MLD v1/v2 • PIM-DM/SM for IPv6 • IPv6 PIM-SSM • IPv6 BIDIR-PIM
Broadcast/multicast/unicast storm control	• Storm control based on port rate percentage • PPS-based storm control • Bps-based storm control
MSTP	• STP/RSTP/MSTP protocol • STP Root Guard • BPDU Guard
Smart Link	• Up to 26 groups • Multi-instance Smart Link
Monitor Link	• Supported

Category	Features
QoS/ACL	• Restriction of the rates at which a port sends and receives packets, with a granularity of 8 kbps. • Packet redirect • Committed access rate (CAR), with a granularity of traffic limit 8 kbps. • Eight output queues for each port • Flexible queue scheduling algorithms based on port and queue, including strict priority (SP), Weighted Deficit Round Robin (WDRR), Weighted Fair Queuing (WFQ), SP + WDRR, and SP + WFQ. • 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) • Queue shaping • User profile • COPP • Explicit Congestion Notification (ECN)
Mirroring	• Flow mirroring • Port mirroring • Multiple mirror observing port
Remote mirroring	• Port remote mirroring (RSPAN) • Layer 3 remote port mirroring(ERSPAM)
Security	• Hierarchical management and password protection of users • AAA authentication • RADIUS authentication • HWTACACS • SSH 2.0 • Port isolation • Port security • IP-MAC-port binding • IP Source Guard • MFF • HTTPS • SSL • PKI • Portal • Boot ROM access control (password recovery)
802.1X	• Up to 2,048 users • Port-based and MAC address-based authentication • Trunk port authentication
Traffic Management	• sFlow

Category	Features
Loading and upgrading	• Loading and upgrading through XModem protocol • Loading and upgrading through FTP • Loading and upgrading through the trivial file transfer protocol (TFTP)
Management	• Configuration at the command line interface • WEB • Remote configuration through Telnet • Configuration through Console port • Python • NETCONF • Simple network management protocol (SNMP) • IMC NMS • System log • Hierarchical alarms • NTP • PTP • EAA • RMON
Maintenance	• Debugging information output • Ping and Tracert • NQA • Track • Remote maintenance through Telnet • 802.1ag • 802.3ah • DLDP

Appendix B Upgrading software

Software upgrade enables you to have new features and fix bugs. Before performing an upgrade, use the release notes for the new software version to verify software and hardware compatibility and evaluate upgrade impacts.

Software types

The following software types are available:

- **BootWare image**—A .bin file that contains a basic segment and an extended segment. The basic segment is the minimum code that bootstraps the system. The extended segment enables hardware initialization and provides system management menus. You can use these menus to load software and the startup configuration file or manage files when the device cannot start up correctly.
- **Comware image**—Includes the following image subcategories:
  - **Boot image**—A .bin file that contains the Linux operating system kernel. It provides process management, memory management, file system management, and the emergency shell.
  - **System image**—A .bin file that contains the software feature modules for device operation and network services, including device management, interface management, configuration management, and routing.
  - **Patch packages**—Irregularly released packages for fixing bugs without rebooting the device. A patch package does not add new features or functions.

  Comware software images that have been loaded are called "current software images." Comware images specified to load at the next startup are called "startup software images."

BootWare image, boot image, and system image are required for the system to work. These images might be released separately or as a whole in one .ipe package file. If an .ipe file is used, the system decompresses the file automatically, loads the .bin boot and system images, and sets them as startup software images. Typically, the BootWare and startup software images for the device are released in an .ipe file.

Software file naming conventions

Software image file names use the *chassis-comware version-image type-release* format, for example, 6125xlg-cmw710-boot-R2306.bin and 6125xlg-cmw710-system-R2306.bin. This document uses **boot.bin** and **system.bin** as boot and system image file names.

Comware image redundancy and loading procedure

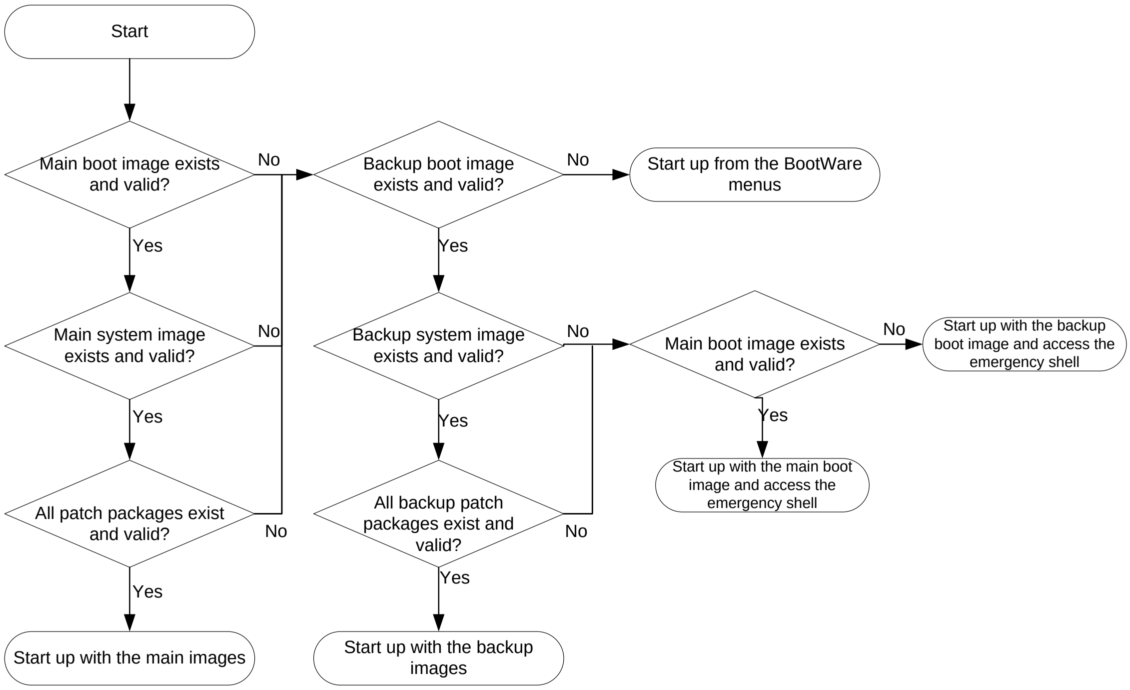
You can specify two sets of Comware software images: one main and one backup.

The system always attempts to start up with the main images. If any main image does not exist or is invalid, the system tries the backup images. Figure 1 shows the entire Comware image loading procedure.

If both of the main and backup boot images are invalid or unavailable, connect to the console port and power cycle the device to access the BootWare menus for loading a boot image.

To access the Comware system from the emergency shell, you must connect to the console port and load a system image. For more information about using the emergency shell, see *HPE 6125XLG Blade Switch Series Fundamentals Configuration Guide*.

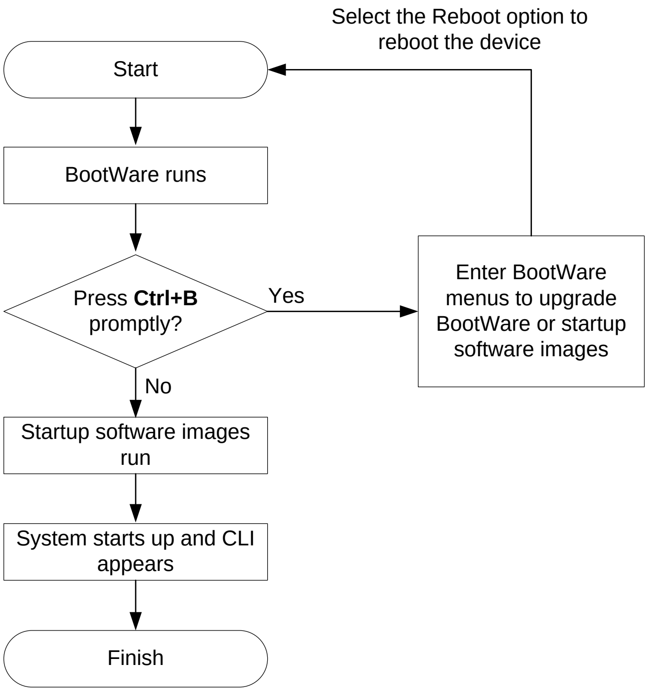
Figure 1 Comware image loading procedure



System startup process

Upon power-on, the BootWare image runs to initialize hardware, and then the startup software images run to start up the entire system, as shown in Figure 2.

Figure 2 System startup process



Upgrade methods

You can upgrade system software by using one of the following methods:

<table>
<tr><th>Upgrading method</th><th>Software types</th><th>Remarks</th></tr>
<tr><td rowspan="2">Upgrading from the CLI:
• Upgrading the software images
• Installing a patch package</td><td>• BootWare image
• Comware images (exclude patches)</td><td>This method is disruptive. You must reboot the entire device to complete the upgrade.</td></tr>
<tr><td>Patch packages</td><td>This method fixes software defects without requiring a system reboot.
Make sure the patch packages match the current software images. A patch package fixes bugs only for its matching software image version.</td></tr>
<tr><td>Upgrading Comware software from the BootWare menus</td><td>• BootWare image
• Comware images</td><td>Use this method when the switch cannot start up correctly.
CAUTION:
Upgrade an IRF fabric from the CLI rather than the BootWare menus.
The BootWare menu method increases the service downtime, because it requires that you upgrade the member switches one by one.</td></tr>
</table>

Upgrading from the CLI

This section uses a two-chassis IRF fabric as an example to describe how to upgrade software from the CLI. If you are upgrading a standalone switch, ignore the steps for upgrading the subordinate switch. If you have more than two subordinate switches, repeat the steps for the subordinate switches to upgrade their software. For more information about setting up and configuring an IRF fabric, see *HPE 6125XLG Blade Switch Series IRF Configuration Guide*.

NOTE:

The output in this document is for illustration only and might vary with software releases.

Preparing for the upgrade

Before you upgrade software, complete the following tasks:

1. Log in to the IRF fabric through Telnet or the console port (details not shown).
2. Execute the **display irf** command in any view to identify the number of IRF members and each member switch's role and IRF member ID.

```
<Sysname> display irf
MemberID   Role   Priority  CPU-Mac         Description
 *+1      Master  5         0023-8927-afdc  ---
   2      Standby 1         0023-8927-af43  ---
--------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The Bridge MAC of the IRF is: 0023-8927-afdb
 Auto upgrade                : no
 Mac persistent              : 6 min
 Domain ID                   : 0
```

3. Identify the free storage space of each member switch:

Identify the free flash space of the master switch.

```
<Sysname> dir
Directory of flash:
     0      -rw-       41424  Jan 01 2011 02:23:44     startup.mdb
     1      -rw-        3792  Jan 01 2011 02:23:44     startup.cfg
     2      -rw-    23129088  Nov 25 2011 09:53:48     system.bin
     3      drw-           -  Jan 01 2011 00:00:07     seclog
     4      drw-           -  Jan 01 2011 00:00:07     diagfile
     5      drw-           -  Jan 02 2011 00:00:07     logfile
     6      -rw-     8996864  Nov 25 2011 09:53:48     boot.bin
     7      -rw-     9012224  Nov 25 2011 09:53:48     backup.bin

524288 KB total (481540 KB free)
```

Identify the free flash space of each subordinate switch (for example, switch 2).

```
<Sysname> dir slot2#flash:/
Directory of slot2#flash:/
     0      -rw-       41424  Jan 01 2011 02:23:44     startup.mdb
     1      -rw-        3792  Jan 01 2011 02:23:44     startup.cfg
```

```
2       -rw-    23129088  Nov 25 2011 09:53:48     system.bin
3       drw-           -  Jan 01 2011 00:00:07     seclog
4       drw-           -  Jan 01 2011 00:00:07     diagfile
5       drw-           -  Jan 02 2011 00:00:07     logfile
6       -rw-     8996864  Nov 25 2011 09:53:48     boot.bin
7       -rw-     9012224  Nov 25 2011 09:53:48     backup.bin

524288 KB total (481540 KB free)
```

4. Compare the free flash space of each member switch with the size of the software file to load. If the space is sufficient, start the upgrade process. If the space is not sufficient, go to the next step.
5. Delete unused files from the flash memory to free space:

CAUTION:

- To avoid data loss, do not delete the current configuration file. To display the current configuration file, execute the **display startup** command in any view. Hewlett Packard Enterprise recommends that you preferentially delete unused software images. To avoid inadvertent delete of the current software images, use the **display boot-loader** command in any view to identify them.
- The **delete /unreserved** *file-url* command deletes a file permanently, and this action cannot be undone.

Use the **delete /unreserved** *file-url* command in user view to delete unused files from the flash memory of the master switch.

```
<Sysname> delete /unreserved flash:/backup.bin
The file cannot be restored. Delete flash:/backup.bin?[Y/N]:y
Deleting the file permanently will take a long time. Please wait...
Start to delete flash:/backup.bin...Done.
```

NOTE:

You cannot use the **delete** *file-url* command for the purpose of this procedure. This command moves a file to the recycle bin and the file still occupies storage space.

Delete unused files from the flash memory of the subordinate switch.

```
<Sysname> delete /unreserved slot2#flash:/backup.bin
The file cannot be restored. Delete slot2#flash:/backup.bin?[Y/N]:y
Deleting the file permanently will take a long time. Please wait...
Start to delete slot2#flash:/backup.bin...Done.
```

Transferring software to the master switch

The switch can work as an FTP server, FTP client, or TFTP server. Before you upgrade Comware images or install patches, use one of the following methods to transfer the upgrade file to the root directory of the master's flash memory:

- Downloading images from an FTP server
- Uploading images from an FTP client to the switch
- Downloading images from a TFTP server

This software guide uses an .ipe file to describe the upgrade procedure.

Prerequisites

Prepare the FTP or TFTP server yourself if you are using the switch as a client.

Make sure the IRF fabric has connectivity with the FTP/TFTP server or FTP client.

Downloading images from an FTP server

1. Configure the FTP server:

   # Run FTP server on the PC.

   # Configure an FTP username and password.

   # Specify the working directory.

   # Copy the image file (for example, **newest.ipe**) to the directory.

2. Execute the **ftp** command in user view on the IRF fabric to access the FTP server (for example, the server at 10.10.110.1).

```
<Sysname> ftp 10.10.110.1
Trying 10.10.110.1...
Press CTRL+K to abort
Connected to 10.10.110.1
220 FTP service ready.
User(10.10.110.1:(none)):username
331 Password required for username.
Password:
230 User logged in
```

3. Enable the binary transfer mode in FTP client view.

```
[ftp] binary
  200 Type set to I.
```

4. Download the upgrade file from the FTP server.

```
[ftp] get newest.ipe
  227 Entering Passive Mode (10,10,110,1,17,97).
  125 BINARY mode data connection already open, transfer starting for /newest.ipe
  226 Transfer complete.
  32133120 bytes received in 35 seconds (896. 0 kbyte/s)
[ftp] bye
221 Server closing.
```

Uploading images from an FTP client to the switch

1. On the IRF fabric:

   # Enable FTP server in system view.

```
<Sysname> system-view
[Sysname] ftp server enable
```

   # Add a local user account in system view.

```
[Sysname] local-user abc
```

   # Set the password to **pwd** in plain text in the user account.

```
[Sysname-luser-abc] password simple pwd
```

   # Set the access service type to **ftp** in the user account.

```
[Sysname-luser-abc] service-type ftp
```

   # Assign the **network-admin** user role to the user account for uploading files.

```
[Sysname-luser-abc] authorization-attribute user-role network-admin
```

   # Execute the **quit** command to return to the system view.

```
[Sysname-luser-abc] quit
```

   # Execute the **quit** command to return to the user view.

```
[Sysname] quit
```

2. On the PC:

   # Use FTP to log in to the IRF fabric (the FTP server at 1.1.1.1).

```
c:\> ftp 1.1.1.1
Connected to 1.1.1.1.
220 FTP service ready.
User(1.1.1.1:(none)):abc
331 Password required for abc.
Password:
230 User logged in.
```

   # Enable the binary file transfer mode.

```
ftp> binary
200 TYPE is now 8-bit binary.
```

   # Upload the file (for example, **newest.ipe**) to the root directory of the master's flash memory.

```
ftp> put newest.ipe
200 PORT command successful
150 Connecting to port 10002
226 File successfully transferred
ftp: 32133120 bytes sent in 64.58 secs (497.60 Kbytes/sec).
```

Downloading images from a TFTP server

To download an image file from a TFTP server (for example, the server at 10.10.110.1):

1. Configure the TFTP server:

   # Run TFTP server on the PC.

   # Specify the working directory.

   # Copy the image file (for example, **newest.ipe**) to the directory.

2. On the IRF fabric, use TFTP to download the image file to the root directory of the master's flash memory.

```
<Sysname> tftp 10.10.110.1 get newest.ipe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 30.6M    0 30.6M    0     0   143k      0 --:--:--  0:03:38 --:--:--  142k
```

Upgrading the software images

To upgrade the software images:

1. Specify the upgrade file as the main startup software image file for the master.

```
<Sysname> boot-loader file flash:/newest.ipe slot 1 main
Images in IPE:
  boot.bin
  system.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to target slot.
The specified file list will be used as the main startup software images at the next
reboot on slot 1.
```

2. Specify the upgrade file as the main startup software image file for the subordinate switch. (The subordinate switch will copy the upgrade file automatically from the master to the root directory of its flash memory.)

```
<Sysname> boot-loader file flash:/newest.ipe slot 2 main
```

```
Images in IPE:
  boot.bin
  system.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to target slot.
The specified file list will be used as the main startup software images at the next
reboot on slot 2.
```

3. (Optional.) If the IRF fabric has multiple subordinate members, enable the software auto-update function.

```
<Sysname> system-view
[Sysname] irf auto-update enable
[Sysname] quit
```

   Software auto-update automatically synchronizes the software images of the master switch to new member switches as the main startup software images.

4. Save the configuration to prevent data loss.

```
<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.
Slot 2:
Save next configuration file successfully.
```

5. Reboot the IRF fabric to complete the upgrade.

```
<Sysname> reboot
Start to check configuration with next startup configuration file, please wait.
........DONE!
This command will reboot the device. Continue? [Y/N]:y
 Now rebooting, please wait...
```

   The system automatically loads the .bin boot and system images in the .ipe file and sets them as the startup software images.

6. If the system detects that the BootWare image has an update, choose to upgrade both the basic and extended segments of the BootWare image for compatibility.

NOTE:

If you choose to not upgrade the BootWare image, the system will prompt for an upgrade at the next reboot. If you fail to make any choice in the required time, the system upgrades the entire BootWare image.

7. Execute the **display version** command to verify that the current main software images have been updated (details not shown).

Installing a patch package

1. Activate the patch package (for example, **system-patch.bin**) on the master switch and the subordinate switch.

```
<Sysname> install activate patch flash:/system-patch.bin slot 1
<Sysname> install activate patch flash:/system-patch.bin slot 2
```

2. Verify that the patch package has been activated.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot.bin
  flash:/system.bin
  flash:/system-patch.bin
Active packages on slot 2:
  flash:/boot.bin
  flash:/system.bin
  flash:/system-patch.bin
```

3. Commit the installation so the patch package continues to take effect after a reboot.

```
<Sysname> install commit
```

4. Verify that the patch package installation has been committed.

```
<Sysname> display install committed
Committed packages on slot 1:
  flash:/boot.bin
  flash:/system.bin
  flash:/system-patch.bin
Committed packages on slot 2:
  flash:/boot.bin
  flash:/system.bin
  flash:/system-patch.bin
```

For more information about installing patch packages, see *HPE 6125XLG Blade Switch Series Fundamentals Configuration Guide*.

Upgrading Comware software from the BootWare menus

Use one of the following methods to upgrade Comware software from the BootWare menus:

- Using TFTP to upgrade through the management Ethernet port
- Using FTP to upgrade through the management Ethernet port
- Using Xmodem to upgrade through the console port

For information about using BootWare, see "Appendix C Using BootWare menus."

NOTE:

- The switch does not come with FTP or TFTP server software. Prepare the software yourself.
- Upgrading through an Ethernet port is faster than through the console port.

Using TFTP to upgrade through the management Ethernet port

This upgrade procedure uses the switch as a TFTP client.

To upgrade software through TFTP:

1. Connect the management Ethernet port of the switch to the file server, and connect the console port of the switch to the configuration terminal.

   The configuration terminal can be co-located with the TFTP server.

2. Run a TFTP server program on the file server, and specify the file path of the upgrade file.
3. Run the terminal emulation program on the configuration terminal.
4. Start the switch and access the EXTENDED-BOOTWARE menu (see "Using the EXTENDED-BOOTWARE menu").
5. Enter **3** in the EXTENDED-BOOTWARE menu to access the Ethernet submenu.

```
==========================<Enter Ethernet SubMenu>==========================
|Note:the operating device is flash                                        |
|<1> Download Image Program To SDRAM And Run                               |
|<2> Update Main Image File                                                |
|<3> Update Backup Image File                                              |
|<4> Modify Ethernet Parameter                                             |
|<0> Exit To Main Menu                                                     |
|<Ensure The Parameter Be Modified Before Downloading!>                    |
============================================================================
Enter your choice(0-4):
```

6. Enter **4** to set Ethernet interface parameters.

NOTE:

To use the default setting for a field, press **Enter** without entering any information.

```
======================<ETHERNET PARAMETER SET>==============================
|Note:       '.' = Clear field.                                            |
|            '-' = Go to previous field.                                   |
|          Ctrl+D = Quit.                                                  |
============================================================================
Protocol (FTP or TFTP):tftp
Load File Name       :test.bin
                     :newest.ipe
Target File Name     :test.bin
                     :newest.ipe
Server IP Address    :192.168.80.22
Local IP Address     :192.168.80.10
Subnet Mask          :255.255.255.0
Gateway IP Address   :0.0.0.0
```

Table 7 Setting TFTP file transfer parameters

Field	Description
'.' = Clear field	Press the dot (.), and then press **Enter** to clear the setting for a field.
'-' = Go to previous field	Press the hyphen (-), and then press **Enter** to return to the previous field.
Ctrl+D = Quit	Press **Ctrl+D** to exit the Ethernet parameter settings menu.
Protocol (FTP or TFTP)	Set the file transfer protocol to TFTP.
Load File Name	Set the name of the file to be downloaded.
Target File Name	Set a file name for saving the file in the current storage medium on the switch. The target file must use the same suffix as the source file. By default, the target file name is the same as the source file

Field	Description
	name.
Server IP Address	Set the IP address of the TFTP server.
Local IP Address	Set the IP address of the switch.
Subnet Mask	Set the IP address mask of the switch.
Gateway IP Address	Set a gateway IP address if the switch is on a different network than the server.

7. Press **Ctrl+D** to return to the Ethernet submenu.

```
==========================<Enter Ethernet SubMenu>==========================
|Note:the operating device is flash                                         |
|<1> Download Image Program To SDRAM And Run                                |
|<2> Update Main Image File                                                 |
|<3> Update Backup Image File                                               |
|<4> Modify Ethernet Parameter                                              |
|<0> Exit To Main Menu                                                      |
|<Ensure The Parameter Be Modified Before Downloading!>                     |
============================================================================
Enter your choice(0-4):
```

8. Enter **2** or **3** to upgrade software images. For example, to upgrade the main Comware software images, enter **2**.

```
Loading.....................................................................
............................................................................
.........................Done!
31911744 bytes downloaded!
Image file BOOT.bin is self-decompressing... Saving file flash:/
BOOT.bin ..............................................Done.
Image file SYSTEM.bin is self-decompressing...Saving file flash:/
SYSTEM.bin .................................. ..Done.

==========================<Enter Ethernet SubMenu>==========================
|Note:the operating device is flash                                         |
|<1> Download Image Program To SDRAM And Run                                |
|<2> Update Main Image File                                                 |
|<3> Update Backup Image File                                               |
|<4> Modify Ethernet Parameter                                              |
|<0> Exit To Main Menu                                                      |
|<Ensure The Parameter Be Modified Before Downloading!>                     |
============================================================================
Enter your choice(0-4):
```

9. Enter **0** in the Ethernet submenu to return to the EXTENDED-BOOTWARE menu.
10. Enter **1** in the EXTENDED-BOOTWARE menu to run the new software images.

Using FTP to upgrade through the management Ethernet port

This upgrade procedure uses the switch as an FTP client.

To upgrade Comware software images through FTP:

1. Connect the management Ethernet port of the switch to the file server, and connect the console port of the switch to the configuration terminal.

   The configuration terminal can be co-located with the FTP server.
2. Run an FTP server program on the file server, specify the file path of the upgrade file, and set the FTP username and password.
3. Run the terminal emulation program on the configuration terminal.
4. Start the switch and access the EXTENDED-BOOTWARE menu (see "Using the EXTENDED-BOOTWARE menu").
5. Enter **3** in the EXTENDED-BOOTWARE menu to access the Ethernet submenu.

```
==========================<Enter Ethernet SubMenu>==========================
|Note:the operating device is flash                                        |
|<1> Download Image Program To SDRAM And Run                               |
|<2> Update Main Image File                                                |
|<3> Update Backup Image File                                              |
|<4> Modify Ethernet Parameter                                             |
|<0> Exit To Main Menu                                                     |
|<Ensure The Parameter Be Modified Before Downloading!>                    |
============================================================================
Enter your choice(0-4):
```

6. Enter **4** to set Ethernet interface parameters.

NOTE:

To use the default setting for a field, press **Enter** without entering any information.

```
======================<ETHERNET PARAMETER SET>==============================
|Note:       '.' = Clear field.                                            |
|            '-' = Go to previous field.                                   |
|          Ctrl+D = Quit.                                                  |
============================================================================
Protocol (FTP or TFTP) :ftp
Load File Name         :test.bin
                       :newest.ipe
Target File Name       :test.bin
                       :newest.ipe
Server IP Address      :192.168.80.20
Local IP Address       :192.168.80.10
Subnet Mask            :255.255.255.0
Gateway IP Address     :0.0.0.0
FTP User Name          :abc
FTP User Password      :PWD
```

Table 8 Setting FTP file transfer parameters

Field	Description
'.' = Clear field	Press the dot (.), and then press **Enter** to clear the setting for a field.
'-' = Go to previous field	Press the hyphen (-), and then press **Enter** to return to the previous field.
Ctrl+D = Quit	Press **Ctrl+D** to exit the Ethernet parameter settings menu.
Protocol (FTP or TFTP)	Set the file transfer protocol to FTP.
Load File Name	Set the name of the file to be downloaded.
Target File Name	Set a file name for saving the file in the current storage medium on the switch. The file suffix must be the same as the one of the source file name. By default, the target file name is the same as the source file name.
Server IP Address	Set the IP address of the FTP server.
Local IP Address	Set the IP address of the switch.
Subnet Mask	Set the IP address mask of the switch.
Gateway IP Address	Set a gateway IP address if the switch is on a different network than the server.
FTP User Name	Set the username for accessing the FTP server. This username must be the same as the one configured on the FTP server.
FTP User Password	Set the password for accessing the FTP server. This password must be the same as the one configured on the FTP server.

7. Press **Ctrl+D** to return to the Ethernet submenu.

```
==========================<Enter Ethernet SubMenu>==========================
|Note:the operating device is flash                                        |
|<1> Download Image Program To SDRAM And Run                               |
|<2> Update Main Image File                                                |
|<3> Update Backup Image File                                              |
|<4> Modify Ethernet Parameter                                             |
|<0> Exit To Main Menu                                                     |
|<Ensure The Parameter Be Modified Before Downloading!>                    |
============================================================================
Enter your choice(0-4):
```

8. Enter **2** to **3** to upgrade software images. For example, to upgrade the main Comware software images, enter **2**.

```
Loading.....................................................................
............................................................................
.........................Done!
31911744 bytes downloaded!
Image file BOOT.bin is self-decompressing... Saving file flash:/
BOOT.bin ..............................................Done.
Image file SYSTEM.bin is self-decompressing...Saving file flash:/
SYSTEM.bin .................................. ..Done.
```

```
==========================<Enter Ethernet SubMenu>==========================
|Note:the operating device is flash                                        |
|<1> Download Image Program To SDRAM And Run                               |
|<2> Update Main Image File                                                |
|<3> Update Backup Image File                                              |
|<4> Modify Ethernet Parameter                                             |
|<0> Exit To Main Menu                                                     |
|<Ensure The Parameter Be Modified Before Downloading!>                    |
============================================================================
Enter your choice(0-4):
```

9. Enter **0** in the Ethernet submenu to return to the EXTENDED-BOOTWARE menu.
10. Enter **1** in the EXTENDED-BOOTWARE menu to run the new software images.

Using Xmodem to upgrade through the console port

1. Connect the console port of the switch to the PC that stores the upgrade image file.
2. Run the terminal emulation program on the PC.
3. Start the switch and access the EXTENDED-BOOTWARE menu (see "Using the EXTENDED-BOOTWARE menu").
4. Enter **2** in the EXTENDED-BOOTWARE menu to access the Serial submenu.

```
===========================<Enter Serial SubMenu>===========================
|Note:the operating device is flash                                        |
|<1> Download Image Program To SDRAM And Run                               |
|<2> Update Main Image File                                                |
|<3> Update Backup Image File                                              |
|<4> Modify Serial Interface Parameter                                     |
|<0> Exit To Main Menu                                                     |
============================================================================
Enter your choice(0-4):
```

5. Enter **4** to change the baud rate of the console port.

```
===============================<BAUDRATE SET>===============================
|Note:'*'indicates the current baudrate                                    |
|     Change The HyperTerminal's Baudrate Accordingly                      |
|---------------------------<Baudrate Available>---------------------------|
|<1> 9600(Default)*                                                        |
|<2> 19200                                                                 |
|<3> 38400                                                                 |
|<4> 57600                                                                 |
|<5> 115200                                                                |
|<0> Exit                                                                  |
============================================================================
Enter your choice(0-5):
```

6. Enter an appropriate baud rate option. For example, enter **2** to select 19200 bps.

```
Baudrate has been changed to 19200 bps.
Please change the terminal's baudrate to 19200 bps, press ENTER when ready.
```

NOTE:

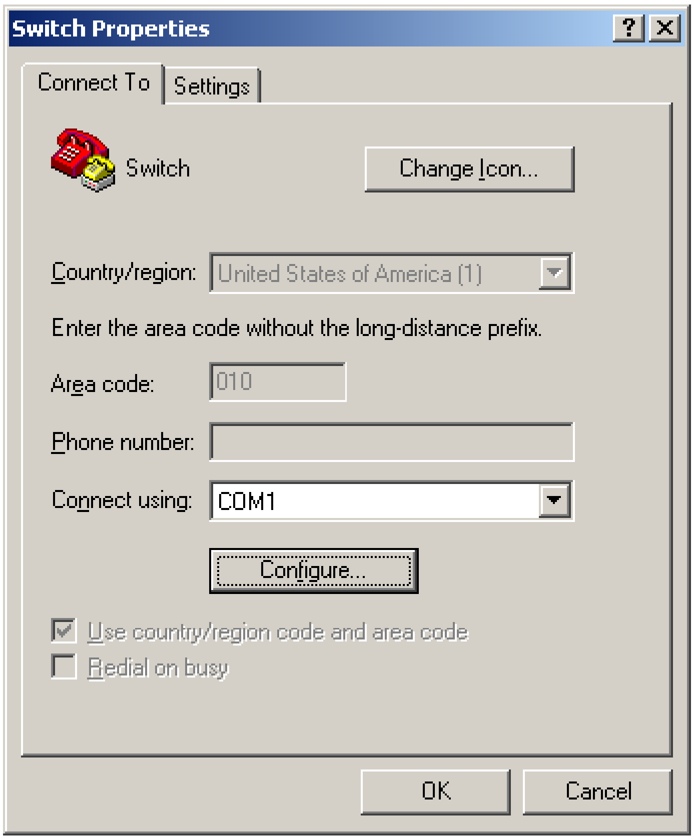
If you choose 9600 bps (the default baud rate), move to step 11.

7. Select **Call** > **Disconnect** from the HyperTerminal window to disconnect the HyperTerminal from the switch.

Figure 3 Disconnecting the HyperTerminal

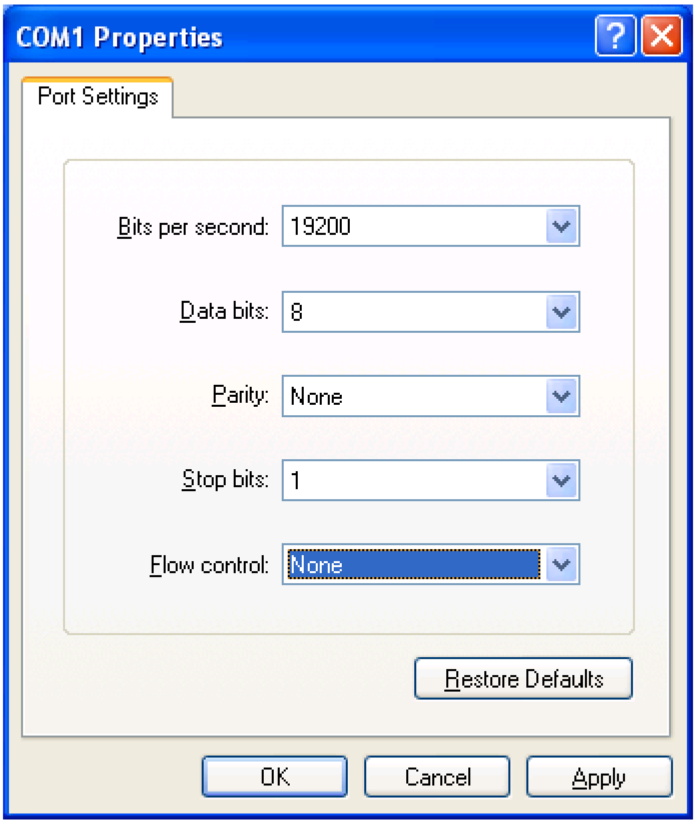
8. Select **File** > **Properties** in the HyperTerminal window, and click **Configure** in the popup dialog box.

Figure 4 Setting switch properties



9. Select **19200** from the **Bits per second** list, and click **OK**.

Figure 5 Modifying the baud rate



10. Select **Call** > **Call** to reconnect to the switch.

Figure 6 Reconnecting to the switch

11. Press **Enter** in the BootWare interface.

```
The current baudrate is 19200 bps
===============================<BAUDRATE SET>===============================
|Note:'*'indicates the current baudrate                                    |
|     Change The HyperTerminal's Baudrate Accordingly                      |
|---------------------------<Baudrate Available>-------------------------|
|<1> 9600(Default)                                                         |
|<2> 19200*                                                                |
|<3> 38400                                                                 |
|<4> 57600                                                                 |
|<5> 115200                                                                |
|<0> Exit                                                                  |
============================================================================
Enter your choice(0-5):
```

12. Enter **0** to return to the Serial submenu.

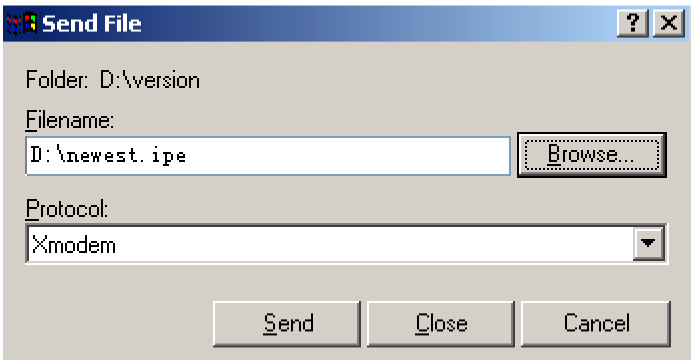
```
==========================<Enter Serial SubMenu>==========================
|Note:the operating device is flash                                      |
|<1> Download Image Program To SDRAM And Run                             |
|<2> Update Main Image File                                              |
|<3> Update Backup Image File                                            |
|<4> Modify Serial Interface Parameter                                   |
|<0> Exit To Main Menu                                                   |
==========================================================================
Enter your choice(0-4):
```

13. Enter **2** to **3** to upgrade the software images. For example, enter **2** to upgrade the main startup software images.

```
Please Start To Transfer File, Press <Ctrl+C> To Exit.
Waiting ...CCCCC
```

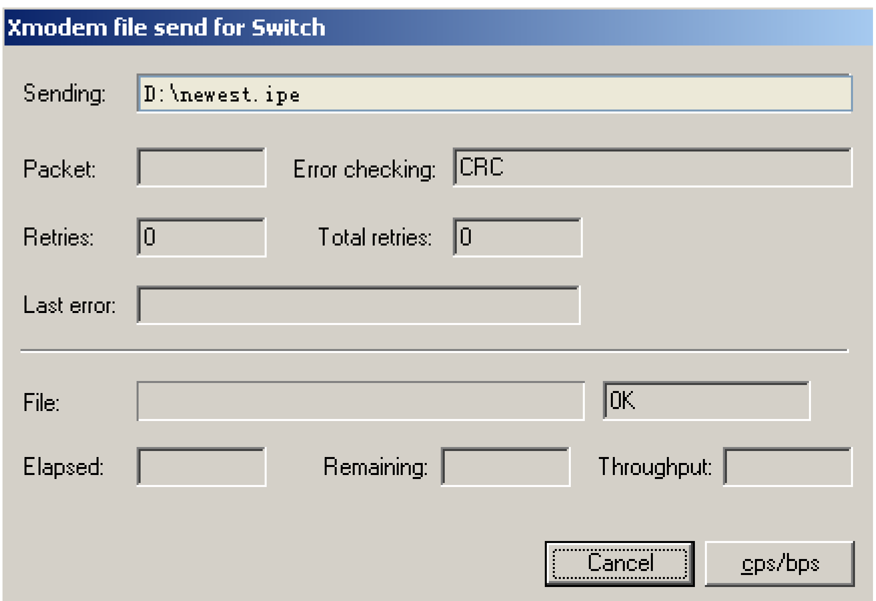
14. Select **Transfer** > **Send File** in the HyperTerminal window. In the **Send File** dialog box, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

Figure 7 Selecting the file to transfer



15. Click **Send**.

Figure 8 File transfer progress



When the file transfer is complete, the following information appears:

```
Download successfully!
31911808 bytes downloaded!Image file boot.bin is self-decompressing....
Input the file name: system.bin
Save file .........................................Done

===========================<Enter Serial SubMenu>===========================
|Note:the operating device is flash                                        |
|<1> Download Image Program To SDRAM And Run                               |
|<2> Update Main Image File                                                |
|<3> Update Backup Image File                                              |
|<4> Modify Serial Interface Parameter                                     |
|<0> Exit To Main Menu                                                     |
============================================================================
Enter your choice(0-4):
```

16. Enter **0** in the Serial submenu to return to the EXTENDED-BOOTWARE menu.
17. Enter **1** in the EXTENDED-BOOTWARE menu to run the new software.
18. Change the baud rate of the HyperTerminal back to 9600 bps, and reconnect to the switch.

NOTE:

The baud rate will restore to the default (9600 bps) at reboot. To set up a console session with the switch after a reboot, you must change the baud rate setting on the configuration terminal back to 9600 bps.

Upgrading BootWare from the BootWare menus

Use one of the following methods to upgrade the BootWare image from the BootWare menus:

- Using TFTP to upgrade through the management Ethernet port
- Using FTP to upgrade through the management Ethernet port
- Using Xmodem to upgrade through the console port

For more information about BootWare, see "Appendix C Using BootWare menus."

NOTE:

- The switch does not come with FTP or TFTP server software. Prepare the software yourself.
- Upgrading through an Ethernet port is faster than through the console port.

Using TFTP to upgrade through the management Ethernet port

This upgrade procedure uses the switch as a TFTP client.

To upgrade the BootWare image through TFTP:

1. Connect the management Ethernet port of the switch to the file server, and connect the console port of the switch to the configuration terminal.

   The configuration terminal can be co-located with the TFTP server.
2. Run a TFTP server program on the file server, and specify the file path of the upgrade file.
3. Run the terminal emulation program on the configuration terminal.

4. Start the switch and access the EXTENDED-BOOTWARE menu (see "Using the EXTENDED-BOOTWARE menu").
5. Enter **7** in the EXTENDED-BOOTWARE menu to access the BootWare Operation menu.

```
=========================<BootWare Operation Menu>=========================
|Note:the operating device is flash                                       |
|<1> Backup Full BootWare                                                 |
|<2> Restore Full BootWare                                                |
|<3> Update BootWare By Serial                                            |
|<4> Update BootWare By Ethernet                                          |
|<0> Exit To Main Menu                                                    |
===========================================================================
Enter your choice(0-4):
```

6. Enter **4** to access the BOOTWARE OPERATION ETHERNET submenu.

```
===================<BOOTWARE OPERATION ETHERNET SUB-MENU>===================
|<1> Update Full BootWare                                                 |
|<2> Update Extended BootWare                                             |
|<3> Update Basic BootWare                                                |
|<4> Modify Ethernet Parameter                                            |
|<0> Exit To Main Menu                                                    |
===========================================================================
Enter your choice(0-4):
```

7. Enter **4** to set file transfer parameters. For field description, see Table 7.

NOTE:

To use the default setting for a field, press **Enter** without entering any information.

```
==========================<ETHERNET PARAMETER SET>==========================
|Note:       '.' = Clear field.                                           |
|            '-' = Go to previous field.                                  |
|          Ctrl+D = Quit.                                                 |
===========================================================================
Protocol (FTP or TFTP) :tftp
Load File Name         :test.btw
                       :mpu.btw
Target File Name       :test.btw
                       :mpu.btw
Server IP Address      :192.168.80.22
Local IP Address       :192.168.80.10
Subnet Mask            :255.255.255.0
Gateway IP Address     :0.0.0.0
```

8. Press **Ctrl**+**D** to return to the BOOTWARE OPERATION ETHERNET submenu.

```
===================<BOOTWARE OPERATION ETHERNET SUB-MENU>===================
|<1> Update Full BootWare                                                 |
|<2> Update Extended BootWare                                             |
|<3> Update Basic BootWare                                                |
|<4> Modify Ethernet Parameter                                            |
|<0> Exit To Main Menu                                                    |
===========================================================================
Enter your choice(0-4):
```

9. Enter a number from **1** to **3** as needed. For example, enter **1** to upgrade the entire BootWare image.

```
Loading...........Done!
447612 bytes downloaded!
Updating Basic BootWare? [Y/N]
```

10. Enter **Y** to upgrade the basic BootWare segment.

```
Updating Basic BootWare.........Done!
Updating Extended BootWare? [Y/N]
```

11. Enter **Y** to upgrade the extended BootWare segment.

```
Updating Extended BootWare.........Done!

===================<BOOTWARE OPERATION ETHERNET SUB-MENU>===================
|<1> Update Full BootWare                                                  |
|<2> Update Extended BootWare                                              |
|<3> Update Basic BootWare                                                 |
|<4> Modify Ethernet Parameter                                             |
|<0> Exit To Main Menu                                                     |
============================================================================
Enter your choice(0-4):
```

12. Enter **0** in the BOOTWARE OPERATION ETHERNET submenu to return to the BootWare Operation menu.
13. Enter **0** in the BootWare Operation menu to return to the EXTENDED-BOOTWARE menu.
14. Enter **0** in the EXTENDED-BOOTWARE menu to reboot the switch.

Using FTP to upgrade through the management Ethernet port

This upgrade procedure uses the switch as an FTP client.

To upgrade the BootWare image through FTP:

1. Connect the management Ethernet port of the switch to the file server, and connect the console port of the switch to the configuration terminal.

   The configuration terminal can be co-located with the FTP server.
2. Run an FTP server program on the file server, specify the file path of the upgrade file, and set the FTP username and password.
3. Run the terminal emulation program on the configuration terminal.
4. Start the switch and access the EXTENDED-BOOTWARE menu (see "Using the EXTENDED-BOOTWARE menu").
5. Enter **7** in the EXTENDED-BOOTWARE menu to access the BootWare Operation menu.

```
=========================<BootWare Operation Menu>==========================
|Note:the operating device is flash                                        |
|<1> Backup Full BootWare                                                  |
|<2> Restore Full BootWare                                                 |
|<3> Update BootWare By Serial                                             |
|<4> Update BootWare By Ethernet                                           |
|<0> Exit To Main Menu                                                     |
============================================================================
Enter your choice(0-4):
```

6. Enter **4** to access the BOOTWARE OPERATION ETHERNET submenu.

```
===================<BOOTWARE OPERATION ETHERNET SUB-MENU>===================
|<1> Update Full BootWare                                                  |
|<2> Update Extended BootWare                                              |
|<3> Update Basic BootWare                                                 |
|<4> Modify Ethernet Parameter                                             |
|<0> Exit To Main Menu                                                     |
============================================================================
Enter your choice(0-4):
```

7. Enter **4** to set file transfer parameters. For field descriptions, see Table 8.

NOTE:

To use the default setting for a field, press **Enter** without entering any information.

```
==========================<ETHERNET PARAMETER SET>==========================
|Note:       '.' = Clear field.                                            |
|            '-' = Go to previous field.                                   |
|          Ctrl+D = Quit.                                                  |
============================================================================
Protocol (FTP or TFTP):ftp
Load File Name        :test.btw
                      :mpu.btw
Target File Name      :test.btw
                      :mpu.btw
Server IP Address     :192.168.80.20
Local IP Address      :192.168.80.10
Subnet Mask           :255.255.255.0
Gateway IP Address    :0.0.0.0
FTP User Name         :abc
FTP User Password     :pwd
```

8. Press **Ctrl**+**D** to return to the BOOTWARE OPERATION ETHERNET submenu.

```
===================<BOOTWARE OPERATION ETHERNET SUB-MENU>===================
|<1> Update Full BootWare                                                  |
|<2> Update Extended BootWare                                              |
|<3> Update Basic BootWare                                                 |
|<4> Modify Ethernet Parameter                                             |
|<0> Exit To Main Menu                                                     |
============================================================================
Enter your choice(0-4):
```

9. Enter a number from **1** to **3** as needed. For example, enter **1** to upgrade the entire BootWare image.

```
Loading...........Done!
447612 bytes downloaded!
Updating Basic BootWare? [Y/N]
```

10. Enter **Y** to upgrade the basic BootWare segment.

```
Updating Basic BootWare.........Done!
Updating Extended BootWare? [Y/N]
```

11. Enter **Y** to upgrade the extended BootWare segment.

```
Updating Extended BootWare.........Done!
```

```
==================<BOOTWARE OPERATION ETHERNET SUB-MENU>===================
|<1> Update Full BootWare                                                 |
|<2> Update Extended BootWare                                             |
|<3> Update Basic BootWare                                                |
|<4> Modify Ethernet Parameter                                            |
|<0> Exit To Main Menu                                                    |
============================================================================
Enter your choice(0-4):
```

12. Enter **0** in the BOOTWARE OPERATION ETHERNET submenu to return to the BootWare Operation menu.
13. Enter **0** in the BootWare Operation menu to return to the EXTENDED-BOOTWARE menu.
14. Enter **0** in the EXTENDED-BOOTWARE menu to reboot the switch.

Using Xmodem to upgrade through the console port

1. Connect the console port of the switch to the PC that stores the upgrade image file.
2. Run the terminal emulation program on the PC.
3. Start the switch and access the EXTENDED-BOOTWARE menu (see "Using the EXTENDED-BOOTWARE menu").
4. Enter **7** in the EXTENDED-BOOTWARE menu to access the BootWare Operation menu.

```
=========================<BootWare Operation Menu>==========================
|Note:the operating device is flash                                       |
|<1> Backup Full BootWare                                                 |
|<2> Restore Full BootWare                                                |
|<3> Update BootWare By Serial                                            |
|<4> Update BootWare By Ethernet                                          |
|<0> Exit To Main Menu                                                    |
============================================================================
Enter your choice(0-4):
```

5. Enter **3** to access the BOOTWARE OPERATION SERIAL submenu.

```
===================<BOOTWARE OPERATION SERIAL SUB-MENU>====================
|<1> Update Full BootWare                                                 |
|<2> Update Extended BootWare                                             |
|<3> Update Basic BootWare                                                |
|<4> Modify Serial Interface Parameter                                    |
|<0> Exit To Main Menu                                                    |
============================================================================
Enter your choice(0-4):
```

6. Enter **4** to change the baud rate of the console port.

```
==============================<BAUDRATE SET>===============================
|Note:'*'indicates the current baudrate                                   |
|     Change The HyperTerminal's Baudrate Accordingly                     |
|---------------------------<Baudrate Available>--------------------------|
|<1> 9600(Default)*                                                       |
|<2> 19200                                                                |
|<3> 38400                                                                |
|<4> 57600                                                                |
```

```
|<5> 115200                                                                   |
|<0> Exit                                                                     |
================================================================================
Enter your choice(0-5):2
```

7. Enter an appropriate baud rate option. For example, enter **2** to select 19200 bps.

```
Baudrate has been changed to 19200 bps.
Please change the terminal's baudrate to 19200 bps, press ENTER when ready.
```

NOTE:

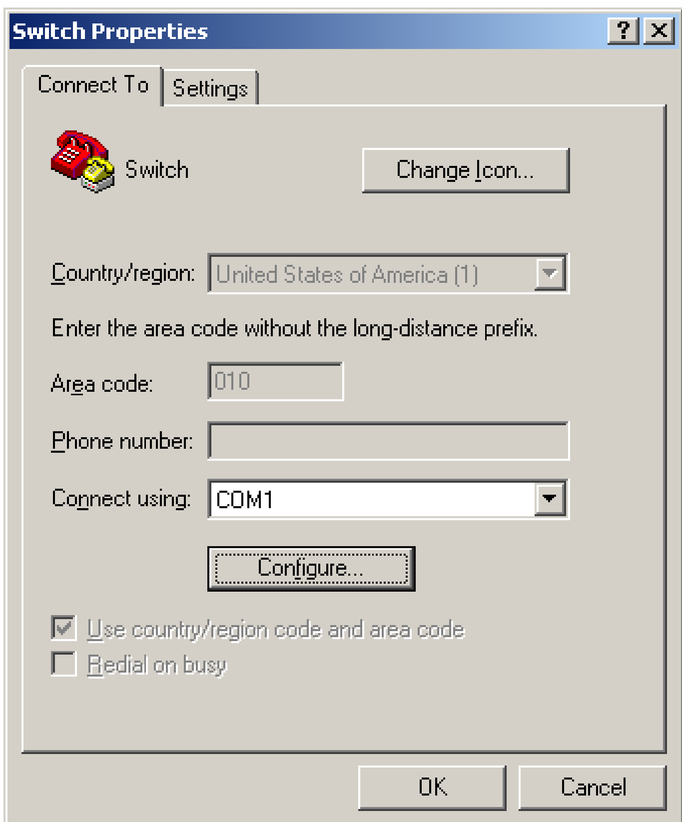
If you choose 9600 bps (the default baud rate), move to step 12.

8. Select **Call** > **Disconnect** from the HyperTerminal window to disconnect the HyperTerminal from the switch.

Figure 9 Disconnecting the HyperTerminal

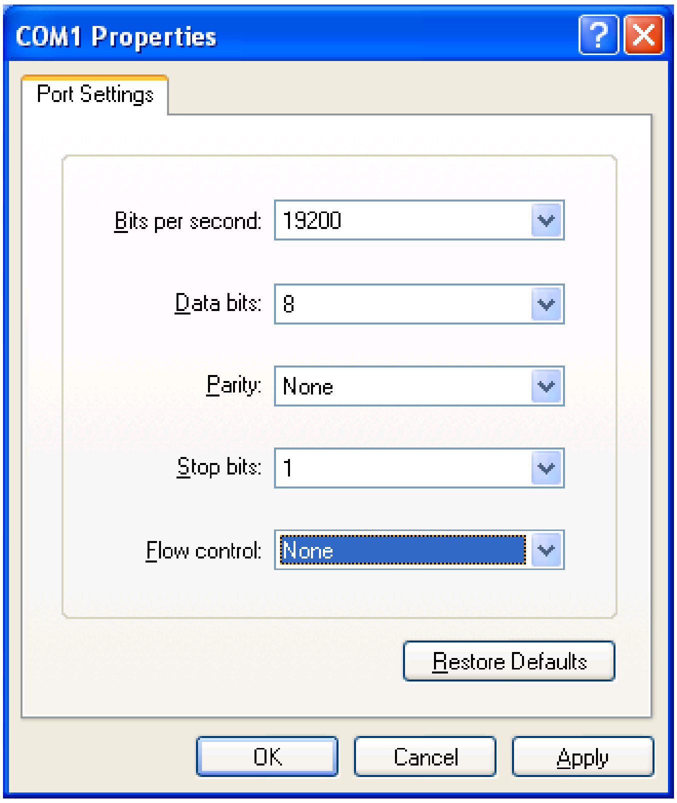
9. Select **File** > **Properties** in the HyperTerminal window, and click **Configure** in the popup dialog box.

Figure 10 Setting switch properties



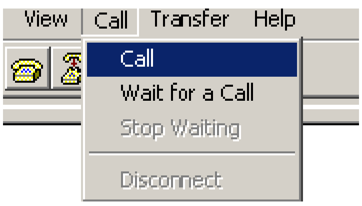
10. Select **19200** from the **Bits per second** list, and click **OK**.

Figure 11 Modifying the baud rate



11. Select **Call** > **Call** to reconnect to the switch.

Figure 12 Reconnecting to the switch



12. Press **Enter** in the BootWare interface.

```
The current baudrate is 19200 bps
===============================<BAUDRATE SET>===============================
|Note:'*'indicates the current baudrate                                    |
|     Change The HyperTerminal's Baudrate Accordingly                      |
|---------------------------<Baudrate Available>---------------------------|
|<1> 9600(Default)                                                         |
|<2> 19200*                                                                |
|<3> 38400                                                                 |
|<4> 57600                                                                 |
|<5> 115200                                                                |
|<0> Exit                                                                  |
============================================================================
Enter your choice(0-5):
```

13. Enter **0** to return to the BOOTWARE OPERATION SERIAL submenu.

```
===================<BOOTWARE OPERATION SERIAL SUB-MENU>===================
```

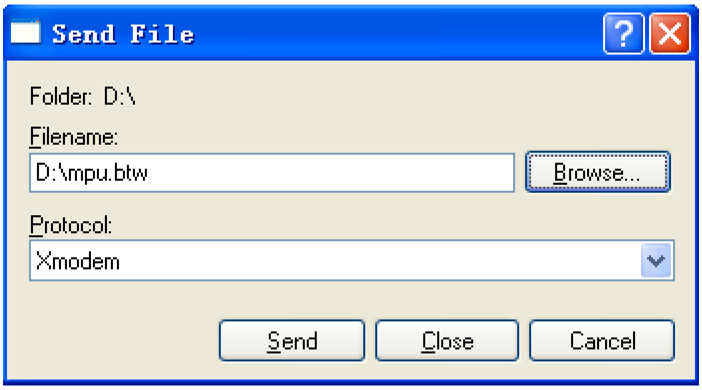
```
|<1> Update Full BootWare                                              |
|<2> Update Extended BootWare                                          |
|<3> Update Basic BootWare                                             |
|<4> Modify Serial Interface Parameter                                 |
|<0> Exit To Main Menu                                                 |
=============================================================================
Enter your choice(0-4):
```

14. Enter a number from **1** to **3** as needed. For example, enter **1** to upgrade the entire BootWare image.

```
Please Start To Transfer File, Press <Ctrl+C> To Exit.
Waiting ...CCCC
```

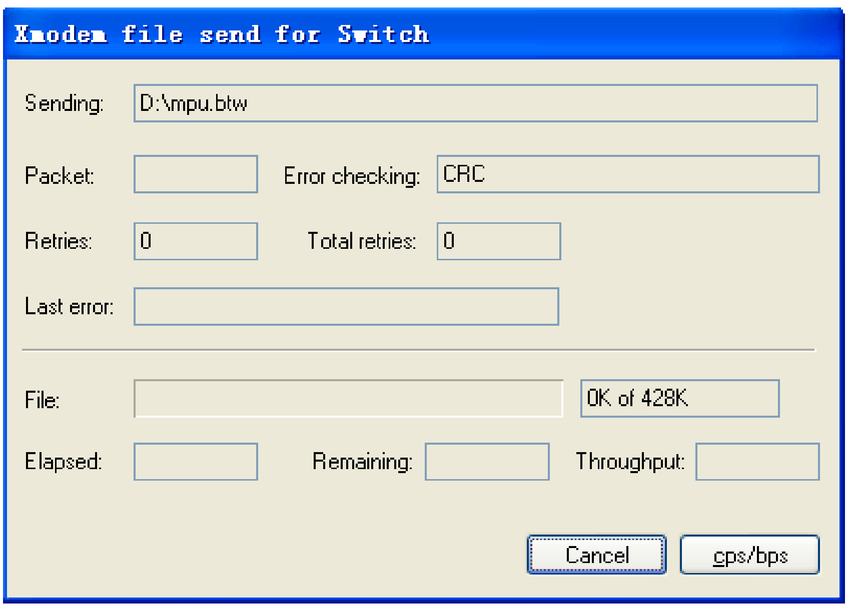
15. Select **Transfer** > **Send File** in the HyperTerminal window. In the **Send File** dialog box, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

Figure 13 Selecting the file to transfer



16. Click **Send**.

Figure 14 File transfer progress



When the file transfer is complete, the following information appears:

```
Download successfully!
447616 bytes downloaded!
```

```
Updating Basic BootWare? [Y/N]
```

17. Enter **Y** to upgrade the basic BootWare segment.

```
Updating Basic BootWare.........Done!
Updating Extended BootWare? [Y/N]
```

18. Enter **Y** to upgrade the extended BootWare segment.

```
Updating Extended BootWare.........Done!
====================<BOOTWARE OPERATION SERIAL SUB-MENU>====================
|<1> Update Full BootWare                                                  |
|<2> Update Extended BootWare                                              |
|<3> Update Basic BootWare                                                 |
|<4> Modify Serial Interface Parameter                                     |
|<0> Exit To Main Menu                                                     |
============================================================================
Enter your choice(0-4):
```

19. Enter **0** in the BOOTWARE OPERATION SERIAL submenu to return to the BootWare Operation menu.
20. Enter **0** in the BootWare Operation menu to return to the EXTENDED-BOOTWARE menu.
21. Enter **0** in the EXTENDED-BOOTWARE menu to reboot the switch.
22. Change the baud rate of the HyperTerminal back to 9600 bps, and reconnect to the switch.

NOTE:

The baud rate will restore to the default (9600 bps) at reboot. To set up a console session with the switch after a reboot, you must change the baud rate setting on the configuration terminal back to 9600 bps.

Handling upgrade failures

If an upgrade failure occurs, the switch runs the original software version.

To handle upgrade failures:

1. Verify that physical ports are connected correctly.
2. If Xmodem is used, verify that the HyperTerminal settings are correct, including the baudrate and data bits.
3. Check the HyperTerminal output for typing errors:
    - If Xmodem is used, verify that the baud rate is the same on the console port and the HyperTerminal.
    - If TFTP is used, verify that you entered the correct TFTP server IP address, filename, and file path.
    - If FTP is used, verify that you entered the correct FTP server IP address, filename, file path, and FTP username and password.
4. Verify that FTP or TFTP server software is running and has correct settings.
5. Verify that the flash memory is sufficient for storing the downloaded files.
6. Verify that the upgrading file is applicable to the switch and the file type is correct.
7. Verify that the versions of Comware software and BootWare are correct. For the compatibility between the Comware software and BootWare, see the hardware and software compatibility matrix in Release Notes.

Appendix C Using BootWare menus

You can use the BootWare menus to upgrade the switch and maintain files when the CLI is not accessible.

Accessing the BootWare menus

Table 9 lists the menus that each segment provides and the major tasks you can perform with these menus. You can access these menus only during system startup.

Table 9 BootWare menus

BootWare segment	Menu	Tasks	Reference
Basic	BASIC-BOOTWARE	• Modify serial port parameters. • Upgrade BootWare. • Start the primary or backup BootWare extended segment.	See "Using the BASIC-BOOTWARE menu."
Basic	BASIC ASSISTANT	Perform RAM test.	See "Accessing the BASIC ASSISTANT menu."
Extended	EXTENDED-BOOTWARE	• Upgrade Comware software. • Manage files. • Access the system when the console login password is lost. • Clear user privilege passwords.	See "Using the EXTENDED-BOOTWARE menu."
Extended	EXTENDED ASSISTANT	• Examine system memory. • Search system memory.	See "Using the EXTENDED ASSISTANT menu."

NOTE:

Availability of some menu options depends on the password recovery capability state. For more information about the feature and its relevant menu options, see "Disabling password recovery capability."

BootWare provides the shortcut keys in Table 10.

Table 10 BootWare shortcut keys

Shortcut key	Prompt message	Function
Ctrl+B	Press Ctrl+B to access EXTENDED-BOOTWARE MENU	Access the EXTENDED-BOOTWARE menu while the switch is starting up.
Ctrl+C	Please Start To Transfer File, Press <Ctrl+C> To Exit	Stop the ongoing file transfer and exits the current operation interface.
	Info: Press Ctrl+C to abort or return to EXTENDED ASSISTANT MENU	Return to the EXTENDED ASSISTANT menu. If the system is outputting the result of an operation, this shortcut key combination

Shortcut key	Prompt message	Function
		aborts the display first.
Ctrl+D	Press Ctrl+D to access BASIC-BOOTWARE MENU	Access the BASIC-BOOTWARE menu.
	Ctrl+D = Quit	Exit the parameter settings menu.
Ctrl+E	Memory Test(press Ctrl+C to skip it,press Ctrl+E to ECHO INFO)	Display the test process.
Ctrl+F	Ctrl+F: Format File System	Format the current storage medium from the EXTENDED-BOOTWARE menu.
Ctrl+T	Press Ctrl+T to start memory test	Start a RAM test before the extended BootWare segment starts to run.
Ctrl+U	Access BASIC ASSISTANT MENU	Access the BASIC ASSISTANT menu from the BASIC-BOOTWARE menu.
Ctrl+V	Press Ctrl+V to start heavy memory test	Perform a memory pressure test from the BASIC-BOOTWARE menu.
Ctrl+Z	Ctrl+Z: Access EXTENDED ASSISTANT MENU	Access the EXTENDED ASSISTANT menu from the EXTENDED-BOOTWARE menu.

Using the BASIC-BOOTWARE menu

To access the BASIC-BOOTWARE menu:

1. Power on the switch.
2. Press **Ctrl+D** within 4 seconds after the "Press Ctrl+D to access BASIC-BOOTWARE MENU" prompt message appears. If you fail to do this within the time limit, the system starts to run the extended BootWare segment.

```
======================<BASIC-BOOTWARE MENU(Ver 1.03)>=======================
|<1> Modify Serial Interface Parameter                                     |
|<2> Update Extended BootWare                                              |
|<3> Update Full BootWare                                                  |
|<4> Boot Extended BootWare                                                |
|<5> Boot Backup Extended BootWare                                         |
|<0> Reboot                                                                |
============================================================================
Ctrl+U: Access BASIC ASSISTANT MENU
Enter your choice(0-5):
```

Table 11 BASIC-BOOTWARE menu options

Option	Task
<1> Modify Serial Interface Parameter	Change the baud rate of the console port. Perform this task before downloading an image through the console port for software upgrade.
<2> Update Extended BootWare	Update the extended BootWare segment. If the extended segment is corrupted, choose this option to repair it.
<3> Update Full BootWare	Update the entire BootWare, including the basic segment and the extended segment.

Option	Task
<4> Boot Extended BootWare	Run the primary extended BootWare segment.
<5> Boot Backup Extended BootWare	Run the backup extended BootWare segment.
<0> Reboot	Reboot the switch.
Ctrl+U: Access BASIC ASSISTANT MENU	Press **Ctrl+U** to access the BASIC ASSISTANT menu. In this menu, you can perform RAM tests.

Modifying serial port parameters

When you use the console port to access the system, make sure the port parameters are consistent with the serial port settings on the configuration terminal, including the baud rate, data bits, parity check, stop bits, flow control, and emulation. If the settings are inconsistent, communication will fail.

You can change the baud rate from the BootWare menus. HPE recommends that you change the default baud rate (9600 bps) to a higher baud rate for faster file transfer before downloading a Comware image file with XMODEM through the console port.

To change the baud rate of the console port:

1. Enter **1** in the BASIC-BOOTWARE menu.

```
Enter your choice(0-5): 1
===============================<BAUDRATE SET>===============================
|Note:'*'indicates the current baudrate                                    |
|     Change The HyperTerminal's Baudrate Accordingly                      |
|---------------------------<Baudrate Available>--------------------------|
|<1> 9600(Default)*                                                        |
|<2> 19200                                                                 |
|<3> 38400                                                                 |
|<4> 57600                                                                 |
|<5> 115200                                                                |
|<0> Exit                                                                  |
============================================================================
Enter your choice(0-5):
```

2. Enter the number that represents the baud rate you want to choose. For example, enter **5** to set the baud rate to 115200 bps.

NOTE:

The baud rate change is a one-time operation. The baud rate will restore to the default (9600 bps) at reboot. To set up a console session with the switch after a reboot, you must change the baud rate setting on the configuration terminal back to 9600 bps.

Updating the extended BootWare segment

If the extended BootWare segment is corrupted, enter **2** in the BASIC-BOOTWARE menu to update it.

```
Enter your choice(0-5): 2
Please Start To Transfer File, Press <Ctrl+C> To Exit.
Waiting ...CCCCC
```

Updating the entire BootWare

To update the entire BootWare, enter **3** in the BASIC-BOOTWARE menu.

```
Enter your choice(0-5): 3
Please Start To Transfer File, Press <Ctrl+C> To Exit.
Waiting ...CCCCC
```

Running the primary extended BootWare segment

To bootstrap the Comware images with the primary extended BootWare segment, enter **4** in the BASIC-BOOTWARE menu.

```
Enter your choice(0-5): 4
Booting Normal Extended BootWare.
The Extended BootWare is self-decompressing..................................
.......Done.

****************************************************************************
*                                                                          *
*                          BootWare, Version 1.09                          *
*                                                                          *
****************************************************************************
Compiled Date       : Feb  1 2013
CPU Type            : P2020
CPU L1 Cache        : 32KB
CPU L2 Cache        : 512KB
CPU Clock Speed     : 1200MHz
Memory Type         : DDR3 SDRAM
Memory Size         : 2048MB
Memory Speed        : 800MHz
BootWare Size       : 1024KB
Flash Size          : 512MB
CPLD Version        : 003
PCB Version         : Ver.A


BootWare Validating...
Press Ctrl+B to access EXTENDED-BOOTWARE MENU...

Password recovery capability is enabled.
Note: The current operating device is flash
Enter < Storage Device Operation > to select device.
```

Running the backup extended BootWare segment

To bootstrap the Comware images with the backup extended BootWare segment, enter **5** in the BASIC-BOOTWARE menu. For information about backing up the extended BootWare segment, see "Managing the BootWare image."

```
Enter your choice(0-5): 5
Booting Backup Extended BootWare.
```

```
The Extended BootWare is self-decompressing...................................
....Done.
```

Accessing the BASIC ASSISTANT menu

IMPORTANT:

Memory tests must be performed under the guidance of HPE technical support engineers.

To access the BASIC ASSISTANT menu, press **Ctrl+U** while you are in the BASIC-BOOTWARE menu.

```
===========================<BASIC ASSISTANT MENU>===========================
|<1> RAM Test                                                              |
|<0> Exit To Main Menu                                                     |
============================================================================
Enter your choice(0-1):
```

Table 12 BASIC ASSISTANT menu

Option	Task
<1> RAM Test	Perform a RAM test.
<0> Exit to Main Menu	Return to the BASIC-BOOTWARE menu.

To perform a RAM test, press **Ctrl+T** within 4 seconds after the prompt message "Press Ctrl+T to start memory test" appears.

To perform a RAM pressure test, press **Ctrl+V** within 4 seconds after the prompt message "Press Ctrl+V to start heavy memory test" appears.

Using the EXTENDED-BOOTWARE menu

To access the EXTENDED-BOOTWARE menu:

1. Reboot the switch or run the primary or backup extended BootWare segment from the BASIC-BOOTWARE menu.
2. Press **Ctrl+B** within 5 seconds after the "Press Ctrl+B to access EXTENDED-BOOTWARE MENU..." prompt message appears. If you fail to do this, the system starts decompressing the Comware software images.

   ```
   Password recovery capability is enabled.
   Note: The current operating device is flash
   Enter < Storage Device Operation > to select device.
   ```

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

   The EXTENDED-BOOTWARE menu appears.

   ```
   ===========================<EXTENDED-BOOTWARE MENU>=========================
   |<1> Boot System                                                           |
   |<2> Enter Serial SubMenu                                                  |
   |<3> Enter Ethernet SubMenu                                                |
   |<4> File Control                                                          |
   |<5> Restore to Factory Default Configuration                              |
   |<6> Skip Current System Configuration                                     |
   |<7> BootWare Operation Menu                                               |
   |<8> Skip Authentication for Console Login                                 |
   ```

```
|<9> Storage Device Operation                                                |
|<0> Reboot                                                                  |
=============================================================================
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format File System
Enter your choice(0-9):
```

Availability of some options in this menu depends on the password recovery capability state (displayed on top of the EXTENDED-BOOTWARE menu). For more information about the feature, see "Disabling password recovery capability."

Table 13 EXTENDED-BOOTWARE menu options

Option	Tasks	Reference
<1> Boot System	Run the Comware software without rebooting the switch. Choose this option after completing operations in the EXTENDED-BOOTWARE menu.	N/A
<2> Enter Serial SubMenu	Use Xmodem to upgrade Comware software through the console port.	See "Upgrading Comware software through the console port."
<3> Enter Ethernet SubMenu	Use FTP or TFTP to upgrade Comware software through the management Ethernet interface.	See "Upgrading Comware software through an Ethernet port."
<4> File Control	• Display files on the current storage medium. • Set a Comware image file as the main or backup startup software image. • Delete files to free storage space.	See "Managing files."
<5> Restore to Factory Default Configuration	Restore the factory-default configuration. This option is available only if password recovery capability is disabled.	See "Restoring the factory-default configuration."
<6> Skip Current System Configuration	Start the switch with the factory-default configuration without loading any configuration file. This is a one-time operation and takes effect only for the first system startup or reboot after you choose this option. This option is available only if password recovery capability is enabled.	See "Starting up without loading the configuration file."
<7> BootWare Operation Menu	Back up, recover, and upgrade the BootWare image.	See "Managing the BootWare image."
<8> Skip Authentication for Console Login	Skip console login authentication. This option is available only if password recovery capability is enabled.	See "Skipping console login authentication."
<9> Storage Device Operation	Set the storage medium from which	See "Managing storage

Option	Tasks	Reference
	the switch will start up. Set the storage medium where file operations are performed. This storage medium is referred to as the "current storage medium" in this chapter.	media."
Ctrl+Z: Access EXTENDED ASSISTANT MENU	Access the EXTENDED ASSISTANT menu.	See "Using the EXTENDED ASSISTANT menu."
Ctrl+F: Format File System	Format the file system.	See "Formatting the file system."
<0> Reboot	Reboot the switch.	N/A

Disabling password recovery capability

Password recovery capability controls console user access to the device configuration and SDRAM from BootWare menus.

If password recovery capability is enabled, console users can perform the following tasks:

- If console users forget their user privilege level passwords, they can skip the current configuration file to configure new passwords.
- If console users forget their console login passwords, they can skip login authentication or the current configuration file to configure new passwords.

If password recovery capability is disabled, console users must restore the factory-default configuration before they can configure new passwords. Restoring the factory-default configuration deletes the next-startup configuration files.

To enhance system security, disable password recovery capability.

To disable password recovery capability:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Disable password recovery capability.	**undo password-recovery enable**	By default, password recovery capability is enabled.

NOTE:

To avoid version compatibility problems, use compatible Comware software and BootWare.

Running the Comware software

To run the Comware software after completing all operations, enter **1** in the EXTENDED-BOOTWARE menu.

```
Enter your choice(0-9): 1
Loading the main image files...
Loading file flash:/system.bin..............................................
.........Done.
Loading file flash:/boot.bin..............Done.
```

```
Image file flash:/boot.bin is self-decompressing....
............................................................................
............................................................................
............................................................................
............................................................................
............................................................................
............................................................................
............................................................................
............................................................................
............................................................................
............................................................................
............................................................................
............................................................................
............................................................................
................................Done.
System image is starting...

Waiting for StackBoard to insert, this process may occupy time up to 300 seconds
.

STM Init Start.
User interface aux1/1 is available.

Press ENTER to get started.
```

Upgrading Comware software through the console port

You can upgrade the Comware software through the console port or modify the baud rate of the console port from the Serial submenu.

To upgrade Comware software through the console port, enter **2** in the EXTENDED-BOOTWARE menu to access the Serial submenu.

```
Enter your choice(0-9): 2
===========================<Enter Serial SubMenu>===========================
|Note:the operating device is flash                                        |
|<1> Download Image  Program To SDRAM And Run                              |
|<2> Update Main Image File                                                |
|<3> Update Backup Image File                                              |
|<4> Modify Serial Interface Parameter                                     |
|<0> Exit To Main Menu                                                     |
============================================================================
Enter your choice(0-4):
```

Table 14 Serial submenu options

Option	Tasks
<1> Download Image Program To SDRAM And Run	Load and run a Comware software image in SDRAM. If password recovery capability is disabled, this option is not available.
<2> Update Main Image File	Download a Comware software image to the current storage

Option	Tasks
	medium as the main image (the file attribute is set to M). If a main system image already exists, the M file attribute of the original image is removed.
<3> Update Backup Image File	Download a Comware software image to the current storage medium as the backup image (the file attribute is set to B). If a backup system image already exists, the B file attribute of the original image is removed.
<4> Modify Serial Interface Parameter	Change the baud rate of the console port. The baud rate change is a one-time operation. The baud rate will restore to the default (9600 bps) at reboot. To set up a console session with the switch after a reboot, you must change the baud rate setting on the configuration terminal to 9600 bps.
<0> Exit To Main Menu	Return to the EXTENDED-BOOTWARE menu.

NOTE:

To set the current storage medium, see "Managing storage media."

Upgrading Comware software through an Ethernet port

You can upgrade Comware software with FTP or TFTP through an Ethernet port from the Ethernet submenu.

To update Comware software through an Ethernet port from the Ethernet submenu:

1. Enter **3** in the EXTENDED-BOOTWARE menu to access the Ethernet submenu.

```
Enter your choice(0-9):3
==========================<Enter Ethernet SubMenu>==========================
|Note:the operating device is flash                                        |
|<1> Download Image Program To SDRAM And Run                               |
|<2> Update Main Image File                                                |
|<3> Update Backup Image File                                              |
|<4> Modify Ethernet Parameter                                             |
|<0> Exit To Main Menu                                                     |
|<Ensure The Parameter Be Modified Before Downloading!>                    |
============================================================================
Enter your choice(0-4):
```

Table 15 Ethernet submenu options

Option	Tasks
<1> Download Image Program To SDRAM And Run	Load and run a Comware software image in SDRAM. If password recovery capability is disabled, this option is not available.
<2> Update Main Image File	Download a Comware software image to the current storage medium as the main image (the file attribute is set to M). If a main system image already exists, the M file attribute of the original image is removed.
<3> Update Backup Image File	Download a Comware software image to the current storage medium as the backup image (the file attribute

Option	Tasks
	is set to B). If a backup system image already exists, the B file attribute of the original image is removed.
<4> Modify Ethernet Parameter	Configure FTP or TFTP file transfer settings.
<0> Exit To Main Menu	Return to the EXTENDED-BOOTWARE menu.

2. Enter **4** in the Ethernet submenu to configure file transfer settings.

```
Enter your choice(0-4):4
=========================<ETHERNET PARAMETER SET>=========================
|Note:       '.' = Clear field.                                          |
|            '-' = Go to previous field.                                 |
|          Ctrl+D = Quit.                                                |
==========================================================================
Protocol (FTP or TFTP) :tftp
Load File Name         :newest.ipe
                       :
Target File Name       :newest.ipe
                       :
Server IP Address      :192.168.0.23
Local IP Address       :192.168.0.105
Subnet Mask            :255.255.255.0
Gateway IP Address     :0.0.0.0
```

Table 16 Setting file transfer parameters

Field	Description
'.' = Clear field	Press the dot (.), and then press **Enter** to clear the setting for a field.
'-' = Go to previous field	Press the hyphen (-), and then press **Enter** to return to the previous field.
Ctrl+D = Quit	Press **Ctrl**+**D** to exit the Ethernet parameter settings menu.
Protocol (FTP or TFTP)	Set the file transfer protocol to FTP or TFTP.
Load File Name	Set the name of the file to be downloaded.
Target File Name	Set a file name for saving the file in the current storage medium on the switch. The target file name must have the same suffix as the source file. By default, the target file name is the same as the source file name.
Server IP Address	Set the IP address of the FTP or TFTP server. If a mask must be set, use a colon (:) to separate the mask length from the IP address. For example, 192.168.2.26:24.
Local IP Address	Set the IP address of the switch.
Subnet Mask	Set the IP subnet mask of the switch.
Gateway IP Address	Set a gateway IP address if the switch is on a different network than the server.
FTP User Name	Set the username for accessing the FTP server. This username must be the same as the one configured on the FTP server. This

Field	Description
	field is not available for TFTP.
FTP User Password	Set the password for accessing the FTP server. This password must be the same as the one configured on the FTP server. This field is not available for TFTP.

Managing files

To change the type of a Comware software image, retrieve files, or delete files, enter **4** in the EXTENDED-BOOTWARE menu.

```
Enter your choice(0-9):4
```

The following File CONTROL submenu appears:

```
===============================<File CONTROL>===============================
|Note:the operating device is flash                                        |
|<1> Display All File(s)                                                   |
|<2> Set Image File type                                                   |
|<3> Delete File                                                           |
|<0> Exit To Main Menu                                                     |
============================================================================
Enter your choice(0-3):
```

Table 17 File CONTROL submenu options

Option	Task
<1> Display All File(s)	Display all files on the current storage medium.
<2> Set Image File type	Set the type of a Comware software image.
<3> Delete File	Delete a file from the current storage medium.
<0> Exit To Main Menu	Return to the EXTENDED-BOOTWARE menu.

Displaying all files

To display all files on the current storage medium, enter **1** in the File CONTROL submenu:

```
Enter your choice(0-3):1
Display all file(s) in flash:
 'M' = MAIN      'B' = BACKUP      'S' = SECURE      'N/A' = NOT ASSIGNED
============================================================================
|NO. Size(B)   Time                 Type   Name                            |
|1   40        Jan/01/2011 03:22:39 N/A    flash:/database.dhcp            |
|2   8         Jan/01/2011 05:14:40 N/A    flash:/test.txt                 |
|3   309754    Jan/01/2011 01:43:54 N/A    flash:/123                      |
|4   73220     Jan/01/2011 00:40:22 N/A    flash:/startup.mdb              |
|5   32973824  Jan/01/2011 01:14:01 N/A    flash:/6125xlg-cmw710-system-t23|
|02.bin                                                                    |
|6   11035648  Jan/01/2011 01:13:49 N/A    flash:/6125xlg-cmw710-boot-R2306|
|.bin                                                                      |
|7   43984896  Jan/01/2011 00:03:43 N/A    flash:/6125xlg.ipe              |
|8   60606464  Jan/07/2013 11:02:10 N/A    flash:/6125xlg-cmw710-system-a23|
```

```
|00.bin                                                                |
|9   3397      Jan/01/2011 00:40:22 M      flash:/startup.cfg          |
|10  12175360  Jan/07/2013 11:02:10 N/A    flash:/6125xlg-cmw710-boot-a2300|
|.bin                                                                  |
|11  0         Jan/01/2011 03:07:36 N/A    flash:/.trash/.trashinfo    |
|12  5         Jan/01/2011 05:15:01 N/A    flash:/.nickname            |
|13  20        Jan/03/2011 09:13:47 N/A    flash:/.snmpboots           |
|14  63        Jan/01/2011 03:04:20 N/A    flash:/test1.txt            |
|15  32985088  Jan/01/2011 00:09:09 M      flash:/6125xlg-cmw710-system-t23|
|02001.bin                                                             |
|16  0         Jan/01/2011 01:43:15 N/A    flash:/lauth.dat            |
|17  536       Jan/01/2011 00:54:25 N/A    flash:/versionInfo/version0.dat |
|18  8         Jan/01/2011 00:54:25 N/A    flash:/versionInfo/versionCtl.da|
|t                                                                     |
|19  536       Jan/01/2011 01:16:03 N/A    flash:/versionInfo/version1.dat |
|20  536       Jan/01/2011 00:11:41 N/A    flash:/versionInfo/version2.dat |
|21  641555    Jan/01/2011 01:15:29 N/A    flash:/logfile/logfile.log  |
|22  18        Jan/03/2011 09:13:42 N/A    flash:/.pathfile            |
|23  789       Jan/03/2011 09:13:42 N/A    flash:/license/DeviceID.did |
|24  789       Jan/01/2011 03:25:36 N/A    flash:/license/history/DeviceID_|
|20110101032536.did                                                    |
|25  789       Jan/01/2011 00:00:17 N/A    flash:/license/history/DeviceID_|
|20110101000017.did                                                    |
|26  789       Jan/01/2011 00:45:15 N/A    flash:/license/history/DeviceID_|
|20110101004515.did                                                    |
|27  789       Jan/01/2011 00:22:25 N/A    flash:/license/history/DeviceID_|
|20110101002225.did                                                    |
|28  789       Jan/03/2011 09:13:42 N/A    flash:/license/history/DeviceID_|
|20110103091342.did                                                    |
|29  789       Jan/03/2011 03:09:31 N/A    flash:/license/history/DeviceID_|
|20110103030931.did                                                    |
|30  789       Jan/01/2011 00:00:16 N/A    flash:/license/history/DeviceID_|
|20110101000016.did                                                    |
|31  789       Jan/03/2011 02:39:04 N/A    flash:/license/history/DeviceID_|
|20110103023904.did                                                    |
|32  789       Jan/03/2011 02:35:43 N/A    flash:/license/history/DeviceID_|
|20110103023543.did                                                    |
|33  789       Jan/01/2011 03:10:07 N/A    flash:/license/history/DeviceID_|
|20110101031007.did                                                    |
|34  789       Jan/03/2011 02:33:50 N/A    flash:/license/history/DeviceID_|
|20110103023350.did                                                    |
|35  789       Jan/01/2011 01:16:00 N/A    flash:/license/history/DeviceID_|
|20110101011600.did                                                    |
|36  789       Jan/01/2011 02:44:29 N/A    flash:/license/history/DeviceID_|
|20110101024429.did                                                    |
|37  10992640  Jan/01/2011 00:08:58 M      flash:/6125xlg-cmw710-boot-R2306|
|001.bin                                                               |
|38  989       Jan/01/2011 00:40:22 N/A    flash:/ifindex.dat          |
```

```
|39  70699     Jan/01/2011 09:52:59 N/A    flash:/archive/my_archive_18.mdb|
|40  4827      Jan/01/2011 09:52:59 N/A    flash:/archive/my_archive_18.cfg|
|41  70255     Jan/01/2011 09:42:58 N/A    flash:/archive/my_archive_17.mdb|
|42  4874      Jan/01/2011 09:42:58 N/A    flash:/archive/my_archive_17.cfg|
|43  70123     Jan/01/2011 09:32:57 N/A    flash:/archive/my_archive_16.mdb|
|44  4758      Jan/01/2011 09:32:57 N/A    flash:/archive/my_archive_16.cfg|
|45  61346     Jan/01/2011 09:22:56 N/A    flash:/archive/my_archive_15.mdb|
|46  4480      Jan/01/2011 09:22:56 N/A    flash:/archive/my_archive_15.cfg|
|47  61346     Jan/01/2011 09:12:55 N/A    flash:/archive/my_archive_14.mdb|
|48  4346      Jan/01/2011 09:12:55 N/A    flash:/archive/my_archive_14.cfg|
============================================================================
```

Changing the Comware software image type

To change the type of a Comware software image:

1. Enter **2** in the File CONTROL submenu.

```
===============================<File CONTROL>===============================
|Note:the operating device is flash                                        |
|<1> Display All File(s)                                                   |
|<2> Set Image File type                                                   |
|<3> Delete File                                                           |
|<0> Exit To Main Menu                                                     |
============================================================================
Enter your choice(0-3):2

'M' = MAIN      'B' = BACKUP      'S' = SECURE      'N/A' = NOT ASSIGNED
============================================================================
|NO. Size(B)   Time                 Type   Name                            |
|1   32973824  Jan/01/2011 01:14:01 N/A    flash:/6125xlg-cmw710-system-t23|
|02.bin                                                                    |
|2   11035648  Jan/01/2011 01:13:49 N/A    flash:/6125xlg-cmw710-boot-R2306|
|.bin                                                                      |
|3   60606464  Jan/07/2013 11:02:10 N/A    flash:/6125xlg-cmw710-system-a23|
|00.bin                                                                    |
|4   12175360  Jan/07/2013 11:02:10 N/A    flash:/6125xlg-cmw710-boot-a2300|
|.bin                                                                      |
|5   32985088  Jan/01/2011 00:09:09 M      flash:/6125xlg-cmw710-system-t23|
|02001.bin                                                                 |
|6   10992640  Jan/01/2011 00:08:58 M      flash:/6125xlg-cmw710-boot-R2306|
|001.bin                                                                   |
|0   Exit                                                                  |
============================================================================
```

2. Enter the file number of the file you are working with.

```
Enter file No.:1

Modify the file attribute:
============================================================================
|<1> +Main                                                                 |
|<2> -Main                                                                 |
|<3> +Backup                                                               |
```

```
|<4> -Backup                                                                 |
|<0> Exit                                                                    |
==============================================================================
Enter your choice(0-4):
```

3. Enter a number in the range of 1 to 4 to add or delete a file attribute for the file. For example, enter **1** to set the file as the main startup image file.

```
Enter your choice(0-4):1
This operation may take several minutes. Please wait....
Set the file attribute success!
```

Deleting a file

To delete a file when the storage medium is insufficient:

1. Enter **3** in the File CONTROL menu.

```
Enter your choice(0-3):3
Deleting the file in flash:
 'M' = MAIN      'B' = BACKUP      'S' = SECURE      'N/A' = NOT ASSIGNED
==============================================================================
|NO. Size(B)   Time                 Type   Name                             |
|1   40        Jan/01/2011 03:22:39 N/A    flash:/database.dhcp             |
|2   8         Jan/01/2011 05:14:40 N/A    flash:/test.txt                  |
|3   309754    Jan/01/2011 01:43:54 N/A    flash:/123                       |
|4   73220     Jan/01/2011 00:40:22 N/A    flash:/startup.mdb               |
|5   32973824  Jan/01/2011 01:14:01 M      flash:/6125xlg-cmw710-system-t23|
|02.bin                                                                      |
|6   11035648  Jan/01/2011 01:13:49 N/A    flash:/6125xlg-cmw710-boot-R2306|
|.bin                                                                        |
|7   43984896  Jan/01/2011 00:03:43 N/A    flash:/6125xlg.ipe               |
|8   60606464  Jan/07/2013 11:02:10 N/A    flash:/6125xlg-cmw710-system-a23|
|00.bin                                                                      |
|9   3397      Jan/01/2011 00:40:22 M      flash:/startup.cfg               |
|10  12175360  Jan/07/2013 11:02:10 N/A    flash:/6125xlg-cmw710-boot-a2300|
|.bin                                                                        |
|11  0         Jan/01/2011 03:07:36 N/A    flash:/.trash/.trashinfo         |
|12  5         Jan/01/2011 05:15:01 N/A    flash:/.nickname                 |
|13  20        Jan/03/2011 09:13:47 N/A    flash:/.snmpboots                |
|14  63        Jan/01/2011 03:04:20 N/A    flash:/test1.txt                 |
|15  32985088  Jan/01/2011 00:09:09 N/A    flash:/6125xlg-cmw710-system-t23|
|02001.bin                                                                   |
|16  0         Jan/01/2011 01:43:15 N/A    flash:/lauth.dat                 |
|17  536       Jan/01/2011 00:54:25 N/A    flash:/versionInfo/version0.dat |
|18  8         Jan/01/2011 00:54:25 N/A    flash:/versionInfo/versionCtl.da|
|t                                                                           |
|19  536       Jan/01/2011 01:16:03 N/A    flash:/versionInfo/version1.dat |
|20  536       Jan/01/2011 00:11:41 N/A    flash:/versionInfo/version2.dat |
|21  641555    Jan/01/2011 01:15:29 N/A    flash:/logfile/logfile.log       |
|22  18        Jan/03/2011 09:13:42 N/A    flash:/.pathfile                 |
|23  789       Jan/03/2011 09:13:42 N/A    flash:/license/DeviceID.did      |
|24  789       Jan/01/2011 03:25:36 N/A    flash:/license/history/DeviceID_|
|20110101032536.did                                                          |
```

```
|25  789       Jan/01/2011 00:00:17 N/A    flash:/license/history/DeviceID_|
|20110101000017.did                                                         |
|26  789       Jan/01/2011 00:45:15 N/A    flash:/license/history/DeviceID_|
|20110101004515.did                                                         |
|27  789       Jan/01/2011 00:22:25 N/A    flash:/license/history/DeviceID_|
|20110101002225.did                                                         |
|28  789       Jan/03/2011 09:13:42 N/A    flash:/license/history/DeviceID_|
|20110103091342.did                                                         |
|29  789       Jan/03/2011 03:09:31 N/A    flash:/license/history/DeviceID_|
|20110103030931.did                                                         |
|30  789       Jan/01/2011 00:00:16 N/A    flash:/license/history/DeviceID_|
|20110101000016.did                                                         |
|31  789       Jan/03/2011 02:39:04 N/A    flash:/license/history/DeviceID_|
|20110103023904.did                                                         |
|32  789       Jan/03/2011 02:35:43 N/A    flash:/license/history/DeviceID_|
|20110103023543.did                                                         |
|33  789       Jan/01/2011 03:10:07 N/A    flash:/license/history/DeviceID_|
|20110101031007.did                                                         |
|34  789       Jan/03/2011 02:33:50 N/A    flash:/license/history/DeviceID_|
|20110103023350.did                                                         |
|35  789       Jan/01/2011 01:16:00 N/A    flash:/license/history/DeviceID_|
|20110101011600.did                                                         |
|36  789       Jan/01/2011 02:44:29 N/A    flash:/license/history/DeviceID_|
|20110101024429.did                                                         |
|37  10992640  Jan/01/2011 00:08:58 M      flash:/6125xlg-cmw710-boot-R2306|
|001.bin                                                                    |
|38  989       Jan/01/2011 00:40:22 N/A    flash:/ifindex.dat               |
|39  70699     Jan/01/2011 09:52:59 N/A    flash:/archive/my_archive_18.mdb|
|40  4827      Jan/01/2011 09:52:59 N/A    flash:/archive/my_archive_18.cfg|
|41  70255     Jan/01/2011 09:42:58 N/A    flash:/archive/my_archive_17.mdb|
|42  4874      Jan/01/2011 09:42:58 N/A    flash:/archive/my_archive_17.cfg|
|43  70123     Jan/01/2011 09:32:57 N/A    flash:/archive/my_archive_16.mdb|
|44  4758      Jan/01/2011 09:32:57 N/A    flash:/archive/my_archive_16.cfg|
|45  61346     Jan/01/2011 09:22:56 N/A    flash:/archive/my_archive_15.mdb|
|46  4480      Jan/01/2011 09:22:56 N/A    flash:/archive/my_archive_15.cfg|
|47  61346     Jan/01/2011 09:12:55 N/A    flash:/archive/my_archive_14.mdb|
|48  4346      Jan/01/2011 09:12:55 N/A    flash:/archive/my_archive_14.cfg|
|0   Exit                                                                   |
============================================================================
Enter file No.:
```

2. Enter the file number of the file to delete. For example, enter **3** to delete flash:/123.

```
Enter file No: 3
```

3. Enter **Y** at the prompt to confirm the deletion.

```
The file you selected is flash:/123,Delete it? [Y/N]
Deleting.....Done!
```

NOTE:

For information about managing files from the CLI, see *HPE 6125XLG Blade Switch Series Fundamentals Configuration Guide*.

Restoring the factory-default configuration

CAUTION:

Performing this task can cause all next-startup configuration files to be permanently deleted.

To restore the factory-default configuration from the EXTENDED-BOOTWARE menu, make sure password recovery capability is disabled. If the capability is enabled, you cannot perform the task.

Disabling password recovery capability can protect your system from unauthorized console access to configuration. However, if you have only console access to the system but you have lost the console login password, you can only access the system after restoring the factory-default configuration.

To enable the system to start up with the factory-default configuration instead of a next-startup configuration file:

1. Enter **5** in the EXTENDED-BOOTWARE menu.
```
Enter your choice(0-9):5
```
2. Follow the system instruction to complete the task:
   - If password recovery capability is enabled, first disable the capability from the CLI, and then reboot the switch to access the EXTENDED-BOOTWARE menu.
   ```
   Password recovery capability is enabled. To perform this operation, first
   disable the password recovery capability using the undo password-recovery
   enable command in CLI.
   ```
   - If password recovery capability is disabled, enter **Y** at the prompt to complete the task.
   ```
   Because the password recovery capability is disabled, this operation can
   cause the configuration files to be deleted, and the system will start up
   with factory defaults. Are you sure to continue?[Y/N]Y
   Setting...Done.
   ```

Starting up without loading the configuration file

You can perform this task only if password recovery capability is enabled.

To ignore all configuration files and start up with the factory-default configuration, enter **6** in the EXTENDED-BOOTWARE menu.

```
Enter your choice(0-9): 6
Flag Set Success.
```

This is a one-time operation. It takes effect only for the first system reboot (option **1** or option **0** in the EXTENDED-BOOTWARE menu) after you select the option.

Managing the BootWare image

You can use BootWare Operation menu to back up, recover, and upgrade the BootWare image.

To access the BootWare Operation menu, enter **7** in the EXTENDED-BOOTWARE menu.

```
Enter your choice(0-9): 7
=======================<BootWare Operation Menu>=========================
```

```
|Note:the operating device is flash                                          |
|<1> Backup Full BootWare                                                    |
|<2> Restore Full BootWare                                                   |
|<3> Update BootWare By Serial                                               |
|<4> Update BootWare By Ethernet                                             |
|<0> Exit To Main Menu                                                       |
============================================================================
Enter your choice(0-4):
```

Table 18 BootWare Operation menu options

Option	Tasks
<1> Backup Full BootWare	Back up the entire BootWare image. When the BootWare image is corrupted, you could use the backup image for recovery.
<2> Restore Full BootWare	Recover the entire BootWare image. If the BootWare image is corrupted, you can use a backup BootWare image to recover it.
<3> Update BootWare By Serial	Update the BootWare from the console port.
<4> Update BootWare By Ethernet	Update the BootWare from an Ethernet port.
<0> Exit To Main Menu	Return to the EXTENDED-BOOTWARE menu.

Skipping console login authentication

IMPORTANT:

- To perform this task, make sure password recovery capability is enabled. If the capability is disabled, you cannot perform this task.
- Skipping console login authentication applies only to console login users.
- Skipping console login authentication is a one-time operation. It takes effective only on the first reboot (option **1** and option **0** on the EXTENDED-BOOTWARE menu) after you perform the operation. If you do not configure a new login password, the original setting continues to take effect for the subsequent reboot.

If you forget the console login password, enter **8** in the EXTENDED-BOOTWARE menu so you can log in to the switch through the console port without login authentication.

```
Enter your choice(0-9): 8
```

Managing storage media

To get information about available storage media, and set the storage medium you want to use for file operations, enter **9** in the EXTENDED-BOOTWARE menu.

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

The following DEVICE CONTROL menu appears:

```
==============================<DEVICE CONTROL>==============================
|<1> Display All Available Nonvolatile Storage Device(s)                     |
|<2> Set The Operating Device                                                |
|<3> Set The Default Boot Device                                             |
|<0> Exit To Main Menu                                                       |
============================================================================
```

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

Table 19 DEVICE CONTROL menu options

Option	Task
<1> Display All Available Nonvolatile Storage Device(s)	Display all available nonvolatile storage media.
<2> Set The Operating Device	Set the current storage medium. All file operations performed using BootWare menus are performed on the current storage medium.
<3> Set The Default Boot Device	Set the default storage medium from which the system will start up.
<0> Exit To Main Menu	Return to the EXTENDED-BOOTWARE menu.

Using the EXTENDED ASSISTANT menu

In the EXTENDED-BOOTWARE menu, press **Ctrl+Z** to access the EXTENDED ASSISTANT menu.

```
=========================<EXTENDED ASSISTANT MENU>=========================
|<1> Display Memory                                                       |
|<2> Search Memory                                                        |
|<0> Exit To Main Menu                                                    |
===========================================================================
Enter your choice(0-2):
```

Table 20 EXTENDED ASSISTANT menu options

Option	Task
<1> Display Memory	Display specified memory information.
<2> Search Memory	Search memory for specified contents.
<0> Exit To Main Menu	Return to the EXTENDED-BOOTWARE menu.

Formatting the file system

CAUTION:

Formatting the file system of a storage medium causes the loss of all files.

To format the file system of the current storage medium:

1. Press **Ctrl + F** while you are in the EXTENDED-BOOTWARE menu.
2. Enter **Y** when the prompt for confirmation appears.

```
Warning:All files on flash will be lost! Are you sure to format? [Y/N]y.
```

HPE 6125XLG-CMW710-R2432P03 Release Notes

Software Feature Changes

The information in this document is subject to change without notice.
© Copyright 2017 Hewlett Packard Enterprise Development LP

Contents

R2432P03

This release has the following changes:

- New feature: Gratuitous ARP packet retransmission for the device MAC address change
- Modified feature: Shutting down a Layer 2 aggregate interface by using OpenFlow

New feature: Gratuitous ARP packet retransmission for the device MAC address change

Configuring gratuitous ARP packet retransmission for the device MAC address change

About gratuitous ARP packet retransmission for the device MAC address change

The device sends a gratuitous ARP packet to inform other devices of its MAC address change. However, the other devices might fail to receive the packet because the device sends the gratuitous ARP packet for only once by default. Configure the gratuitous ARP packet retransmission feature to ensure that the other devices can receive the packet.

Procedure

To configure gratuitous ARP packet retransmission for the device MAC address change:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the times and the interval for retransmitting a gratuitous ARP packet for the device MAC address change.	**gratuitous-arp mac-change retransmit** *times* **interval** *seconds*	By default, the device sends a gratuitous packet to inform its MAC address change for only once.

Command reference

gratuitous-arp mac-change retransmit

Use **gratuitous-arp mac-change retransmit** to set the times and the interval for retransmitting a gratuitous ARP packet for the device MAC address change.

Use **undo gratuitous-arp mac-change retransmit** to restore the default.

Syntax

gratuitous-arp mac-change retransmit *times* **interval** *seconds*

undo gratuitous-arp mac-change retransmit

Default

The device sends a gratuitous packet for its MAC address change for only once.

Views

System view

Predefined user roles

network-admin

Parameters

times: Specifies the times of retransmitting a gratuitous packet, in the range of 1 to 10.

interval *seconds*: Specifies the interval for retransmitting a gratuitous packet, in the range of 1 to 10 seconds.

Usage guidelines

The device sends a gratuitous ARP packet to inform other devices of its MAC address change. However, the other devices might fail to receive the packet because the device sends the gratuitous ARP packet for only once by default. Use this command to configure gratuitous ARP retransmission parameters to ensure that the other devices can receive the packet.

After you execute this command, the device will retransmit a gratuitous ARP packet for its MAC address change at the specified interval for the specified times.

Examples

Set the times to 3 and the interval to 5 for retransmitting a gratuitous ARP packet for the device MAC address change.

```
<Sysname> system-view
[Sysname] gratuitous-arp mac-change retransmit 3 interval 5
```

Modified feature: Shutting down a Layer 2 aggregate interface by using OpenFlow

Feature change description

In this release and later, Layer 2 aggregate interfaces can be shut down by using OpenFlow.

Command changes

Modified command: openflow shutdown

Syntax

openflow shutdown

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Change description

Before modification, only Layer 2 Ethernet interfaces can be shut down by using OpenFlow.

After modification, Layer 2 Ethernet interfaces and Layer 2 aggregate interfaces can be shut down by using OpenFlow.

R2432P02

This release has the following changes:

- New feature: Setting the MAC address for a Layer 3 Ethernet interface, Layer 3 Ethernet subinterface, Layer 3 aggregate interface or Layer 3 aggregate subinterface
- Modified feature: Value range for the interval for an OpenFlow instance to reconnect to a controller.

New feature: Setting the MAC address for a Layer 3 Ethernet interface, Layer 3 Ethernet subinterface, Layer 3 aggregate interface or Layer 3 aggregate subinterface

Setting the MAC address for a Layer 3 Ethernet interface, Layer 3 Ethernet subinterface, Layer 3 aggregate interface or Layer 3 aggregate subinterface

To set the MAC address for a Layer 3 Ethernet interface, Layer 3 Ethernet subinterface, Layer 3 aggregate interface or Layer 3 aggregate subinterface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	• Enter Layer 3 Ethernet interface or subinterface view: **interface** *interface-type* { *interface-number* | *interface-number.subnumber* } • Enter Layer 3 aggregate interface or subinterface view: **interface route-aggregation** { *interface-number* | *interface-number.subnumber* }	N/A
3. Set the MAC address for the Layer 3 Ethernet interface, Layer 3 Ethernet subinterface or Layer 3 aggregate interface.	**mac-address** *mac-address*	By default, no MAC address is set for a Layer 3 Ethernet interface, Layer 3 Ethernet subinterface, Layer 3 aggregate interface or Layer 3 aggregate subinterface.

Command reference

mac-address

Use **mac-address** to set the MAC address of a Layer 3 Ethernet interface, Layer 3 Ethernet subinterface, Layer 3 aggregate interface or Layer 3 aggregate subinterface.

Use **undo mac-address** to restore the default.

Syntax

mac-address *mac-address*

undo mac-address

Default

No MAC address is set for a Layer 3 Ethernet interface, Layer 3 Ethernet subinterface, Layer 3 aggregate interface or Layer 3 aggregate subinterface.

Views

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Layer 3 aggregate interface view

Layer 3 aggregate subinterface view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a MAC address in the format of H-H-H.

Examples

Set the MAC address of FortyGigE 1/1/1 to 0001-0001-0001.

```
<Sysname> system-view
[Sysname] interface fortygige 1/1/1
[Sysname-FortyGigE1/1/1] mac-address 1-1-1
```

Modified feature: Value range for the interval for an OpenFlow instance to reconnect to a controller.

Feature change description

The value range changed for the interval for an OpenFlow instance to reconnect to a controller.

Command changes

Modified command: controller connect interval

Syntax

controller connect interval *interval*

undo controller connect interval

Views

OpenFlow instance view

Change description

Before modification: The interval for an OpenFlow instance to reconnect to a controller is in the range of 10 to 120.

After modification: The interval for an OpenFlow instance to reconnect to a controller is in the range of 1 to 120.

R2432P01

This release has no feature changes.

R2432

This release has the following changes:

- New feature: ISSU
- New feature: Displaying burst records for interfaces
- New feature: Loop guard for an OpenFlow instance
- New feature: Shutting down an interface by OpenFlow
- New feature: Ignoring the ingress ports of ARP packets during user validity check
- New feature: Specifying ignored packet fields for the default link-aggregation load sharing
- New feature: Parity error alarming for entries on forwarding chips
- New feature: Excluding a subnet from load sharing on link aggregations
- New feature: ISP domain for users assigned to nonexistent domains
- Modified feature: Displaying operating information for diagnostics
- Modified feature: Displaying history about ports that are blocked by spanning tree protection features
- Modified feature: Displaying BGP MDT peer or peer group information
- Modified feature: Displaying BGP MDT routing information
- Modified feature: Applying an ACL to an interface for packet filtering
- Modified feature: Applying a QoS policy to an interface
- Modified feature: Configuring data buffer monitoring
- Modified feature: Defining QoS match criteria
- Modified feature: Software patching
- Modified feature: User password configuration in RADIUS test profiles
- Modified feature: Configuring SSH client access control
- Modified feature: Predefined user roles of SSH client and FTP client commands
- Modified feature: Username format modification for device login
- Modified feature: Specifying a PW data encapsulation type
- Modified feature: Device diagnostic information
- Modified feature: Memory usage statistics
- Modified feature: Displaying group table statistics

New feature: ISSU

ISSU overview

The In-Service Software Upgrade (ISSU) feature upgrades software with a minimum amount of downtime.

ISSU is implemented on the basis of the following design advantages:

- **Separation of service features from basic functions**—Device software is segmented into boot, system, and feature images. The images can be upgraded individually.

* **Independence between service features**—Features run independently. One feature can be added or upgraded without affecting the operation of the system or other features.
* **Support for hotfix**—Patch images are available to fix system bugs without a system reboot.
* **Hardware redundancy**—In an IRF fabric, one member device can be upgraded while other member devices are providing services.

For more information about images, see "Upgrading software."

ISSU methods

ISSU supports the following upgrade types:

* **Compatible upgrade**—The running software version is compatible with the upgrade software version. This upgrade type supports the ISSU methods in Table 1.
* **Incompatible upgrade**—The running software version is incompatible with the upgrade software version. The two versions cannot run concurrently.

  This upgrade type supports only one upgrade method (also called incompatible upgrade). This method requires a cold reboot. It is service disruptive if hardware redundancy is not available.

Table 1 ISSU methods for compatible upgrade

ISSU method	Description
Incremental upgrade: • Service Upgrade • File Upgrade	Upgrades only segments that contain differences between the new and old software versions. • **Service upgrade**—Upgrades service features. The upgrade does not affect the operation of features that are not being upgraded. • **File upgrade**—Upgrades hidden system program files. The system can provide services during the upgrade.
ISSU Reboot	Reboots CPUs to complete software upgrade. During the reboot, the data plane can still forward traffic. This method saves all data (running, configuration, and hardware) and status to memory before rebooting CPUs. For services that require regular communication with their peers, this method uses protocol agents to maintain their connectivity and status. After the reboot, all data is restored to CPU.
Reboot	**CAUTION:** The Reboot method is service disruptive if the device stands alone. As a best practice, schedule the downtime carefully to minimize the upgrade impact on the services. This method reboots both the control and data planes to complete the software upgrade.

ISSU commands

ISSU provides the **install** and **issu** command sets. After you identify the ISSU method, use Table 2 to choose the command set you want to use.

Table 2 Command set comparison

Item	issu commands	install commands
Upgrade types	• Compatible. • Incompatible.	Compatible.

Item	issu commands	install commands
Patch install/uninstall	Not supported.	Supported.
Upgrade mode	Chassis by chassis.	Chassis by chassis.
Impact on the system	Large.	Small.
Technical skill requirements	Low. As a best practice, use this command set.	High. Administrators must have extensive system knowledge and understand the impact of each upgrade task on the network.

Preparing for ISSU

To perform a successful ISSU, make sure all the preparation requirements are met.

Identifying availability of ISSU and licensing requirements

Read the software release notes to identify the following items:

- Support of the device for ISSU.
- Licensing requirements for the upgrade software images.

Verifying the device operating status

Use the **display device** command to verify that all member devices are operating correctly.

Preparing the upgrade images

1. Use the **dir** command to verify that all member devices has sufficient storage space for the upgrade images. If the storage space is not sufficient, delete unused files by using the **delete** command. For more information, see "Managing the file system."
2. Use FTP or TFTP to transfer upgrade image files to the root directory of any storage medium in the IRF fabric.

Identifying requirements for a patch or an upgrade to a middle version

Use the **display install ipe-info** or **display install package** command to display the software image signature information. The signature of a software image might be HP, HP-US, or HPE.

The Comware system can be upgraded from a version with the HP or HP-US signature to a version with the HPE signature. To upgrade the Comware system from a version without a signature to a version with the HPE signature, you must first complete one of the following tasks:

- Patch the Comware system.
- Upgrade the Comware system to a version with the HP or HP-US signature.

Identifying the ISSU method

1. Execute the **display version comp-matrix file** command for the upgrade image version.
2. Check the **Version compatibility list** field.
   - If the running software version is in the list, a compatible upgrade is required.
   - If the running software version is not in the list, an incompatible upgrade is required.
3. Identify the ISSU method:
   - If a compatible upgrade is required, check the **Upgrade Way** field to identify the ISSU method. For more information about ISSU methods, see Table 1.
   - If an incompatible upgrade is required, check the end of command output for the **Incompatible upgrade** string.

Verifying feature status

For service continuity during ISSU, configure the following feature settings:

Feature	Setting requirements
GR/NSR	Enable GR or NSR for protocols including LDP, RSVP, OSPF, ISIS, BGP, and FSPF.
BFD	Disable BFD for protocols including LDP, RSVP, OSPF, ISIS, RIP, BGP, VRRP, and NQA.
Ethernet link aggregation	Use the long LACP timeout interval (the **lacp period short** command is not configured) on all member ports in dynamic aggregation groups.
IRF	Configure IRF bridge MAC persistence as follows: • **Compatible upgrade**—Configure the **irf mac-address persistent timer** or **irf mac-address persistent always** command. • **Incompatible upgrade**—Configure the **irf mac-address persistent always** command if the bridge MAC address is the MAC address of the device for which you want to execute the **issu load** command.

For an **ISSU Reboot** upgrade on a single-member IRF fabric, also verify that the following features are disabled:

Feature	Remarks
Spanning tree feature	If the spanning tree feature is enabled, service discontinuity might occur during the upgrade because the feature advertises the network topology change.
Dynamic Ethernet link aggregation	During an ISSU reboot, only static aggregation is supported, and dynamic aggregate interfaces might not be able to provide services.
CFD	If CFD is enabled, the CFD CC feature will be disabled during an ISSU reboot, which results in traffic abnormality.
DLDP	If DLDP is enabled, the peer device might consider a link a unidirectional link and shut down the port because it cannot receive probe packets.
Loop detection	If loop detection is enabled, the peer device might enable looped ports because of false loop removal detection.

Determining the upgrade procedure

1. Use Table 2 to choose an upgrade command set, depending on the ISSU method.

2. Identify the hardware redundancy condition.

   ISSU can maintain service continuity only when the IRF fabric has multiple members and uses the ring topology.

> **IMPORTANT:**
>
> If hardware redundancy is not available, service discontinuity is not avoidable. Make sure you understand the impact of the upgrade on the network.

3. Choose the correct procedure from the procedures described in "Performing an ISSU by using issu commands" or "Performing an ISSU by using install commands."

Understanding ISSU guidelines

During an ISSU, use the following guidelines:

- In a multiuser environment, make sure no other administrators access the device while you are performing the ISSU.
- Do not perform any of the following tasks during an ISSU:
  - Reboot, add, or remove member devices.
  - Execute commands that are not related to the ISSU.
  - Modify, delete, or rename image files.
- You cannot use both **install** and **issu** commands for an ISSU. However, you can use **display issu** commands with both command sets.

After an ISSU, you must log in to the device again before you can configure the device.

Logging in to the device through the console port

Log in to the device through the console port after you finish all the preparation tasks and understand all the ISSU guidelines. If you use Telnet or SSH, you might be disconnected from the device before the ISSU is completed.

Saving the running configuration

Use the **save** command to save the running configuration.

Performing an ISSU by using issu commands

The ISSU procedure varies depending on whether the IRF fabric has a single or multiple members.

Upgrading a multichassis IRF fabric

On a multichassis IRF fabric, always start ISSU with a subordinate member.

Performing a compatible upgrade

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. (Optional.) Set the automatic rollback timer.	**issu rollback-timer** *minutes*	By default, the automatic rollback timer is set to 45 minutes.

Step	Command	Remarks
		This timer starts when you execute the **issu run switchover** command. If you do not execute the **issu accept** or **issu commit** command before this timer expires, the system automatically rolls back to the original software images.
3. Return to user view.	**quit**	N/A
4. Load the upgrade images as main startup software images on subordinate members.	• Use .bin files: **issu load file** { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> } *** slot** *slot-number* • Use an .ipe file: **issu load file ipe** *ipe-filename* **slot** *slot-number*&<1-9>	Specify the member ID of a subordinate member for the *slot-number* argument.
5. Perform a master/subordinate switchover.	**issu run switchover**	N/A
6. (Optional.) Accept the upgrade and delete the automatic rollback timer.	**issu accept**	N/A
7. Upgrade the remaining members to complete the ISSU.	**issu commit chassis** *chassis-number*	**IMPORTANT:** After executing the command for one member, you must wait for the member to restart and join the IRF fabric before you execute the command for another member. Repeat the **issu commit** command to upgrade the remaining members one by one, including the original master. To manually roll back to the original software images during this ISSU process, use the **issu rollback** command. For more information about rollback, see *Fundamentals Command Reference*.

Performing an incompatible upgrade

Perform this task in user view.

Step	Command	Remarks
1. Load the upgrade images as main startup software images on subordinate members.	• Use .bin files: **issu load file** { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> } *** slot** *slot-number*&<1-9> • Use an .ipe file: **issu load file ipe** *ipe-filename* **slot** *slot-number*&<1-9>	Specify the member ID of a subordinate member for the *slot-number* argument. As a best practice on a ring-topology IRF fabric, specify half of the subordinate members for this command to reduce service interruption. Make sure the specified subordinate members are physically connected.

Step	Command	Remarks
2. Perform a master/subordinate switchover to complete the ISSU process.	**issu run switchover**	To roll back to the original software images during this ISSU process, use the **issu rollback** command. This ISSU process does not support automatic rollback. For more information about rollback, see *Fundamentals Command Reference*.
3. Verify that the ISSU is finished.	**display issu state**	If the **ISSU state** field displays **Init**, the ISSU is finished.

Upgrading a single-chassis IRF fabric

Performing a service upgrade or file upgrade

Perform this task in user view.

Step	Command	Remarks
1. Load the upgrade images as main startup software images.	• Use .bin files: **issu load file** { **boot** *filename* | **system** *filename* | **feature** *filename*<1-30> } * **slot** *slot-number* • Use an .ipe file: **issu load file ipe** *ipe-filename* **slot** *slot-number*	Specify the member ID of the device for the *slot-number* argument.
2. Complete the ISSU process.	**issu commit slot** *slot-number*	Specify the member ID of the device for the *slot-number* argument. To roll back to the original software images during this ISSU process, use the **issu rollback** command. This ISSU process does not support automatic rollback. For more information about rollback, see *Fundamentals Command Reference*.
3. Verify that the ISSU is finished.	**display issu state**	If the **ISSU state** field displays **Init**, the ISSU is finished.

Performing a reboot/ISSU reboot/incompatible upgrade

Step	Command	Remarks
1. Load the upgrade images as main startup software images.	• Use .bin files: **issu load file** { **boot** *filename* | **system** *filename* | **feature** *filename*<1-30> } * **slot** *slot-number* • Use an .ipe file: **issu load file ipe** *ipe-filename* **slot** *slot-number*	Specify the member ID of the device for the *slot-number* argument.
2. Verify that the ISSU is finished.	**display issu state**	If the **ISSU state** field displays **Init**, the ISSU is finished.

Performing an ISSU by using install commands

ISSU task list

Tasks at a glance	Remarks
(Optional.) Decompressing an .ipe file	To use **install** commands for upgrade, you must use .bin image files. If the upgrade file is an .ipe file, perform this task before you use **install** commands for upgrade.

(Required.) Perform one of the following tasks to update software:
• Installing or upgrading software images
  ○ Installing or upgrading images except for patches
  ○ Installing patch images
• Uninstalling feature or patch images
  ○ Uninstalling feature images
  ○ Uninstalling patch images
	Perform an activate operation to install new images or upgrade existing images.
	Perform an inactivate operation to uninstall feature or patch images.
	An image is added to or removed from the current software image list when it is activated or deactivated.

(Optional.) Rolling back the running software images	Perform this task to roll back running software image status after activate or deactivate operations. A commit operation removes all rollback points. You can perform this task only before software changes are committed.
(Optional.) Aborting a software activate/deactivate operation	You can perform this task while an image is being activated or deactivated. This task is available only for service upgrade or file upgrade.
(Optional.) Committing software changes	This task updates the main startup image list with the changes. If service upgrade or file upgrade is performed, you must perform this task for the changes to take effect after a reboot.
(Optional.) Verifying software images	Perform this task to verify that the software changes are correct.
(Optional.) Removing inactive software images	Perform this task to remove images

Decompressing an .ipe file

Perform this task in user view.

Step	Command
1. (Optional.) Identify images that are included in the .ipe file.	**display install ipe-info**
2. Decompress the .ipe file.	**install add** *ipe-filename medium-name*:

Installing or upgrading software images

Use one of the following methods to perform this task:

- **Chassis by chassis**—Activate all the images on one member device, and then move to the next member device.
- **Image by image**—Activate one image on all member devices before activating another image.

When you install an image, you must begin with the master device.

When you upgrade an image, you must begin with a subordinate device.

Installing or upgrading images except for patches

Perform this task in user view.

Step	Command
1. (Optional.) Identify the ISSU method and possible impacts of the upgrade.	**install activate** { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> } * **slot** *slot-number* **test**
2. Activate images.	**install activate** { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> } * **slot** *slot-number*

Installing patch images

Perform this task in user view.

Task	Command
Activate patch images.	**install activate patch** *filename* { **all** | **slot** *slot-number* }

Uninstalling feature or patch images

The uninstall operation only removes images from the current software image list. For the change to take effect after a reboot, you must perform a commit operation to remove the images from the main startup image list.

Uninstalled images are still stored on the storage medium. To permanently remove the images, execute the **install remove** command. For more information, see "Removing inactive software images."

Boot and system images cannot be uninstalled.

Uninstalling feature images

Perform this task in user view.

Task	Command
Deactivate feature images.	**install deactivate feature** *filename*&<1-30> **slot** *slot-number*

Uninstalling patch images

Perform this task in user view.

Task	Command
Deactivate patch images.	**install deactivate patch** { **all** | *filename* **slot** *slot-number* }

Rolling back the running software images

For each service or file upgrade performed through activate or deactivate operation, the system creates a rollback point. The rollback points are retained until any of the following event occurs:

- An ISSU reboot or reboot upgrade is performed.
- The **install commit** command is executed.

After an ISSU reboot or reboot upgrade is performed, you can roll back the running software images only to the status before any activate or deactivate operations are performed.

After a commit operation is performed, you cannot perform a rollback.

For a rollback to take effect after a reboot, you must perform a commit operation to update the main startup software image list.

To roll back the software, execute the following commands in user view:

Step	Command	Remarks
1. (Optional.) Display available rollback points.	**display install rollback**	A maximum of 50 rollback points are available for service and file upgrades. The earliest rollback point is removed if this limit has been reached when a rollback point is created.
2. Roll back the software.	**install rollback to** { *point-id* | **original** }	N/A

Aborting a software activate/deactivate operation

This task is available only for service upgrade or file upgrade performed through activate or deactivate operation. After the operation is aborted, the system runs with the software images that it was running with before the operation.

Step	Command
1. Press **Ctrl+C** while a software image is being activated or deactivated.	N/A
2. Abort a software activate/deactivate operation in user view.	**install abort** [*job-id*]

Committing software changes

If the ISSU method is service upgrade or file upgrade for an activate or deactivate operation, the main startup image list does not update with the changes. The software changes are lost at reboot. For the changes to take effect after a reboot, you must commit the changes.

Perform this task in user view.

Task	Command	Remarks
Commit the software changes.	**install commit**	This command commits all software changes.

Verifying software images

Perform this task to verify the following items:

- **Integrity**—Verify that the boot, system, and feature images are integral.
- **Consistency**—Verify that the same active images are running across the entire system.
- **Software commit status**—Verify that the active images are committed as needed.

If an image is not integral, consistent, or committed, use the **install activate**, **install deactivate**, and **install commit** commands as appropriate to resolve the issue.

Perform this task in user view.

Task	Command
Verify software images.	**install verify**

Removing inactive software images

Removing a software image deletes the image file permanently. You cannot use the **install rollback to** command after the operation.

Perform this task in user view.

Task	Command
Remove inactive software images.	**install remove** [**slot** *slot-number*] { *filename* | **inactive** }

Displaying and maintaining ISSU

The **display issu state** command applies only to an ISSU that uses the **issu** series commands. All the other **display** commands and all **reset** commands can be used during an ISSU, regardless of whether the **install** or **issu** commands are used.

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display version compatibility information.	**display version comp-matrix**
Display ISSU status information.	**display issu state**
Display automatic rollback timer information.	**display issu rollback-timer**
Display active software images.	**display install active** [**slot** *slot-number*] [**verbose**]
Display inactive software images.	**display install inactive** [**slot** *slot-number*] [**verbose**]
Display main startup software images.	**display install committed** [**slot** *slot-number*] [**verbose**]
Display backup startup software images.	**display install backup** [**slot** *slot-number*] [**verbose**]
Display ongoing ISSU activate, deactivate, and rollback operations.	**display install job**
Display ISSU log entries.	**display install log** [**verbose**]
Display software image file information.	**display install package** { *filename* | **all** } [**verbose**]
Display the software images included in an .ipe file.	**display install ipe-info** *ipe-filename*
Display rollback point information.	**display install rollback**
Display all software image files that include a specific component or file.	**display install which** { **component** *name* | **file** *filename* } [**slot** *slot-number*]
Clear ISSU log entries.	**reset install log-history oldest** *log-number*
Clear ISSU rollback points.	**reset install rollback oldest** *point-id*

Troubleshooting ISSU

Failure to execute the issu load/issu run switchover/issu commit/install activate/install deactivate command

Symptom

The following commands cannot be executed:

- **issu commands**—**issu load**, **issu run switchover**, and **issu commit**.
- **install commands**—**install activate** and **install deactivate**.

Solution

To resolve this issue:

1. Use the **display device** command to verify that all cards are not in **Fault** state.
2. If the problem persists, contact HPE Support.

ISSU examples for using issu commands

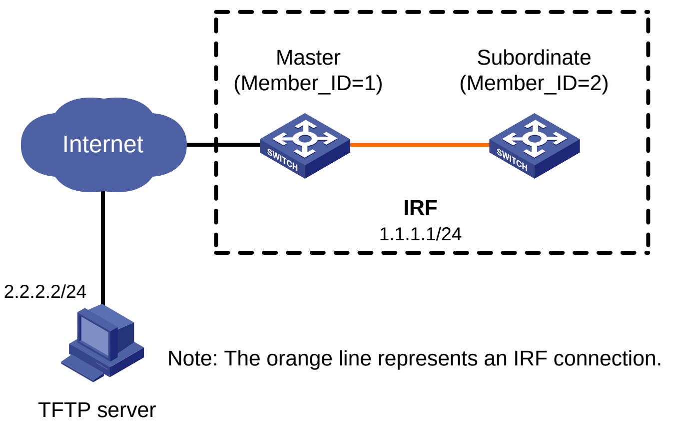
Software image upgrade to a compatible version

Upgrade requirements

As shown in Figure 1, the IRF fabric has two members.

Upgrade feature1 from R0201 to R0202. The two versions are compatible.

Figure 1 Network diagram



Upgrade procedure

Save the running configuration.

```
<Sysname> save
```

Download the image file that contains the feature1 image from the TFTP server.

```
<Sysname> tftp 2.2.2.2 get feature1-r0202.bin
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   256  100   256    0     0    764      0 --:--:-- --:--:-- --:--:--   810
```

Display active software images.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0201.bin
Active packages on slot 2:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0201.bin
```

Identify the ISSU method to be used for the upgrade and view the possible impact of the upgrade.

```
<Sysname> display version comp-matrix file feature flash:/feature1-r0202.bin
Feature image: flash:/feature1-r0202.bin
  Version:
  V700R001B31D002
  Version Compatibility List:
  V700R001B31D001
  V700R001B31D002
  Version Dependency System List:
  V700R001B31D001
  V700R001B31D002

  Slot                        Upgrade Way
  1                           Service Upgrade
  2                           Service Upgrade

Influenced service according to following table on slot 1:
  flash:/feature1-r0202.bin
         feature1
Influenced service according to following table on slot 2:
  flash:/feature1-r0202.bin
         feature1
```

The output shows that an incremental upgrade is recommended. The feature1 module will be rebooted during the upgrade process.

Upgrade feature1 on the subordinate member.

```
<Sysname> issu load file feature flash:/feature1-r0202.bin slot 2
This operation will delete the rollback point information for the previous upgrade and
maybe get unsaved configuration lost. Continue? [Y/N]:y
Upgrade summary according to following table:
Copying file flash:/feature1-r0202.bin to slot2#flash:/feature1-r0202.bin......Done.
flash:/feature1-r0202.bin
  Running Version             New Version
  Alpha 0201                  Alpha 0202

  Slot                        Upgrade Way
  2                           Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]: y
This operation might take several minutes, please wait......Done.
```

Perform a master/subordinate switchover.

```
<Sysname> issu run switchover
Upgrade summary according to following table:

flash:/feature1-r0202.bin
  Running Version             New Version
  Alpha 0201                  Alpha 0202

  Slot                        Switchover Way
  1                           Active standby process switchover
Upgrading software images to compatible versions. Continue? [Y/N]: y
This operation might take several minutes, please wait......Done.
```

Upgrade the feature on the original master.

```
<Sysname> issu commit slot 1
Upgrade summary according to following table:

flash:/feature1-r0202.bin
  Running Version             New Version
  Alpha 0201                  Alpha 0202

  Slot                        Upgrade Way
  1                           Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]: y
This operation might take several minutes, please wait......Done.
```

Verify that both members are running the new image.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0202.bin
Active packages on slot 2:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0202.bin
```

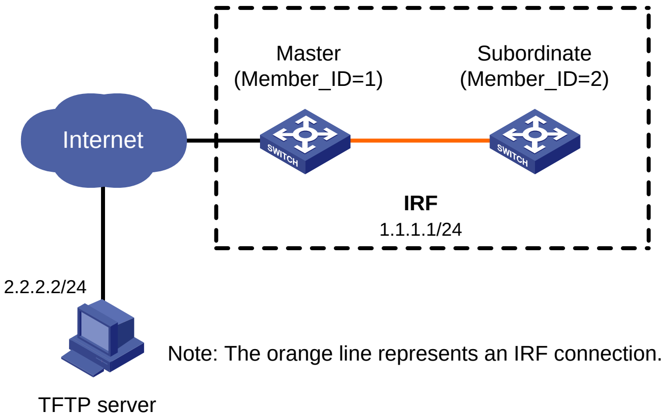
Software image upgrade to an incompatible version

Upgrade requirements

As shown in Figure 2, the IRF fabric has two members.

Upgrade feature1 from R0201 to R0202. The two versions are incompatible.

Figure 2 Network diagram



Upgrade procedure

Save the running configuration.

```
<Sysname> save
```

Download the image file that contains the R0202 feature1 image from the TFTP server.

```
<Sysname> tftp 2.2.2.2 get feature1-r0202.bin
  % Total     % Received % Xferd  Average Speed   Time    Time     Time  Current
                                  Dload  Upload   Total   Spent    Left  Speed
100    256  100   256     0     0    764      0 --:--:-- --:--:-- --:--:--   810
```

Display active software images.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0201.bin
Active packages on slot 2:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0201.bin
```

Identify the ISSU method to be used for the upgrade and view the possible impact of the upgrade.

```
<Sysname> display version comp-matrix file feature flash:/feature1-r0202.bin
Feature image: flash:/feature1-r0202.bin
  Version:
  V700R001B31D002
  Version Compatibility List:
  V700R001B31D002
  Version Dependency System List:
  V700R001B31D001
  V700R001B31D002
Incompatible upgrade.
```

The output shows that the two versions are incompatible. The cards will be rebooted for the upgrade.

Upgrade feature1 on the subordinate member.

```
<Sysname> issu load file feature flash:/feature1-r0202.bin slot 2
```

```
This operation will delete the rollback point information for the previous upgrade and
maybe get unsaved configuration lost. Continue? [Y/N]:y
Copying file flash:/feature1-r0202.bin to slot2#flash:/feature1-r0202.bin......Done.
Upgrade summary according to following table:

flash:/feature1-r0202.bin
  Running Version             New Version
  Alpha 0201                  Alpha 0202

  Slot                        Upgrade Way
  2                           Reboot
Upgrading software images to incompatible versions. Continue? [Y/N]: y
This operation might take several minutes, please wait......Done.
```

Upgrade feature1 on the original master.

```
<Sysname> issu run switchover
Upgrade summary according to following table:

flash:/feature1-r0202.bin
  Running Version             New Version
  Alpha 0201                  Alpha 0202

  Slot                        Upgrade Way
  1                           Reboot
Upgrading software images to incompatible versions. Continue? [Y/N]: y
This operation might take several minutes, please wait......Done.
```

Verify that both members are running the new image.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0202.bin
Active packages on slot2:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0202.bin
```

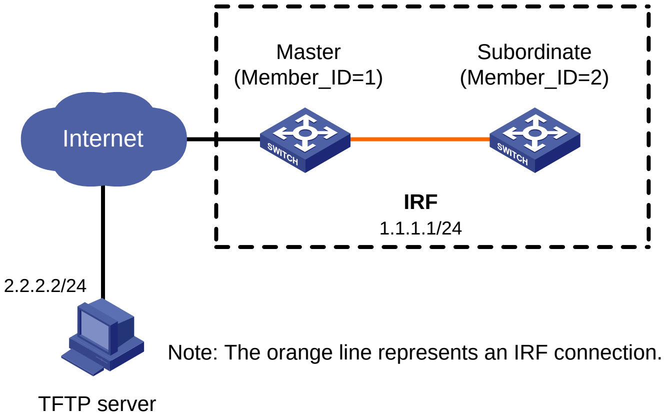
Software image rollback example

Rollback requirement

As shown in Figure 3, the IRF fabric has two members.

Roll back feature1 from R0202 to R0201 after upgrading it from R0201 to R0202. The two versions are compatible.

Figure 3 Network diagram



Rollback procedure

Save the running configuration.

```
<Sysname> save
```

Download the image file that contains the R0202 feature1 image from the TFTP server.

```
<Sysname> tftp 2.2.2.2 get feature1-r0202.bin
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  256k  100  256k    0     0   764k      0 --:--:-- --:--:-- --:--:--  810k
```

Display active software images.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0201.bin
Active packages on slot 2:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0201.bin
```

Identify the ISSU method to be used for the upgrade and view the possible impact of the upgrade.

```
<Sysname> display version comp-matrix file feature flash:/feature1-r0202.bin
Feature image: flash:/feature1-r0202.bin
  Version:
  V700R001B31D002
  Version Compatibility List:
  V700R001B31D001
  V700R001B31D002
  Version Dependency System List:
  V700R001B31D001
  V700R001B31D002

  Slot                          Upgrade Way
  1                             Service Upgrade
  2                             Service Upgrade
```

```
Influenced service according to following table on slot 1:
  flash:/feature1-r0202.bin
         feature1
Influenced service according to following table on slot 2:
  flash:/feature1-r0202.bin
         feature1
```

The output shows that an incremental upgrade is recommended, and the feature1 module will be rebooted during the upgrade process.

Upgrade feature1 on the subordinate member.

```
<Sysname> issu load file feature flash:/feature1-r0202.bin slot 2
This operation will delete the rollback point information for the previous upgrade and
maybe get unsaved configuration lost. Continue? [Y/N]:y
Copying file flash:/feature1-r0202.bin to slot2#flash:/feature1-r0202.bin......Done.
Upgrade summary according to following table:

flash:/feature1-r0202.bin
  Running Version             New Version
  Alpha 0201                  Alpha 0202

  Slot                        Upgrade Way
  2                           Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]: y
This operation might take several minutes, please wait......Done.
```

Perform a master/subordinate switchover.

```
<Sysname> issu run switchover
Upgrade summary according to following table:

flash:/feature1-r0202.bin
  Running Version             New Version
  Alpha 0201                  Alpha 0202

  Slot                        Switchover Way
  1                           Active standby process switchover
Upgrading software images to compatible versions. Continue? [Y/N]: y
This operation might take several minutes, please wait......Done.
```

Display active software images.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0201.bin
Active packages on slot 2:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0202.bin
```

Roll back feature1 to R0201.

```
<Sysname> issu rollback
```

```
This command will quit the ISSU process and roll back to the previous version. Continue?
[Y/N]:Y
```

Verify that both members are running the old image.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0201.bin
Active packages on slot 2:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0201.bin
```

ISSU examples for using install commands

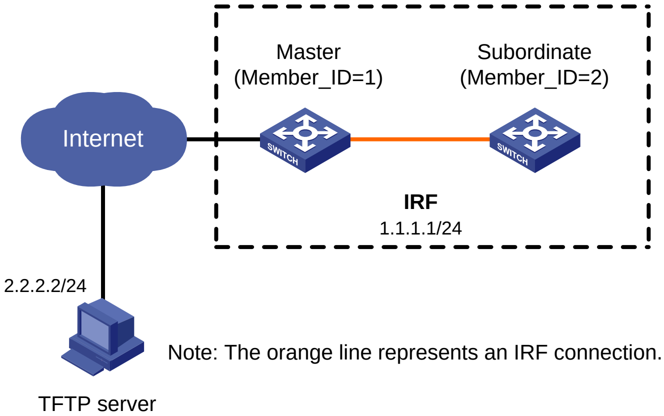
Software image upgrade example

Upgrade requirements

As shown in Figure 4, the IRF fabric has two members.

Upgrade feature1 from R0201 to R0202. The two versions are compatible.

Figure 4 Network diagram



Upgrade procedure

Save the running configuration.

```
<Sysname> save
```

Download the .ipe file that contains the R0202 feature1 image from the TFTP server.

```
<Sysname> tftp 2.2.2.2 get feature1-r0202.ipe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  256k  100  256k    0     0   764k      0 --:--:-- --:--:-- --:--:--  810k
```

Decompress the .ipe file.

```
<Sysname> install add flash:/feature1-r0202.ipe flash:
```

Display active software images.

```
<Sysname> display install active
```

```
Active packages on slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0201.bin
Active packages on slot 2:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0201.bin
```

Identify the ISSU methods for the upgrade and view the possible impact of the upgrade.

```
<Sysname> install activate feature flash:/feature1-r0202.bin slot 2 test
Copying file flash:/feature1-r0202.bin to slot2#flash:/feature1-r0202.bin......Done.
Upgrade summary according to following table:

flash:/feature1-r0202.bin
  Running Version            New Version
  Alpha 0201                 Alpha 0202

  Slot                       Upgrade Way
  2                          Service Upgrade

Influenced service according to following table on slot 2:
  flash:/feature1-r0202.bin
         feature1
<Sysname> install activate feature flash:/feature1-r0202.bin slot 1 test
Upgrade summary according to following table:

flash:/feature1-r0202.bin
  Running Version            New Version
  Alpha 0201                 Alpha 0202

  Slot                       Upgrade Way
  1                          Service Upgrade

Influenced service according to following table on slot 1:
  flash:/feature1-r0202.bin
         feature1
```

The output shows that both members require a service upgrade and the feature1 module will be rebooted during the upgrade process.

Activate the new feature1 image to upgrade feature1.

```
<Sysname> install activate feature flash:/feature1-r0202.bin slot 2
flash:/feature1-r0202.bin already exists on slot 2.
Overwrite it?[Y/N]:y
Copying file flash:/feature1-r0202.bin to slot2#flash:/feature1-r0202.bin......Done.
Upgrade summary according to following table:

flash:/feature1-r0202.bin
  Running Version            New Version
  Alpha 0201                 Alpha 0202
```

```
  Slot                          Upgrade Way
  2                             Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]: y
This operation might take several minutes, please wait......Done.
<Sysname> install activate feature flash:/feature1-r0202.bin slot 1
Upgrade summary according to following table:

flash:/feature1-r0202.bin
  Running Version               New Version
  Alpha 0201                    Alpha 0202

  Slot                          Upgrade Way
  1                             Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]: y
This operation might take several minutes, please wait......Done.
```

Display active software images.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0202.bin
Active packages on slot 2:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0202.bin
```

Confirm the software change.

```
<Sysname> install commit
```

Software image rollback example

Rollback requirement

As shown in Figure 4, the IRF fabric has two members. The feature1 feature has been upgraded from R0201 to R0202, but the software change has not been confirmed.

Roll back feature1 from R0202 to R0201.

Rollback procedure

Display active software images.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0202.bin
Active packages on slot2:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0202.bin
```

Display available rollback points.

```
<Sysname> display install rollback
  Install rollback information 1 on slot 1:
    Updating from flash:/feature1-r0201.bin
             to flash:/feature1-r0202.bin.
  Install rollback information 2 on slot 2:
    Updating from flash:/feature1-r0201.bin
             to flash:/feature1-r0202.bin.
```

Roll back feature1 to R0201.

```
<Sysname> install rollback to original
```

Display active software images.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0201.bin
Active packages on slot 2:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0201.bin
```

Confirm the software change.

```
<Sysname> install commit
```

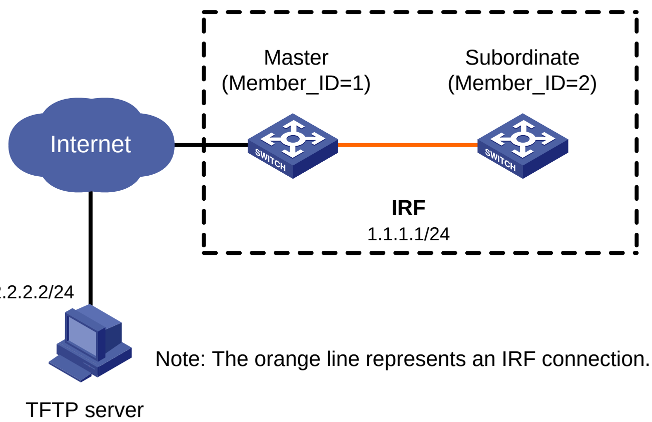
Software image patching example

Patching requirements

As shown in Figure 5, the IRF fabric has two members.

Patch the software images running on the members.

Figure 5 Network diagram



Patching procedure

Download the patch images **boot-patch.bin** and **system-patch.bin** from the TFTP server to the root directory of the flash memory on the master.

```
<Sysname> tftp 2.2.2.2 get boot-patch.bin

  File will be transferred in binary mode
```

```
  Downloading file from remote TFTP server, please wait...|
  TFTP:     100752 bytes received in 11 second(s)
  File downloaded successfully.
<Sysname> tftp 2.2.2.2 get system-patch.bin

  File will be transferred in binary mode
  Downloading file from remote TFTP server, please wait...|
  TFTP:     100112 bytes received in 9 second(s)
  File downloaded successfully.
```

Display active software images.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot.bin
  flash:/system.bin
Active packages on slot 2:
  flash:/boot.bin
  flash:/system.bin
```

The output shows that the patch images are not active.

Activate the patch images on the member devices.

```
<Sysname> install activate patch flash:/boot-patch.bin slot 1
<Sysname> install activate patch flash:/system-patch.bin slot 1
<Sysname> install activate patch flash:/boot-patch.bin slot 2
<Sysname> install activate patch flash:/system-patch.bin slot 2
```

Display active software images.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot.bin
  flash:/system.bin
  flash:/boot-patch.bin
  flash:/system-patch.bin
Active packages on slot 2:
  flash:/boot.bin
  flash:/system.bin
  flash:/boot-patch.bin
  flash:/system-patch.bin
```

Confirm the software change.

```
<Sysname> install commit
```

Display the main startup software images.

```
<Sysname> display install committed
Committed packages on slot 1:
  flash:/boot.bin
  flash:/system.bin
  flash:/boot-patch.bin
  flash:/system-patch.bin
Committed packages on slot 2:
  flash:/boot.bin
  flash:/system.bin
```

```
  flash:/boot-patch.bin
  flash:/system-patch.bin
```

The output shows that the patch images have been specified as the startup software images.

Command reference

display install active

Use **display install active** to display active software images.

Syntax

display install active [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member by its member ID. If you do not specify this option, the command is applied to all IRF members.

verbose: Displays detailed information. If you do not specify this keyword, the command displays only the names of the active software images.

Examples

Display active software images.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot.bin
  flash:/system.bin
```

Display detailed information about active software images.

```
<Sysname> display install active verbose
Active packages on slot 1:
flash:/boot.bin
 [Package]
 Vendor: HPE
 Product: 6127XLG
 Service name: boot
 Platform version: 7.1.022
 Product version: Test 2201
 Supported board: mpu
 [Component]
 Component: boot
 Description: boot package
 Software image signature: HP

flash:/system.bin
```

```
 [Package]
 Vendor: HPE
 Product: 6127XLG
 Service name: system
 Platform version: 7.1.022
 Product version: Test 2201
 Supported board: mpu
[Component]
 Component: system
 Description: system package
 Software image signature: HP
```

Table 3 Command output

Field	Description
Active packages on slot *n*	Active software images on the specified member. The argument *n* indicates the member ID of the member.
[Package]	Detailed information about the software image.
Service name	Image type: • **boot**—Boot image. • **system**—System image. • **boot-patch**—Patch image for the boot image. • **system-patch**—Patch image for the system image. • Any other value indicates a feature image.
Supported board	Cards supported by the software image. The **mpu** string indicates a member device.
[Component]	Information about components included in the image file.

Related commands

install active

display install backup

Use **display install backup** to display backup startup software images.

Syntax

display install backup [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member by its member ID. If you do not specify this option, the command is applied to all IRF members.

verbose: Displays detailed information. If you do not specify this keyword, the command displays only the names of the software images.

Usage guidelines

Backup startup images are used only when the main boot or system image is missing or corrupt. For more information, see *Fundamental Configuration Guide*.

To modify the backup startup image list, you must use the **boot-loader file** command.

Examples

Display the backup startup software images.

```
<Sysname> display install backup
Backup startup software images on slot 1:
  flash:/boot-a0201.bin
  flash:/system-a0201.bin
```

Display detailed information about backup startup software images.

```
<Sysname> display install backup verbose
Backup startup software images on slot 1:
 flash:/boot-a0201.bin
 [Package]
 Vendor: HPE
 Product: 6127XLG
 Service name: boot
 Platform version: 7.1.022
 Product version: Beta 1330
 Supported board: mpu
 [Component]
 Component: boot
 Description: boot package
 Software image signature: HP

 flash:/system-a0201.bin
 [Package]
 Vendor: HPE
 Product: 6127XLG
 Service name: system
 Platform version: 7.1.022
 Product version: Beta 1330
 Supported board: mpu
 [Component]
 Component: system
 Description: system package
 Software image signature: HP
```

For command output descriptions, see Table 3.

Related commands

- **boot-loader file**
- **display install committed**

display install committed

Use **display install committed** to display main startup software images.

Syntax

display install committed [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member by its member ID. If you do not specify this option, the command is applied to all IRF members.

verbose: Displays detailed information. If you do not specify this keyword, the command displays only the names of the software images.

Usage guidelines

After you execute the **install commit** command, use the **display install committed** command to verify that the main startup image list has been updated with the software image change.

Both the **install commit** and **boot-loader file** commands modify the main startup software image list.

For more information about main and backup startup images, see *Fundamental Configuration Guide*.

Examples

Display the main startup software images.

```
<Sysname> display install committed
Committed packages on slot 1:
 flash:/boot-a0201.bin
 flash:/system-a0201.bin
 flash:/system-patch.bin
```

Display detailed information about main startup software images.

```
<Sysname> display install committed verbose
Committed packages on slot 1:
 flash:/boot-a0201.bin
 [Package]
 Vendor: HPE
 Product: 6127XLG
 Service name: boot
 Platform version: 7.1.022
 Product version: Beta 1330
 Supported board: mpu
 [Component]
 Component: boot
 Description: boot package
 Software image signature: HP

 flash:/system-a0201.bin
 [Package]
 Vendor: HPE
```

```
 Product: 6127XLG
 Service name: system
 Platform version: 7.1.022
 Product version: Beta 1330
 Supported board: mpu
 [Component]
 Component: system
 Description: system package
 Software image signature: HP
```

For command output descriptions, see Table 3.

Related commands

- **boot-loader file**
- **display install backup**
- **install commit**

display install inactive

Use **display install inactive** to display inactive software images.

Syntax

display install inactive [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member by its member ID. If you do not specify this option, the command is applied to all IRF members.

verbose: Displays detailed information. If you do not specify this keyword, the command displays only the names of the software images.

Usage guidelines

This command displays inactive images in the root directories of the storage media.

Examples

Display brief information about inactive software images in the root directory of each storage medium.

```
<Sysname> display install inactive
Inactive packages on slot 1:
 flash:/ssh-feature.bin
```

Display detailed information about inactive software images in the root directory of each storage medium.

```
<Sysname> display install inactive verbose
Inactive packages on slot 1:
flash:/ssh-feature.bin
 [Package]
```

```
Vendor: HPE
Product: 6127XLG
Service name: ssh
Platform version: 7.1.022
Product version: Beta 1330
Supported board: mpu
[Component]
Component: ssh
Description: ssh package
Software image signature: HP
```

For information about the command output, see Table 3.

Related commands

install deactivate

display install ipe-info

Use **display install ipe-info** to display the software images included in an .ipe file.

Syntax

display install ipe-info *ipe-filename*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipe *ipe-filename*: Specifies the name of an .ipe file, a case-insensitive string of up to 63 characters. Use one of the following formats:

- *storage-medium*:**/***base-filename***.ipe** on the master.
- **slot***n*#*storage-medium*:**/***base-filename***.ipe** on a subordinate member. For example, slot1#flash:/a.ipe.

Usage guidelines

An .ipe file contains one or more software images. You can use the software images for a software upgrade.

The specified file must be saved in the root directory of the storage medium.

Examples

Display information about the .ipe file **flash:/test.ipe**.

```
<Sysname> display install ipe-info flash:/test.ipe
Verifying image file...Done.
Verifying the IPE file and the images.....Done.
Images in IPE:
  boot.bin
  system.bin
  Software image signature: HP
```

Related commands

display install package

display install job

Use **display install job** to display ongoing ISSU activate, deactivate, and rollback operations.

Syntax

display install job

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display ongoing ISSU activate, deactivate, and rollback operations.

```
<Sysname> display install job
 JobID:5
  Action:install activate flash:/ssh-feature.bin on slot 1
```

The output shows that the device is executing the **install activate flash:/ssh-feature.bin slot 1** command.

display install log

Use **display install log** to display ISSU log information.

Syntax

display install log [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

verbose: Displays detailed ISSU log information. If you do not specify this keyword, the command displays brief ISSU log information.

Usage guidelines

The device creates one log entry for each ISSU operation to track the process and operation result.

The ISSU log can contain a maximum of 50 entries. The latest entry overwrites the oldest entry if the log is full.

Examples

Display all ISSU log entries.

```
<Sysname> display install log
Install job 1 started by user admin at 01/01/2011 04:53:40.
```

```
 Job 1 completed successfully at 01/01/2011 04:53:46.
----------------------------------------------------------------------
 Install job 2 started by user admin at 01/01/2011 04:55:23.
 Job 2 completed successfully at 01/01/2011 04:55:29.
```

Displays detailed information about ISSU log entry 1.

```
<Sysname> display install log 1 verbose
Install job 1 started by user admin at 01/01/2011 04:53:40.
 Job 1 completed successfully at 01/01/2011 04:53:46.

 Detail of activating packages on slot 1.
    Got upgrade policy successfully.
----------------------------------------------------------------------
 Install job 2 started by user admin at 01/01/2011 04:55:23.
 Job 2 completed successfully at 01/01/2011 04:55:29.

 Detail of activating packages on slot 1.
    Got upgrade policy successfully.

 Detail of activating packages on slot 1.
    Updated active package list successfully.

 Detail of activating packages on slot 1.
    Set startup software images successfully.

 Detail of activating packages on slot 1.
    Start ISSU Reboot successfully.
```

Related commands

reset install log-history oldest

display install package

Use **display install package** to display software image file information.

Syntax

display install package { *filename* **|** **all** } [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

filename: Specifies the name of a software image file, a case-insensitive string of up to 63 characters. Use one of the following formats:

- *storage-medium***:/***base-filename***.bin** on the master.
- **slot***n#storage-medium***:/***base-filename***.bin** on a subordinate member. For example, slot1#flash:/a.bin.

all: Specifies all software image files in the root directories of the master's storage media.

verbose: Displays detailed information. If you do not specify this keyword, the command displays only basic software image information.

Usage guidelines

The specified file must be saved in the root directory of the storage medium.

Examples

Display information about software image file **system.bin**.

```
<Sysname> display install package flash:/system.bin
  flash:/system.bin
  [Package]
  Vendor: HPE
  Product: 6127XLG
  Service name: system
  Platform version: 7.1.022
  Product version: Beta 1330
  Supported board: mpu
  Software image signature: HP
```

Display detailed information about software image file **system.bin**.

```
<Sysname> display install package flash:/system.bin verbose
  flash:/system.bin
  [Package]
  Vendor: HPE
  Product: 6127XLG
  Service name: system
  Platform version: 7.1.022
  Product version: Beta 1330
  Supported board: mpu
  [Component]
  Component: system
  Description: system package
  Software image signature: HP
```

For more information about the command output, see Table 3.

display install rollback

Use **display install rollback** to display rollback point information.

Syntax

display install rollback

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Use this command to identify available rollback points during an ISSU that uses **install** commands. The system does not record rollback points during an ISSU that uses **issu** commands.

Examples

Display all rollback points.

```
<Sysname> display install rollback
Install rollback information 1 on slot 1:
    Updating from flash:/boot-a2403.bin
             to flash:/boot-a2404.bin.
    Updating from flash:/system-a2403.bin
             to flash:/system-a2404.bin.
```

The output shows that the device has one rollback point. At this rollback point, **flash:/boot-a2403.bin** and **system-a2403.bin** were upgraded to **flash:/boot-a2404.bin** and **system-a2404**, respectively.

Related commands

- **install rollback**
- **reset install rollback oldest**

display install which

Use **display install which** to display all software image files that include a specific component or file.

Syntax

display install which { **component** *name* | **file** *filename* } [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

component *name*: Specifies a component name.

file *filename*: Specifies a file name, a case-insensitive string of up to 63 characters. It cannot contain path information.

slot *slot-number*: Specifies an IRF member by its member ID. If you do not specify this option, the command is applied to all IRF members.

Usage guidelines

A component is a collection of features. The features of a component are installed or uninstalled at the same time.

When the system displays a component or file error, use this command to identify the relevant image files before you make a software upgrade decision.

This command searches only the root directory of the storage medium.

Examples

Display all software image files that include file **sshc.cli**.

```
<Sysname> display install which file pkg_ctr
```

```
File pkg_ctr is in following packages on slot 1:
  flash:/system-1330.bin
  [Package]
  Vendor: HPE
  Product: 6127XLG
  Service name: system
  Platform version: 7.1.022
  Product version: Beta 1330
  Supported board: mpu
  Software image signature: HP
```

For more information about the command output, see Table 3.

display issu rollback-timer

Use **display issu rollback-timer** to display automatic rollback timer information.

Syntax

display issu rollback-timer

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Change to the automatic rollback interval does not take effect on the ongoing ISSU process. The current remaining rollback time might be greater than the configured automatic rollback interval.

Examples

Display automatic rollback timer information after the **issu run switchover** command is executed.

```
<Sysname> display issu rollback-timer
Rollback timer: Working
Rollback interval: 45 minutes
Rollback time remaining : 40 minutes
```

Display automatic rollback timer information after the **issu accept** command is executed.

```
<Sysname> display issu rollback-timer
Rollback timer: Not working
Rollback interval: 30 minutes
```

Display automatic rollback timer information when no ISSU process is taking place.

```
<Sysname> display issu rollback-timer
Rollback timer: Not working
Rollback interval: 45 minutes
```

Related commands

issu rollback-timer

display issu state

Use **display issu state** to display ISSU status information.

Syntax

display issu state

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

During an ISSU that uses **issu** commands, you can use this command to verify the ISSU status and determine what to do next.

This command does not apply to an ISSU that uses **install** commands, because the ISSU state machine is not involved.

Examples

Display ISSU status information when no upgrade is taking place.

```
<Sysname> display issu state
ISSU state: Init
Compatibility: Unknown
Work state: Normal
Upgrade method: Card by card
Upgraded slot: None
Current upgrading slot: None
Current version list:
  boot: 7.1.041, Demo 2402
  system: 7.1.041, Demo 2402
Current software images:
  flash:/boot.bin
  flash:/system.bin
```

Display ISSU status information while the **issu load** command is being executed.

```
<Sysname> display issu state
ISSU state: Loading
Compatibility: Incompatible
Work state: Normal
Upgrade method: Card by card
Upgraded slot: None
Current upgrading slot:
  slot 1
Previous version list:
  boot: 7.1.041, Demo 2402
  system: 7.1.041, Demo 2402
Previous software images:
  flash:/boot.bin
  flash:/system.bin
```

```
Upgrade version list:
  boot: 7.1.041, Demo 2403
  system: 7.1.041, Demo 2403
Upgrade software images:
  flash:/boot02.bin
  flash:/system04.bin
```

Table 4 Command output

Field	Description
ISSU state	ISSU status: • **Init**—The ISSU process has not started or has finished. • **Loading**—The system is executing the **issu load** command. • **Loaded**—The **issu load** command is completed. • **Switching**—The system is executing the **issu run switchover** command. • **Switchover**—The **issu run switchover** command is completed. • **Accepted**—The **issu accept** command is completed. • **Committing**—The system is executing the **issu commit** command. • **Rollbacking**—A rollback is in process.
Compatibility	Version compatibility: • **Compatible**. • **Incompatible**. • **Unknown**—No upgrade is in process.
Work state	Operating state of the device: • **Normal**—The device is operating correctly. • **Independent active**—When you perform an ISSU for an incompatible version, the member devices that have been upgraded enter this state. In this state, the member devices of the IRF fabric are running different software versions.
Upgrade method	Upgrade mode. If this field displays **Card by card**, the upgrade is performed on a member-by-member basis.
Upgraded slot	Upgraded member device.
Current upgrading slot	Member devices that are being upgraded.
Previous version list	Software versions running on the device before the ISSU.
Previous software images	Software images running on the device before the ISSU.
Upgrade version list	Software versions to upgrade to.
Upgrade software images	Software images used for the upgrade.

Related commands

- **issu accept**
- **issu commit**
- **issu load**
- **issu rollback**
- **issu run switchover**

display version comp-matrix

Use **display version comp-matrix** to display version compatibility information.

Syntax

display version comp-matrix

display version comp-matrix file { **boot** *filename* **|** **system** *filename* **|** **feature** *filename*<1-30> } *****

display version comp-matrix file ipe *ipe-filename*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

boot: Specifies a boot image file.

system: Specifies a system image file.

feature: Specifies feature image files. You can specify a space-separated list of up to 30 feature image files.

filename: Specifies the name of a software image file on the master, in the format *storage-medium***:/***base-filename***.bin**. It can be a case-insensitive string of up to 63 characters and cannot contain slot information.

ipe *ipe-filename*: Specifies the name of an .ipe file on the master, in the format *storage-medium***:/***base-filename***.ipe**. It can be a case-insensitive string of up to 63 characters and cannot contain slot information.

Usage guidelines

The specified image files must be saved in the root directory of the storage medium.

If you do not specify any image files, the command displays compatibility information for the running software images.

If you specify file names, the command displays compatibility information for the specified images and the recommended ISSU methods for upgrade the running images to the specified images.

Examples

Display compatibility information for the running software images.

```
<Sysname> display version comp-matrix
Boot image: flash:/boot-r2208p01.bin
  Version:
  7.1.035P05

System image: flash:/system-r2208p01.bin
  Version:
  R2208P01
  Version compatibility list:
  E2206P02
  R2207
  R2208
  R2208P01
```

```
  Version dependency boot list:
  7.1.035P02
  7.1.035P03
  7.1.035P04
  7.1.035P05
```

Display compatibility information for **flash:/boot-a2403.bin** and **flash:/system-a2403.bin**, and the recommended ISSU method. (In this example, the specified versions are incompatible with the running versions.)

```
<Sysname> display version comp-matrix file boot flash:/boot-a2403.bin system
flash:/system-a2403.bin
Boot image: flash:/boot-a2403.bin
  Version:
  7.1.046

System image: flash:/system-a2403.bin
  Version:
  A2403
  Version compatibility list:
  A2403
  Version dependency boot list:
  7.1.046
Incompatible upgrade.
```

Display compatibility information for **flash:/boot-f2209.bin** and **flash:/system-f2209.bin**, and the recommended ISSU method. (In this example, the specified versions are compatible with the running versions.)

```
<Sysname> display version comp-matrix file boot flash:/boot-f2209.bin system
flash:/system-f2209.bin
Boot image: flash:/boot-f2209.bin
  Version:
  7.1.035P08

System image: flash:/system-f2209.bin
  Version:
  F2209
  Version compatibility list:
  E2206P02
  R2207
  R2208
  R2208P01
  F2209
  Version dependency boot list:
  7.1.035P02
  7.1.035P03
  7.1.035P04
  7.1.035P05
  7.1.035P07
  7.1.035P08

  Slot                        Upgrade Way
```

```
1                                  ISSU Reboot
2                                  ISSU Reboot
```

Table 5 Command output

Field	Description
Version compatibility list	• Under a system image, this field shows all system image versions that are compatible with the system image. • Under a feature image, this field shows all feature image versions that are compatible with the feature image.
Version dependency boot list	Boot image versions that support the system image. To install the system image, you must install one of the boot image versions that is in the list.
Version dependency system list	System image versions that support the feature image. To install the feature image, you must install one of the system image versions that is in the list.
Influenced service according to following table	Services that will be affected by the upgrade. This field is displayed only for compatible versions.
Incompatible upgrade	You are upgrading the software to an incompatible version.
Slot	Member ID of the device in the IRF fabric. This field is displayed only for compatible versions.
Upgrade Way	ISSU method to be used for a compatible version: • **Service Upgrade**—Service-level incremental upgrade. • **File Upgrade**—File-level incremental upgrade. • **ISSU Reboot**—Reboots CPUs to complete the upgrade. • **Reboot**—Reboots the entire device to complete the upgrade. For more information about ISSU methods, see *Fundamentals Configuration Guide*.

Related commands

issu load

install abort

Use **install abort** to abort an ISSU operation.

Syntax

install abort

Views

User view

Predefined user roles

network-admin

Usage guidelines

The system creates a software image management job each time you use the **install activate**, **install add**, **install commit**, **install deactivate**, **install remove**, or **install rollback to** command. Each job represents one command and is assigned a unique job ID. You can abort only ongoing activate and deactivate operations.

To obtain the ID of a job, use the **display install job** command.

Examples

Abort a software image operation.

```
<Sysname> install abort
```

Related commands

display install job

install activate

Use **install activate** to activate software images, or identify the ISSU method and the possible impact on the device.

Syntax

install activate { **boot** *filename* **|** **system** *filename* **|** **feature** *filename*&<1-30> } * **slot** *slot-number* [**test**]

install activate patch *filename* { **all** **|** **slot** *slot-number* }

Views

User view

Predefined user roles

network-admin

Parameters

all: Specifies all IRF members.

boot: Specifies a boot image file. For more information about software images, see *Fundamental Configuration Guide*.

system: Specifies a system image file.

feature: Specifies feature image files. You can specify a space-separated list of up to 30 feature image files.

patch: Specifies a patch image file.

filename: Specifies the name of a software image file on the master, in the format *storage-medium***:/***base-filename***.bin**. It can be a case-insensitive string of up to 63 characters and cannot contain slot information.

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

test: Only checks for the ISSU method to be used for the upgrade. If you do not specify this keyword, the command activates the specified software images.

Usage guidelines

The specified files must be saved in the root directory of the storage medium.

Before you use this command to activate a software image, read the release notes to identify the licensing requirement for the image.

An image runs in memory immediately after it is activated. However, an activated image cannot stay activated after a reboot unless it meets the following requirements:

- It is a patch image.
- It was activated on all IRF members by using the **install activate patch** *filename* **all** command.

For activated images that cannot stay activated after a reboot, you must execute the **install commit** command to commit the software changes.

If you specify a subordinate member for the command, the command copies the images to the subordinate member automatically.

At reboot, a subordinate device automatically synchronizes the master device's configuration and status data. You must wait for the synchronization to complete before using the **install activate** command on the subordinate device. To check the synchronization progress, use the **display device** command. The synchronization is completed when all member devices are in normal state.

Examples

Identify the ISSU method for feature upgrade with **ssh2.bin** on subordinate member 2 and the upgrade impact on the device.

```
<Sysname> install activate feature flash:/ssh2.bin slot 2 test
Copying file flash:/ssh2.bin to slot2#flash:/ssh2.bin......Done.
Upgrade summary according to following table:

flash:/ssh2.bin
  Running Version             New Version
  Beta 1330                   Beta 1331

  Slot                        Upgrade Way
  2                           Service Upgrade

Influenced service according to following table:
flash:/ssh2.bin
     SSH       IFMGR     CFA       LAGG
```

The output shows that a service upgrade is recommended. The SSH, IFMGR, CFA, and LAGG modules will be rebooted during the upgrade.

Activate the patch image **system-patch.bin** on member device 1.

```
<Sysname> install activate system-patch.bin slot 1
```

Activate the system image in file **system.bin** and feature images in file **feature.bin** on member device 2.

```
<Sysname> install activate system flash:/system.bin feature flash:/feature.bin slot 2
Copying file flash:/system.bin to slot2#flash:/system.bin......Done.
Copying file flash:/feature.bin to slot2#flash:/feature.bin......Done.
Upgrade summary according to following table:

flash:/system.bin
  Running Version             New Version
  Beta 1330                   Beta 1331

flash:/feature.bin
  Running Version             New Version
  None                        Beta 1330

  Slot                        Upgrade Way
  2                           Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait......Done.
```

Table 6 Command output

Field	Description
Upgrade summary according to following table	Upgrade summary.

Field	Description
Running Version	Version number of the running software.
New Version	Version number of the new software.
Slot	Member ID of the device in the IRF fabric.
Upgrade Way	ISSU methods: • **Service Upgrade**—Service-level incremental upgrade. • **File Upgrade**—File-level incremental upgrade. The upgrade involves only hidden program files and does not affect the operation of the system or services. • **ISSU Reboot**—Reboots CPUs to complete the upgrade. • **Reboot**—Reboots the entire device to complete the upgrade. This field is displayed only for an upgrade to a compatible version.
Influenced service according to following table	Services influenced by the upgrade.

Related commands

- **display install active**
- **install commit**
- **install deactivate**

install add

Use **install add** to decompress an .ipe file.

Syntax

install add *ipe-filename medium-name***:**

Views

User view

Predefined user roles

network-admin

Parameters

ipe-filename: Specifies the name of an .ipe file on the master, in the format *storage-medium***:/***base-filename***.ipe**. It can be a case-insensitive string of up to 63 characters and cannot contain slot information.

medium-name: Specifies the name of the storage medium for saving the software images. If the storage medium is on a subordinate member, use the **slot***n#storage-medium* format, for example, slot1#flash.

Usage guidelines

The .ipe file must be saved in the root directory of the storage medium.

To use **install** commands for upgrade, you must use .bin image files. If the upgrade file is an .ipe file, use this command to decompress the .ipe file before you start the upgrade.

The images decompressed from the .ipe file will be saved to the root directory of the specified medium.

To identify software images that are included in an .ipe file, use the **display install ipe-info** command.

Examples

Decompress **all.ipe** to the flash memory.

```
<Sysname> install add flash:/all.ipe flash:
Verifying image file.........................Done.
Decompressing file boot.bin to flash:/boot.bin.......................Done.
Decompressing file system.bin to lash:/system.bin.................................Done.
```

install commit

Use **install commit** to commit software changes.

Syntax

install commit

Views

User view

Predefined user roles

network-admin

Usage guidelines

This command revises the main startup software image list to be the same as the committed image list. Software changes take effect at the next startup.

You must execute this command after using the following commands:

- The **install activate** command in an incremental upgrade.
- The **install deactivate** command.
- The **install rollback** command.

In a reboot or ISSU reboot upgrade, the **install activate** command revises both the current and startup software image lists. You do not need to commit software changes.

Both the **install commit** and **boot-loader file** commands change main startup software images. To change backup startup images or add inactive images as main startup images, however, you must use the **boot-loader file** command.

For more information about main and backup startup software images, see *Fundamental Configuration Guide*.

Examples

Commit software changes.

```
<Sysname> install commit
```

Related commands

- **install activate**
- **install deactivate**
- **install rollback**

install deactivate

Use **install deactivate** to deactivate feature or patch images.

Syntax

install deactivate feature *filename*<1-30> **slot** *slot-number*

install deactivate patch *filename* { **all** **|slot** *slot-number* }

Views

User view

Predefined user roles

network-admin

Parameters

all: Specifies all IRF members.

feature: Specifies feature image files. You can specify a space-separated list of up to 30 feature image files.

patch: Specifies a patch image file.

filename: Specifies the name of a software image file on the master, in the format *storage-medium***:/***base-filename***.bin**. It can be a case-insensitive string of up to 63 characters and cannot contain slot information.

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

Usage guidelines

The specified files must be saved in the root directory of the storage medium.

You can deactivate only active feature and patch images.

An image stops running in memory immediately after it is deactivated. However, a deactivated image becomes active again after a reboot unless it meets the following requirements:

- It is a patch image.
- It was deactivated on all IRF members by using the **install deactivate patch** *filename* **all** command.

To prevent deactivated images from running again after a reboot, execute the **install commit** command to commit the software changes.

At reboot, a subordinate device automatically synchronizes the master device's configuration and status data. You must wait for the synchronization to complete before using the **install deactivate** command on the subordinate device. To check the synchronization progress, use the **display device** command. The synchronization is completed when all member device are in normal state.

Examples

Deactivate the patch images in file **route-patch.bin** on IRF member 1.

```
<Sysname> install deactivate patch flash:/route-patch.bin slot 1
```

Related commands

- **display install active**
- **display install inactive**

install remove

Use **install remove** to remove inactive software images.

Syntax

install remove [**slot** *slot-number*] { *filename* **|** **inactive** }

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member by its member ID. If you do not specify this option, the command is applied to all IRF members.

filename: Specifies the name of a software image file on the master, in the format *storage-medium***:/***base-filename***.bin**. It can be a case-insensitive string of up to 63 characters and cannot contain slot information.

inactive: Removes all inactive software image files in the root directories of the specified storage media.

Usage guidelines

The specified files must be saved in the root directory of the storage medium.

This command deletes only inactive software image files saved in the root directories of the specified storage media.

Removing a software image deletes the image file from the device permanently. You cannot use the **install rollback to** command to revert the operation, or use the **install abort** command to abort the operation.

Examples

Remove inactive software image file **flash:/ssh-feature.bin**.

```
<Sysname> install remove flash:/ssh-feature.bin
```

Remove inactive patch package **flash:/ssh-patch.bin**.

```
<Sysname> install remove flash:/ssh-patch.bin
```

install rollback to

Use **install rollback to** to roll back the software to an earlier rollback point.

Syntax

install rollback to { *point-id* | **original** }

Views

User view

Predefined user roles

network-admin

Parameters

point-id: Specifies a rollback point ID. This option is supported only when there are two or more rollback points. To view available rollback points, use the **display install rollback** command.

original: Rolls back to the software images that were running before the ISSU.

Usage guidelines

The system creates a rollback point for each service or file upgrade performed through activate or deactivate operation. The rollback points are retained until any of the following events occur:

- An ISSU reboot or reboot upgrade is performed.
- The **install commit** command is executed.

After an ISSU reboot or reboot upgrade is performed, you can roll back the running software images only to the status before any activate or deactivate operations were performed.

After a commit operation is performed, you cannot perform a rollback.

For a rollback to take effect after a reboot, you must perform a commit operation to update the main startup software image list.

A maximum of 50 rollback points are available for service and file upgrades. The earliest rollback point is removed if this limit has been reached when a rollback point is created.

Patch images do not support rollback.

Examples

Roll back the software to rollback point 1.

```
<Sysname>install rollback to 1
```

Roll back the software to the original software versions and observe the change made by the rollback.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-a0201.bin
   flash:/system-a0201.bin
   flash:/ssh-feature-a0201.bin
<Sysname> display install rollback
Install rollback information 1 on slot 1:
  Update from no package
         to flash:/ssh-feature-a0201.bin.
```

The output shows that currently three images are active but only two of them are confirmed. Image flash:/ssh-feature-a0201.bin is not confirmed yet.

```
<Sysname> install rollback to original
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-a0201.bin
  flash:/system-a0201.bin
<Sysname> display install committed
Committed packages on slot 1:
  flash:/boot-a0201.bin
  flash:/system-a0201.bin
```

The output shows the SSH feature has been rolled back to the original version. Image flash:/ssh-feature-a0201.bin has been removed.

Related commands

display install rollback

install verify

Use **install verify** to verify the software change confirmation status and software image integrity and consistency.

Syntax

install verify

Views

User view

Predefined user roles

network-admin

Usage guidelines

To ensure a successful ISSU and make sure the system can start up and operate correctly after an ISSU, execute this command to verify the following items:

- **Integrity**—Verify that the boot, system, and feature images are integral.
- **Consistency**—Verify that the same active images are running across the entire system.
- **Software commit status**—Verify that the active images are committed as needed.

If a software image fails the verification, perform the following tasks to resolve the problem:

- To ensure software integrity, download and install the software images again.
- To guarantee software image consistency or change software commit status, use the **install activate**, **install deactivate**, and **install commit** commands as appropriate.

Examples

Verify the software change confirmation status and software image integrity and consistency on member devices.

```
<Sysname> install verify
Active packages on slot 1 are the reference packages.
Packages will be compared with the reference packages.
This operation will take several minutes, please wait...
  Verifying packages on slot 1:
  Start to check active package completeness.
    flash:/boot-a0101.bin verification successful.
    flash:/system-a0101.bin verification successful.
  Start to check active package consistency.
    Active packages are consistent with committed packages on their own board.
    Active packages are consistent with the reference packages.
  Verifying packages on slot 2:
  Start to check active package completeness.
    flash:/boot-a0101.bin verification successful.
    flash:/system-a0101.bin verification successful.
  Start to check active package consistency.
    Active packages are consistent with committed packages on their own board.
    Active packages are consistent with the reference packages.
Verification is done.
```

issu accept

Use **issu accept** to accept the upgrade to a compatible version and delete the automatic rollback timer.

Syntax

issu accept

Views

User view

Predefined user roles

network-admin

Usage guidelines

The system cannot perform automatic rollback for the ISSU process after you execute this command. However, you can still use the **issu rollback** command to perform a manual rollback.

You can execute the **issu commit** command to finish the ISSU process without executing this command.

The **issu accept** command does not apply to the ISSU to an incompatible version. The system will display an error message if you execute this command during this type of ISSU.

Examples

Accept the upgrade to a compatible version.

```
<Sysname> issu accept
```

Related commands

- **issu load**
- **issu run switchover**

issu commit

Use **issu commit** to upgrade subordinate members (including the original master) during an ISSU to a compatible version.

Syntax

issu commit slot *slot-number*

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies the member ID of the original master or a subordinate member that has not been upgraded.

Usage guidelines

For a multichassis IRF fabric, use this command to upgrade subordinate members one by one. You must wait for the upgraded subordinate member to start up again and join the IRF fabric before upgrading another subordinate member. After all members are upgraded, the ISSU status changes to Init, and the ISSU process ends and cannot be rolled back.

For an IRF fabric with a single member, this command ends the ISSU process. When this command is completed, the ISSU status changes to Init, and the ISSU process cannot be rolled back.

At reboot, a subordinate device automatically synchronizes the master device's configuration and status data. You must wait for the synchronization to complete before using the **issu commit** command on the subordinate device. To check the synchronization progress, use the **display device** command. The synchronization is completed when all member device are in normal state.

Examples

After member 2 is upgraded and becomes the new master, upgrade the original master (member 3) and the other subordinate members that have not been upgraded (member 4 and member 1).

```
<Sysname> issu commit slot 3
Upgrade summary according to following table:

flash:/feature.bin
```

```
  Running Version             New Version
  Alpha 7122                  Alpha 7123

  Slot                        Upgrade Way
  3                           Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]: y
This operation might take several minutes, please wait.....done
<Sysname> issu commit slot 4
Copying file flash:/feature.bin to slot4#flash:/feature.bin...Done.
Upgrade summary according to following table:

flash:/feature.bin
  Running Version             New Version
  Alpha 7122                  Alpha 7123

  Slot                        Upgrade Way
  4                           Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait.....done
<Sysname> issu commit slot 1
Copying file flash:/feature.bin to slot1#flash:/feature.bin...Done.
Upgrade summary according to following table:

flash:/feature.bin
  Running Version             New Version
  Alpha 7122                  Alpha 7123

  Slot                        Upgrade Way
  1                           Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait.....done
```

For field descriptions, see Table 5.

Related commands

- **issu accept**
- **issu load**
- **issu run switchover**

issu load

Use **issu load** to upgrade the software images of subordinate members and configure the upgrade images as the main startup software images for the subordinate members.

Syntax

issu load file { **boot** *filename* | **system** *filename* | **feature** *filename*<1-30> } ***** **slot** *slot-number*<1-9>

issu load file ipe *ipe-filename* **slot** *slot-number*<1-9>

Views

User view

Predefined user roles

network-admin

Parameters

boot: Specifies a boot image file.

system: Specifies a system image file.

feature: Specifies feature image files. You can specify a space-separated list of up to 30 feature image files.

filename: Specifies the name of a software image file in the root directory of the master's flash memory, in the format **flash:/***xxx***.bin**. It can be a case-insensitive string of up to 63 characters and cannot contain slot information.

filename: Specifies the name of a software image file on the master, in the format *storage-medium***:/***base-filename***.bin**. It can be a case-insensitive string of up to 63 characters and cannot contain slot information.

ipe *ipe-filename*: Specifies the name of an .ipe file on the master, in the format *storage-medium***:/***base-filename***.ipe**. It can be a case-insensitive string of up to 63 characters and cannot contain slot information.

slot *slot-number*: Specifies the member ID of a subordinate member. For a compatible upgrade, you can specify only one member ID. For an incompatible upgrade, you can specify a space-separated list of up to three member IDs. If the IRF fabric has only one member, enter the member ID of this member to upgrade the entire fabric.

Usage guidelines

The specified files must be saved in the root directory of the storage medium.

On a single-chassis IRF fabric, specify the member ID of the member for this command.

On a multichassis IRF fabric, specify one or more subordinate members for this command. If the member devices of the IRF fabric are connected into a ring topology, specify half of the subordinate members for this command to reduce service interruption. Make sure the specified subordinate members are physically connected.

This command performs the following tasks:

- Examines the compatibility of the specified images with the running images. The result might be compatible or incompatible.
- Determines the ISSU methods.

  The ISSU methods available for a compatible version include:

  - Incremental upgrade. During the upgrade, the involved processes will be upgrade.
  - ISSU reboot. During the upgrade, CPUs will be rebooted.
  - Reboot. During the upgrade, the specified member devices will be rebooted.

  The ISSU method for an incompatible version is always reboot.
- Uses the ISSU methods to upgrade the specified member devices, and configures the upgrade software images as the main startup software images for the specified member devices.

At reboot, a subordinate device automatically synchronizes the master device's configuration and status data. You must wait for the synchronization to complete before using the **issu load** command on the subordinate device. To check the synchronization progress, use the **display device** command. The synchronization is completed when all member device are in normal state.

For more information about ISSU methods, see *Fundamentals Configuration Guide*.

Examples

Upgrade member device 2 (subordinate member) with the feature image file **flash:/feature.bin**. (In this example, the image is compatible with the running images.)

```
<Sysname> issu load file feature flash:/feature.bin slot 2
This operation will delete the rollback point information for the previous upgrade and
maybe get unsaved configuration lost. Continue? [Y/N]:Y
Copying file flash:/feature.bin to slot2#flash:/feature.bin......Done.
Upgrade summary according to following table:

flash:/feature.bin
  Running Version              New Version
  Alpha 7122                   Alpha 7123

  Slot                         Upgrade Way
  2                            Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait......Done.
```

Upgrade member device 3 and 4 (subordinate members) with the feature image file **flash:/feature.bin**. (In this example, the image is incompatible with the running images.)

```
<Sysname> issu load file feature flash:/feature.bin slot 3 4
This operation will delete the rollback point information for the previous upgrade and
maybe get unsaved configuration lost. Continue? [Y/N]:Y
Copying file flash:/feature.bin to slot3#flash:/feature.bin......Done.
Copying file flash:/feature.bin to slot4#flash:/feature.bin......Done.
Upgrade summary according to following table:

flash:/feature.bin
  Running Version              New Version
  Alpha 7122                   Alpha 7123

  Slot                         Upgrade Way
  3                            Reboot
  4                            Reboot
Upgrading software images to incompatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait......Done.
```

Table 7 Command output

Field	Description
Slot	Member ID of the device in the IRF fabric.
Upgrade Way	ISSU method: • **Service Upgrade**—Service-level incremental upgrade. • **File Upgrade**—File-level incremental upgrade. • **ISSU Reboot**—Reboots CPUs to complete the upgrade. • **Reboot**—Reboots the entire device to complete the upgrade. For more information about ISSU methods, see *Fundamentals Configuration Guide*.

issu rollback

Use **issu rollback** to cancel the ISSU and roll back to the original software versions.

Syntax

issu rollback

Views

User view

Predefined user roles

network-admin

Usage guidelines

The device supports automatic rollback and manual rollback. This command performs a manual rollback.

You can perform a manual rollback while an ISSU is in one of the following states:

- Loaded.
- Switching (during an upgrade to a compatible version).
- Switchover (during an upgrade to a compatible version).
- Accepted.

If you perform a manual rollback while an ISSU is in Loading state, the ISSU process ends without changing the original software versions.

When an ISSU to an incompatible version is in Switching state, you cannot perform a manual rollback.

When an ISSU is in Committing state, rollback is not supported.

If the IRF fabric has multiple members, a rollback performed after you execute the **issu run switchover** command cancels all operations performed during the ISSU process, including the master/subordinate switchover operation.

Examples

Roll back to the original software versions.

```
<Sysname> issu rollback
This command will quit the ISSU process and roll back to the previous version. Continue?
[Y/N]:y
```

Related commands

- **issu accept**
- **issu commit**
- **issu load**
- **issu run switchover**

issu rollback-timer

Use **issu rollback-timer** to set the automatic rollback timer.

Use **undo issu rollback-timer** to restore the default.

Syntax

issu rollback-timer *minutes*

undo issu rollback-timer

Default

The automatic rollback interval is 45 minutes.

Views

System view

Predefined user roles

network-admin

Parameters

minutes: Specifies the automatic rollback interval in minutes, in the range of 0 to 120. Setting it to 0 disables the automatic rollback feature.

Usage guidelines

The automatic software version rollback feature is only available on a multichassis IRF fabric during an ISSU to a compatible version.

The system starts the automatic rollback timer when you execute the **issu run switchover** command in a scenario where automatic rollback is supported. If you do not execute the **issu accept** or **issu commit** command before the timer expires, the system automatically rolls back to the software versions before the ISSU.

Change to the automatic rollback interval does not take effect on the ongoing ISSU process.

Examples

Set the automatic rollback timer to 50 minutes.

```
<Sysname> system-view
[Sysname] issu rollback-timer 50
```

Related commands

issu rollback

issu run switchover

Use **issu run switchover** to perform a master/subordinate switchover. If the new and old versions are incompatible, this command also upgrades all members that have not been upgraded.

Syntax

issu run switchover

Views

User view

Predefined user roles

network-admin

Usage guidelines

Use this command on multichassis IRF fabrics.

- For a compatible version, this command performs tasks depending on the ISSU method:
  - **Incremental upgrade**—Performs a process-level master/subordinate switchover for the processes to be upgraded.
  - **Reboot** upgrade or **ISSU upgrade**—Reboots the current master with the old software version, causing the upgraded subordinate member to be elected as the new master.
- For an incompatible version, the **issu load** command splits the IRF fabric into two fabrics, with the upgraded members forming a new fabric. The **issu run switchover** command reboots the

members in the old IRF fabric with the upgrade images. After startup, the members join the new IRF fabric as subordinate members.

At reboot, a subordinate device automatically synchronizes the master device's configuration and status data. You must wait for the synchronization to complete before using the **issu run switchover** command on the subordinate device. To check the synchronization progress, use the **display device** command. The synchronization is completed when all member device are in normal state.

Examples

On a multichassis IRF fabric, perform a master/subordinate switchover during an ISSU to a compatible version.

```
<Sysname> issu run switchover
Upgrade summary according to following table:

flash:/feature.bin
  Running Version              New Version
  Alpha 7122                   Alpha 7123

  Slot                         Switchover Way
  1                            Active standby process switchover
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait.....done
```

On a multichassis IRF fabric, perform a master/subordinate switchover and upgrade members that have not been upgraded (member 1 and member 2) during an ISSU to an incompatible version.

```
<Sysname> issu run switchover
Copying file flash:/feature.bin to slot2#flash:/feature.bin...Done.
Upgrade summary according to following table:

flash:/feature.bin
  Running Version              New Version
  Alpha 7122                   Alpha 7123

  Slot                         Upgrade Way
  1                            Reboot
  2                            Reboot
Upgrading software images to incompatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait.....done
```

Table 8 Command output

Field	Description
Switchover Way	Switchover method: • **Active standby process switchover**—Switch from the active process to the standby process. • **Master subordinate switchover**—Switch from the master to a subordinate member.

For descriptions of other fields, see Table 5.

Related commands

issu load

reset install log-history oldest

Use **reset install log-history oldest** to clear ISSU log entries.

Syntax

reset install log-history oldest *log-number*

Views

User view

Predefined user roles

network-admin

Parameters

log-number: Specifies the number of ISSU log entries to be deleted.

Usage guidelines

This command clears the specified number of log entries, beginning with the oldest log entry.

Examples

Clear the two oldest ISSU log entries.

```
<Sysname> reset install log-history oldest 2
```

Related commands

display install log

reset install rollback oldest

Use **reset install rollback oldest** to clear ISSU rollback points.

Syntax

reset install rollback oldest *point-id*

Views

User view

Predefined user roles

network-admin

Parameters

point-id: Specifies a rollback point by its ID.

Usage guidelines

This command clears the specified rollback point and all rollback points older than the specified rollback point.

Examples

Clear rollback point 2 and all rollback points older than rollback point 2.

```
<Sysname> reset install rollback oldest 2
```

Related commands

display install rollback

New feature: Displaying burst records for interfaces

Displaying burst records for interfaces

You can display burst records for Layer 2 and Layer 3 Ethernet interfaces in any view.

Command reference

display burst-detect interface

Use **display burst-detect interface** to display burst records for interfaces.

Syntax

display burst-detect interface [*interface-type* [*interface-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type [*interface-number*]: Specify an interface by its type and number. If you do not specify the *interface-type* argument, this command displays burst records for all interfaces. If you specify the *interface-type* argument without the *interface-number* argument, this command displays burst records for the interfaces of the specified type.

Usage guidelines

This command displays burst records for only Layer 2 and Layer 3 Ethernet interfaces.

A burst occurs when an output queue on an interface receives traffic exceeding the buffer usage threshold. If no burst occurs on an output queue, this command displays no burst information for the queue.

Examples

Display burst records for all interfaces.

```
<Sysname> display burst-detect interface
Interface FGE1/1/1
Burst record 1
Queue                : 5
Occurred at          : 2016-01-05  03:55:39:922
Duration             : 9199 milliseconds
Peak count           : 7556224 bytes
Threshold            : 16640 bytes
Dropped packets      : 467908550 packets
Dropped bytes        : 29946147200 bytes
Burst record 2
```

```
Queue                  : 5
Occurred at            : 2016-01-04  04:12:42:882
Duration               : 2937 milliseconds
Peak count             : 8458528 bytes
Threshold              : 16640 bytes
Dropped packets        : 126031698 packets
Dropped bytes          : 8066028672 bytes
```

Table 9 Command output

Field	Description
Duration	Number of milliseconds that the burst lasted.
Peak count	Peak byte count during the burst.
Threshold	Buffer usage threshold for the interface. If the buffer usage threshold is set in percentage, the switch displays the number of bytes converted from the percentage.
Dropped packets	Number of packets dropped during the burst.
Dropped bytes	Number of bytes dropped during the burst.

New feature: Loop guard for an OpenFlow instance

Enabling loop guard for an OpenFlow instance

After an OpenFlow instance is deactivated, loops might occur in forwarding traffic in VLANs associated with the OpenFlow instance. To avoid loops, you can enable loop guard for the OpenFlow instance. This feature enables the deactivated OpenFlow instance to create a flow entry for dropping all traffic in theses VLANs.

To enable loop guard 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. Enable loop guard for the OpenFlow instance.	**loop-protection enable**	By default, loop guard is disabled for an OpenFlow instance.

Command reference

loop-protection enable

Use **loop-protection enable** to enable loop guard for an OpenFlow instance.

Use **undo loop-protection enable** to restore the default.

Syntax

loop-protection enable

undo loop-protection enable

Default

Loop guard is disabled for an OpenFlow instance.

Views

OpenFlow instance view

Predefined user roles

network-admin

Usage guidelines

After an OpenFlow instance is deactivated, loops might occur in forwarding traffic in VLANs associated with the OpenFlow instance. To avoid loops, you can enable loop guard for the OpenFlow instance. This feature enables the deactivated OpenFlow instance to create a flow entry for dropping all traffic in theses VLANs.

Examples

Enable loop guard for OpenFlow instance 1.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] loop-protection enable
```

New feature: Shutting down an interface by OpenFlow

Shutting down an interface by OpenFlow

After an interface is shut down by OpenFlow, the **Current state** field displays **OFP DOWN** in the **display interface** command output.

You can use the **undo openflow shutdown** command to bring up an interface shut down by OpenFlow. The interface can also be brought up by port modification messages from controllers.

To shut down an interface by OpenFlow:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Shut down the interface by OpenFlow.	**openflow shutdown**	By default, an interface is not shut down by OpenFlow.

Command reference

openflow shutdown

Use **openflow shutdown** to shut down an interface by OpenFlow.

Use **undo openflow shutdown** to restore the default.

Syntax

openflow shutdown

undo openflow shutdown

Default

An interface is not shut down by OpenFlow.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

After an interface is shut down by OpenFlow, the **Current state** field displays **OFP DOWN** in the **display interface** command output.

You can use the **undo openflow shutdown** command to bring up an interface shut down by OpenFlow. The interface can also be brought up by port modification messages from controllers.

Examples

Shut down FortyGigE 1/1/1 by OpenFlow.

```
<Sysname> system-view
[Sysname] interface fortygige1/1/1
[Sysname-FortyGigE1/1/1] openflow shutdown
```

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

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

ARP attack 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
1. Enter system view.	**system-view**	N/A
2. Ignore the ingress ports of ARP packets during user validity check.	**arp detection port-match-ignore**	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

Predefined user roles

network-admin

Usage guidelines

This command configures ARP attack detection to ignore the ingress port information of ARP packets when the packets are compared with the following entries:

- Static IP source guard bindings.
- DHCP snooping entries.
- 802.1X security entries.

Examples

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

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

Related commands

`arp detection enable`

New feature: Specifying ignored packet fields for the default link-aggregation load sharing

Specifying ignored packet fields for the default link-aggregation load sharing

In the default load sharing mode, an aggregation group might fail to load share traffic in a balanced manner. To resolve the problem, you can configure the device to ignore specific packet fields for link-aggregation load sharing. The specified packet field values are ignored during the load sharing calculation.

To specify ignored packet fields for the default link-aggregation load sharing:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Specify ignored packet fields for the default link-aggregation load sharing.	**link-aggregation load-sharing ignore ethernet-type**	By default, no ignored packet fields are specified for the default link-aggregation load sharing.

Command reference

link-aggregation load-sharing ignore

Use **link-aggregation load-sharing ignore** to specify ignored packet fields for the default link-aggregation load sharing.

Use **undo link-aggregation load-sharing ignore** to restore the default.

Syntax

link-aggregation load-sharing ignore ethernet-type

undo link-aggregation load-sharing ignore

Default

No ignored packet fields are specified for the default link-aggregation load sharing.

Views

System view

Predefined user roles

network-admin

Parameters

ethernet-type: Specifies the EtherType value.

Usage guidelines

In the default load sharing mode, an aggregation group might fail to load share traffic in a balanced manner. To resolve the problem, you can configure the device to ignore specific packet fields for link-aggregation load sharing. The specified packet field values are ignored during the load sharing calculation.

Examples

Configure the device to ignore the EtherType value for the default link-aggregation load sharing.

```
<Sysname> system-view
[Sysname] link-aggregation load-sharing ignore ethernet-type
```

Related commands

link-aggregation global load-sharing mode

New feature: Parity error alarming for entries on forwarding chips

Configuring parity error alarming for entries on forwarding chips

The device detects parity errors in entries on forwarding chips. The parity error alarming feature enables the device to perform the following operations:

- Collects statistics for parity errors at an interval, and issues an alarm if the number of the errors exceeds the alarm threshold.
- Generates logs for the detected parity errors.

To configure parity error alarming for entries on forwarding chips:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the parity error statistics interval for entries on forwarding chips.	**parity-error monitor period** *value*	By default, the parity error statistics interval is 60 seconds.
3. Set the parity error alarm threshold for entries on forwarding chips.	**parity-error monitor threshold** *value*	By default, the parity error alarm threshold is 5000.
4. Enable parity error logging for entries on forwarding chips.	**parity-error monitor log enable**	By default, parity error logging is disabled for entries on forwarding chips.

Command reference

parity-error monitor log enable

Use **parity-error monitor log enable** to enable parity error logging for entries on forwarding chips.

Use **undo parity-error monitor log enable** to disable parity error logging for entries on forwarding chips.

Syntax

parity-error monitor log enable

undo parity-error monitor log enable

Default

Parity error logging is disabled for entries on forwarding chips.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The device detects parity errors in entries on forwarding chips. The parity error logging feature generates logs for the detected parity errors.

Examples

Enable parity error logging for entries on forwarding chips.

```
<Sysname> system-view
[Sysname] parity-error monitor log enable
```

parity-error monitor period

Use **parity-error monitor period** to set the parity error statistics interval for entries on forwarding chips.

Use **undo parity-error monitor period** to restore the default.

Syntax

parity-error monitor period *value*

undo parity-error monitor period

Default

The parity error statistics interval is 60 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies the parity error statistics interval, in the range of 1 to 86400 seconds.

Usage guidelines

The device detects parity errors in entries on forwarding chips, and collects parity error statistics at the interval set by using this command.

Examples

Set the parity error statistics interval to 120 seconds.

```
<Sysname> system-view
[Sysname] parity-error monitor period 120
```

Related commands

parity-error monitor threshold

parity-error monitor threshold

Use **parity-error monitor threshold** to set the parity error alarm threshold for entries on forwarding chips.

Use **undo parity-error monitor threshold** to restore the default.

Syntax

parity-error monitor threshold *value*

undo parity-error monitor threshold

Default

The parity error alarm threshold is 5000.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies the parity error alarm threshold in the range of 1 to 1000000.

Usage guidelines

The device detects and collects statistics for parity errors in entries on forwarding chips. If the number of parity errors in a parity error statistics interval reaches the parity error alarm threshold, the system issues an alarm.

Examples

Set the parity error alarm threshold to 8000.

```
<Sysname> system-view
[Sysname] parity-error monitor threshold 8000
```

Related commands

parity-error monitor period

New feature: Excluding a subnet from load sharing on link aggregations

Excluding a subnet from load sharing on link aggregations

Typically, a link aggregate interface distributes traffic across its Selected member ports. Traffic with the same destination might be distributed to different ports. To forward traffic destined for a host on a subnet out of a fixed member port, you can exclude that subnet from load sharing by specifying it as the management subnet.

When a link aggregate interface receives an ARP packet from the management subnet, the device looks up the sender IP address in the ARP table for a matching entry.

- If no matching entry exists, the device creates an ARP entry on the aggregation member port from which the packet came in. Then, all entry matching traffic will be forwarded out of that member port.
- If an ARP entry already exists on a different port than the link aggregate interface or its member ports, the device does not update that ARP entry. Instead, the device broadcasts an ARP request out of all ports to relearn the ARP entry.

When a link aggregate interface sends an ARP packet to the management subnet, the device sends the packet out of all Selected member ports of the link aggregate interface.

To exclude a subnet from load sharing on link aggregations:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Specify the subnet as the management subnet.	**link-aggregation management-subnet** *ip-address* { *mask* | *mask-length* }	By default, no subnet is specified as the management subnet.

Command reference

link-aggregation management-subnet

Use **link-aggregation management-subnet** to specify a subnet as the management subnet.

Use **undo link-aggregation management-subnet** to remove the management subnet.

Syntax

link-aggregation management-subnet *ip-address* { *mask* **|** *mask-length* }

undo link-aggregation management-subnet

Default

No subnet is specified as the management subnet.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies an IP address in dotted decimal notation.

mask: Specifies the subnet mask in dotted decimal notation.

mask-length: Specifies the subnet mask length. The value range is 1 to 32.

Usage guidelines

The device supports only one management subnet.

Typically, a link aggregate interface distributes traffic across its Selected member ports. Traffic with the same destination might be distributed to different ports. To forward traffic destined for a host on a subnet out of a fixed member port, you can exclude that subnet from load sharing by specifying it as the management subnet.

Examples

Specify 22.1.1.1 255.0.0.0 as the management subnet.

```
<Sysname> system-view
[Sysname] link-aggregation management-subnet 22.1.1.1 255.0.0.0
```

New feature: ISP domain for users assigned to nonexistent domains

Specifying an ISP domain for users assigned to nonexistent domains

Perform this task to specify an ISP domain to accommodate users that are assigned to nonexistent domains.

The device chooses an authentication domain for each user in the following order:

1. The authentication domain specified for the access module.
2. The ISP domain in the username.
3. The default ISP domain of the device.

If the chosen domain does not exist on the device, the device searches for the ISP domain that accommodates users that are assigned to nonexistent domains. If no such ISP domain is configured, user authentication fails.

To specify an ISP domain to accommodate users that are assigned to nonexistent domains:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Specify an ISP domain to accommodate users that are assigned to nonexistent domains.	**domain if-unknown** *isp-domain-name*	By default, no ISP domain is specified to accommodate users that are assigned to nonexistent domains.

Command reference

domain if-unknown

Use **domain if-unknown** to specify an ISP domain to accommodate users that are assigned to nonexistent domains.

Use **undo domain if-unknown** to restore the default.

Syntax

domain if-unknown *isp-domain-name*

undo domain if-unknown

Default

No ISP domain is specified to accommodate users that are assigned to nonexistent domains.

Views

System view

Predefined user roles

network-admin

Parameters

isp-domain-name: Specifies the ISP domain name, a case-insensitive string of 1 to 24 characters. The name must meet the following requirements:

- The name cannot contain a forward slash (/), backslash (\), vertical bar (|), quotation marks ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@).
- The name cannot be **d**, **de**, **def**, **defa**, **defau**, **defaul**, **default**, **i**, **if**, **if-**, **if-u**, **if-un**, **if-unk**, **if-unkn**, **if-unkno**, **if-unknow**, or **if-unknown**.

Usage guidelines

The device chooses an authentication domain for each user in the following order:

1. The authentication domain specified for the access module.
2. The ISP domain in the username.
3. The default ISP domain of the device.

If the chosen domain does not exist on the device, the device searches for the ISP domain that accommodates users that are assigned to nonexistent domains. If no such ISP domain is configured, user authentication fails.

Examples

Specify ISP domain **test** to accommodate users that are assigned to nonexistent domains.

```
<Sysname> system-view
[Sysname] domain if-unknown test
```

Related commands

display domain

Modified feature: Displaying operating information for diagnostics

Feature change description

The **display diagnostic-information** command saves operating information for diagnostics to a default file if you choose to save the information but do not specify a file name. The file name includes the device name and the system time when the command is executed.

In previous releases, the saving operation fails if the device name contains any of the following special characters: forward slash (/), backward slash (\ ), colon (:),asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), and vertical bar (|). In this release, a special character in the device name is replaced with an underscore sign (_). For example, if the device name is **A/B**, the command uses a file name like **flash:/diag_A_B_20160101-000438.tar.gz**.

Command changes

Modified command: display diagnostic-information

Syntax

display diagnostic-information [**hardware | infrastructure | l2 | l3 | service**] [*filename*]

Views

Any view

Change description

Before modification: The **display diagnostic-information** command cannot save operating information to the default diagnostics file if the device name contains any of the following special characters: forward slash (/), backward slash (\ ), colon (:),asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), and vertical bar (|).

After modification: The **display diagnostic-information** command can save operating information to the default diagnostics file successfully even if the device name contains special characters. The special characters in the file name are replaced with underscore signs (_).

Modified feature: Displaying history about ports that are blocked by spanning tree protection features

Feature change description

The **display stp abnormal-port** command can display history about ports that are blocked by spanning tree protection features.

Command changes

Modified command: display stp abnormal-port

Syntax

display stp abnormal-port

Views

Any view

Change description

Before modification, the command displays the following information:

```
<Sysname> display stp abnormal-port
 MST ID      Blocked Port                   Reason
 1           FortyGigE1/1/1                 Root-Protected
 2           FortyGigE1/1/2                 Loop-Protected
 12          FortyGigE1/1/3                 Loopback-Protected
```

After modification, the command displays the following information:

```
<Sysname> display stp abnormal-port
---[FortyGigE1/1/1]---
    MST ID   BlockReason                     Time
    0        Loopback-Protected              07:56:44 02/01/2011
    0        Disputed                        07:56:37 02/01/2011
    0        Loop-Protected                  06:56:13 02/01/2011
---[FortyGigE1/1/2]---
    MST ID   BlockReason                     Time
    0        Loopback-Protected              07:55:51 02/01/2011
```

In an MSTI or VLAN, this command can display a maximum of three history records for a blocked port. The **BlockReason** field displays the reason why the port was blocked. The **Time** field displays the spanning tree protection feature trigger time.

Modified feature: Displaying BGP MDT peer or peer group information

Feature change description

In this release, you can display backup BGP MDT peer or peer group information for the specified IRF member device.

Command changes

Modified command: display bgp peer

Old syntax

display bgp peer ipv4 [**mdt**] [*ip-address mask-length* **|** { *ip-address* **|** *group-name* } **log-info |** [[*ip-address*] **verbose**]]

display bgp peer ipv4 [**unicast**] [**vpn-instance** *vpn-instance-name*] [*ip-address mask-length* **|** { *ip-address* **|** *group-name* } **log-info |** [[*ip-address*] **verbose**]]

display bgp peer ipv6 [**unicast**] [**vpn-instance** *vpn-instance-name*] [*ipv6-address prefix-length* **|** { *ipv6-address* **|** *group-name* } **log-info |** [[*ipv6-address*] **verbose**]]

display bgp peer ipv6 [**unicast**] [*ip-address mask-length* | *ip-address* **log-info |** [[*ip-address*] **verbose**]]

display bgp peer vpnv4 [**vpn-instance** *vpn-instance-name*] [*ip-address mask-length* **|** { *ip-address* **|** *group-name* } **log-info |** [[*ip-address*] **verbose**]]

display bgp peer { **l2vpn | vpnv6** } [*ip-address mask-length* **|** { *ip-address* **|** *group-name* } **log-info |** [[*ip-address*] **verbose**]]

New syntax

display bgp peer ipv4 [**mdt**] [*ip-address mask-length* | { *ip-address* **|** *group-name* } **log-info |** [[*ip-address*] **verbose**] [**standby slot** *slot-number*]]

display bgp peer ipv4 [**unicast**] [**vpn-instance** *vpn-instance-name*] [*ip-address mask-length* **|** { *ip-address* **|** *group-name* } **log-info |** [[*ip-address*] **verbose**] [**standby slot** *slot-number*]]

display bgp peer ipv6 [**unicast**] [**vpn-instance** *vpn-instance-name*] [*ipv6-address prefix-length* **|** { *ipv6-address* **|** *group-name* } **log-info** **|** [[*ipv6-address*] **verbose**] [**standby slot** *slot-number*]]

display bgp peer ipv6 [**unicast**] [*ip-address mask-length* **|** *ip-address* **log-info** **|** [[*ip-address*] **verbose**] [**standby slot** *slot-number*]]

display bgp peer vpnv4 [**vpn-instance** *vpn-instance-name*] [*ip-address mask-length* **|** { *ip-address* **|** *group-name* } **log-info** **|** [[*ip-address*] **verbose**] [**standby slot** *slot-number*]]

display bgp peer { **l2vpn** **|** **vpnv6** } [*ip-address mask-length* **|** { *ip-address* **|** *group-name* } **log-info** **|** [[*ip-address*] **verbose**] [**standby slot** *slot-number*]]

Views

Any view

Change description

After modification, you can display backup BGP MDT peer or peer group information for the specified IRF member device.

Modified feature: Displaying BGP MDT routing information

Feature change description

In this release, you can display backup BGP MDT routing information for the specified member device.

Command changes

Modified command: display bgp routing-table ipv4 mdt

Old syntax

display bgp routing-table ipv4 mdt [**route-distinguisher** *route-distinguisher*] [*ip-address* [**advertise-info**]]

New syntax

display bgp routing-table ipv4 mdt [**route-distinguisher** *route-distinguisher*] [*ip-address* [**advertise-info**]] [**standby slot** *slot-number*]

Views

Any view

Change description

After modification, you can display backup BGP MDT routing information for the specified member device.

Modified feature: Applying an ACL to an interface for packet filtering

Feature change description

In this release, Layer 2 aggregate interface view and Layer 3 aggregate interface view were added to the **packet-filter** command. However, you can apply an ACL only to the inbound direction of a Layer 2 or Layer 3 aggregate interface.

Command changes

Modified command: packet-filter

Syntax

packet-filter [**ipv6**] { *acl-number* **| name** *acl-name* } { **inbound | outbound** } [**hardware-count**]

undo packet-filter [**ipv6**] { *acl-number* **| name** *acl-name* } { **inbound | outbound** }

Views

Layer 2/Layer 3 Ethernet interface view

Layer 2/Layer 3 aggregate interface view

VLAN interface view

S-channel interface/S-channel aggregate interface view

Change description

After modification, you can apply an ACL to the inbound direction of a Layer 2 or Layer 3 aggregate interface for packet filtering.

Modified feature: Applying a QoS policy to an interface

Feature change description

In this release, Layer 2 aggregate interface view and Layer 3 aggregate interface view were added to the **qos apply policy** command. However, a QoS policy applied to the outbound direction of a Layer 2 or Layer 3 aggregate interface can only contain the mirroring action.

Command changes

Modified command: qos apply policy

Syntax

qos apply policy *policy-name* { **inbound | outbound** }

undo qos apply policy *policy-name* { **inbound** | **outbound** }

Views

Control plane view

Layer 2/Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Layer 2/Layer 3 aggregate interface view

S-channel interface/S-channel aggregate interface view

Change description

After modification, you can apply a QoS policy to a Layer 2 or Layer 3 aggregate interface.

Modified feature: Configuring data buffer monitoring

Feature change description

In this release, you can set a per-interface buffer usage threshold in bytes.

Command changes

Modified command: buffer usage threshold

Old syntax

buffer usage threshold slot *slot-number* **ratio** *ratio*

New syntax

buffer usage threshold slot *slot-number* { **ratio** *ratio* | *size* }

Views

System view

Change description

After modification, you can set a per-interface buffer usage threshold in percentage or in bytes.

Modified feature: Defining QoS match criteria

Feature change description

This release added support for matching different traffic types (broadcast, multicast, unicast, and unknown unicast traffic).

Command changes

Modified command: if-match

Syntax

if-match *match-criteria*

undo if-match *match-criteria*

Views

Traffic class view

Change description

After modification, the **traffic-type** { **broadcast** | **multicast** | **unicast** | **unknown-unicast** } parameter was added for the command to match broadcast, multicast, unicast, or unknown unicast traffic.

Modified feature: Software patching

Feature change description

Before modification: A new patch package covers all functions provided by the previous patch package. The device can load only one patch package. Loading a new patch package overwrites the previous patch package.

After modification: A new patch package might not cover all functions provided by the previous patch package.

- If a new patch package covers all functions provided by the previous patch package, loading the patch package overwrites the previous patch package.
- If a new patch package does not cover one or more functions provided by the previous patch package, loading the patch package does not affect the previous patch package. The device uses both of the patch packages.

Modified feature: User password configuration in RADIUS test profiles

Feature change description

Support for user password configuration was added to RADIUS test profiles. The device includes the user password of a test profile into the detection packets to detect the status of a RADIUS server that is specified to use the test profile. The user password prevents the RADIUS server from mistaking detection packets that contain randomly generated passwords as attack packets.

Command changes

Modified command: radius-server test-profile

Old syntax

radius-server test-profile *profile-name* username *name* [interval *interval*]

undo radius-server test-profile *profile-name*

New syntax

radius-server test-profile profile-name username name [password { cipher | simple } string] [interval interval]

undo radius-server test-profile profile-name

Views

System view

Change description

Before modification: User password configuration is not supported when you use this command. The device randomly generates a user password for each detection packet.

After modification: The **password** { **cipher | simple** } *string* option was added to this command.

- **password**: Specifies the user password in the detection packets. If you do not specify a user password, the device randomly generates a user password for each detection packet. As a best practice to prevent the RADIUS server from mistaking detection packets that contain randomly generated passwords as attack packets, specify a user password.
- **cipher**: Specifies the password in encrypted form.
- **simple**: Specifies the password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.
- *string*: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

Modified feature: Configuring SSH client access control

Feature change description

The **mac** keyword was removed from the command for configuring an SSH login control ACL.

Command changes

Modified command: ssh server acl

Old syntax

ssh server acl { *advanced-acl-number* | *basic-acl-number* | **mac** *mac-acl-number* }

undo ssh server acl

New syntax

ssh server acl { *advanced-acl-number* **|** *basic-acl-number* **|** *mac-acl-number* }

undo ssh server acl

Views

System view

Change description

The **mac** *mac-acl-number* option was changed to the *mac-acl-number* argument to specify a Layer 2 ACL.

Modified command: ssh server ipv6 acl

Old syntax

ssh server ipv6 acl { **ipv6** { *advanced-acl-number* **|** *basic-acl-number* } **| mac** *mac-acl-number* }

undo ssh server ipv6 acl

New syntax

ssh server ipv6 acl { **ipv6** { *advanced-acl-number* **|** *basic-acl-number* } **|** *mac-acl-number* }

undo ssh server ipv6 acl

Views

System view

Change description

The **mac** *mac-acl-number* option was changed to the *mac-acl-number* argument to specify a Layer 2 ACL.

Modified feature: Predefined user roles of SSH client and FTP client commands

Feature change description

Predefined user roles were changed for the following SSH client and FTP client commands:

- **bye**
- **exit**
- **help**
- **quit**

Command changes

Modified command: bye

Syntax

bye

Views

SFTP client view, FTP client view

Old predefined user roles

network-admin

New predefined user roles

network-admin

network-operator

Modified command: exit

Syntax

exit

Views

SFTP client view

Old predefined user roles

network-admin

New predefined user roles

network-admin

network-operator

Modified command: help

Syntax

help

Views

SFTP client view, FTP client view

Old predefined user roles

network-admin

New predefined user roles

network-admin

network-operator

Modified command: quit

Syntax

quit

Views

SFTP client view, FTP client view

Old predefined user roles

network-admin

New predefined user roles

network-admin

network-operator

Modified feature: Username format modification for device login

Feature change description

Before modification: To log in to the device with a username that carries the ISP domain, the user must follow the *username@domain* format to enter the username.

After modification: To log in to the device with a username that carries the ISP domain, the user can use one of the following formats: *username@domain*, *username/domain*, and *domain\username.*

Command changes

None.

Modified feature: Specifying a PW data encapsulation type

Feature change description

In this release, you can force the device to use the Ethernet or VLAN encapsulation type to negotiate with peers for BGP VPLS PW establishment.

Command changes

Modified command: pw-type

Old syntax

pw-type { **ethernet** | **vlan** }

undo pw-type

New syntax

pw-type { **ethernet** | **vlan** } [**force-for-vpls**]

undo pw-type

Views

PW class view

Change description

Before modification: For the device to establish a BGP VPLS PW with a Comware 5 device, the Comware 5 device must use the BGP-VPLS encapsulation type.

After modification: The **force-for-vpls** keyword was added. It forces VPLS to use the Ethernet or VLAN encapsulation type to establish a BGP PW with a Comware 5 device that uses the Ethernet or VLAN encapsulation type.

Modified feature: Device diagnostic information

Feature change description

The **key-info** keyword was added to the **display diagnostic-information** command to help you focus on critical device diagnostic information.

Command changes

Modified command: display diagnostic-information

Old syntax

display diagnostic-information [**hardware | infrastructure | l2 | l3 | service**] [*filename*]

New syntax

display diagnostic-information [**hardware** | **infrastructure** | **l2** | **l3** | **service**] [**key-info**] [*filename*]

Views

Any view

Change description

Before modification: The command does not support the **key-info** keyword.

After modification: The command supports the **key-info** keyword.

Modified feature: Memory usage statistics

Feature change description

The output from the **display memory** command changed.

Command changes

Modified command: display memory

Syntax

display memory [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Change description

Before modification, the output from the command is as follows:

```
<Sysname>display memory
The statistics about memory is measured in KB:
Slot 10:
             Total       Used       Free     Shared    Buffers     Cached   FreeRatio
Mem:       3854876     651188    3203688          0        740     157844       83.3%
-/+ Buffers/Cache:     492604    3362272
Swap:          0        0        0After modification: The command supports the key-info
keyword.
```

After modification, the output from the command is as follows:

```
<Sysname>display memory
The statistics about memory is measured in KB:
Slot 10:
             Total       Used       Free     Shared    Buffers     Cached   FreeRatio
Mem:       3854876     651188    3203688          0        740     157844       83.3%
-/+ Buffers/Cache:     492604    3362272
Swap:            0          0          0
LowMem:     709152     303772     405380         --         --         --       57.2%
HighMem:   3145724     347416    2798308         --         --         --       89.0%
```

The following fields were added to the output:

- **LowMem**—Low-memory usage information.
- **HighMem**—High-memory usage information.

Modified feature: Displaying group table statistics

Feature change description

In this release, the command output of the **display openflow group** command displays the byte count and packet count for each action bucket in a group table.

Command changes

Modified command: display openflow group

Syntax

display openflow instance *instance-id* **group** [*group-id*]

Views

Any view

Change description

Before modification: The command output does not support displaying the byte count and packet count for an action bucket.

```
<Sysname> display openflow instance 10 group
Instance 10 group table information:
 Group count: 1

Group entry 1:
 Type: All, byte count: --, packet count: --
 Bucket 1 information:
Action count 1, watch port: any, watch group: any
Byte count --, packet count --
  Output interface: FGE1/1/1
```

After modification: The command output supports displaying the byte count and packet count for an action bucket.

```
<Sysname> display openflow instance 10 group
Instance 10 group table information:
 Group count: 1

Group entry 1:
 Type: All, byte count: 55116, packet count: 401
 Bucket 1 information:
Action count 1, watch port: any, watch group: any
Byte count 55116, packet count 401
  Output interface: FGE1/1/1
```

F2428

This release has the following changes:

- New feature: Configuring the RIB to flush route attribute information to the FIB
- New feature: Displaying the outbound PBR configuration and statistics for an interface
- New feature: RADIUS stop-accounting packet buffering
- New feature: HWTACACS stop-accounting packet buffering
- New feature: 802.1X MAC address binding
- New feature: Support of 802.1X for redirect URL assignment
- New feature: Support of MAC authentication for redirect URL assignment
- New feature: Support of port security for redirect URL assignment in specific modes
- New feature: Specifying ITU channel numbers for transceiver modules
- New feature: Configuring the DHCP smart relay feature
- New feature: Configuring a description for a network access user
- New feature: Configuring the validity period for a network access user
- New feature: Enabling the auto-delete feature for expired local user accounts
- New feature: Configuring periodic MAC reauthentication
- New feature: Enabling preprovisioning
- New feature: Enabling SNMP notifications for RRPP
- Modified feature: Displaying PBR configuration
- Modified feature: Displaying MAC address table information for VSIs
- Modified feature: Enabling the BFD echo packet mode
- Modified feature: NTP authentication
- Modified feature: Displaying MAC address move records
- Modified feature: MAC address move notifications
- Modified feature: Default size of the TCP receive and send buffer
- Modified feature: Displaying MPLS LSP statistics
- Modified feature: Configuring BGP route summarization
- Modified feature: Displaying OSI connection information

New feature: Configuring the RIB to flush route attribute information to the FIB

Configuring the RIB to flush route attribute information to the FIB

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Enter RIB view.	**rib**	N/A
3. Create the RIB IPv4 address family, and enter its view.	**address-family ipv4**	By default, no RIB IPv4 address family exists.
4. Configure the RIB to flush route attribute information to the FIB.	**flush route-attribute** *protocol*	By default, the RIB does not flush route attribute information to the FIB.

Command reference

flush route-attribute

Use **flush route-attribute** to configure the RIB to flush route attribute information to the FIB.

Use **undo flush route-attribute** to remove the configuration.

Syntax

flush route-attribute *protocol*

undo flush route-attribute *protocol*

Default

The RIB does not flush route attribute information to the FIB.

Views

RIB IPv4 address family view

Predefined user roles

network-admin

Parameters

protocol: Specifies a protocol. Only BGP is supported.

Examples

Configure the RIB to flush BGP route attribute information to FIB.

```
<Sysname> system-view
[Sysname] rib
[Sysname-rib] address-family ipv4
[Sysname-rib-ipv4] flush route-attribute bgp
```

New feature: Displaying the outbound PBR configuration and statistics for an interface

Displaying the outbound PBR configuration and statistics for an interface

If you have configured outbound PBR on an interface, use the **display ip policy-based-route egress interface** command to display the outbound PBR configuration and statistics for the interface.

Command reference

display ip policy-based-route egress interface

Use **display ip policy-based-route egress interface** to display the outbound PBR configuration and statistics for an interface.

Syntax

display ip policy-based-route egress interface *interface-type interface-number* [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for the specified interface on the master device.

Examples

Display the outbound PBR configuration and statistics for Tunnel 0.

```
<Sysname> display ip policy-based-route egress interface Tunnel 0
Policy based routing information for interface Tunnel0:
Policy name: aaa
  node 0 deny:
  Matched: 0
  node 1 permit:
    if-match acl 3999
  Matched: 0
  node 2 permit:
    if-match acl 2000
```

```
    apply next-hop 2.2.2.2
  Matched: 0
  node 5 permit:
    if-match acl 3101
    apply next-hop 1.1.1.1
    apply output-interface Ten-gigabitethernet1/0/2 track 1
    apply output-interface Ten-gigabitethernet1/1/3 track 2
  Matched: 0
Total matched: 0
```

Table 1 Command output

Field	Description
Policy based routing information for interface *xxxx*(failed)	Outbound PBR configuration and statistics for the interface. **NOTE:** If you specify a slot number, this field displays **failed** in brackets for a policy that failed to be issued to the driver. The failure means that all node configurations in the PBR policy failed to be issued.
node 0 deny(not support) node 2 permit(no resource)	Match mode of the node, **permit** or **deny**. **NOTE:** If you specify a slot number, this field displays the cause in brackets for a node that does not take effect: • **not support**—The device does not support the match criteria configured on the node. • **no resource**—The node does not have sufficient resources (for example, ACLs).
if-match acl	Compares packets with the ACL.
apply next-hop	Specifies a next hop for permitted packets.
apply output-interface *xxxx* track 1 (down)	Specifies an output interface and its associated track entry for permitted packets. This field displays the interface status in brackets. • **up**—The interface is up. • **down**—The interface is down at the network layer. • **inactive**—The card that hosts the interface is not in position.
Matched: 0 (no statistics resource)	Number of successful matches on the node. **NOTE:** If you specify a slot number but the device does not have sufficient resources to collect statistics on the slot, this field displays **no statistics resource** in brackets.
Total matched	Total number of successful matches on all nodes.

Related commands

reset ip policy-based-route statistics

New feature: RADIUS stop-accounting packet buffering

Configuring RADIUS stop-accounting packet buffering

The device sends RADIUS stop-accounting requests when it receives connection teardown requests from hosts or connection teardown commands from an administrator. However, the device might fail to receive a response for a stop-accounting request in a single transmission.

Enable the device to buffer RADIUS stop-accounting requests that have not received responses from the accounting server. The device will resend the requests until responses are received.

To limit the transmission times, set a maximum number of transmission attempts that can be made for individual RADIUS stop-accounting requests. When the maximum attempts are made for a request, the device discards the buffered request.

To configure RADIUS stop-accounting packet buffering:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter RADIUS scheme view.	**radius scheme** *radius-scheme-name*	N/A
3. Enable buffering of RADIUS stop-accounting requests to which no responses have been received.	**stop-accounting-buffer enable**	By default, the buffering feature is enabled.
4. Set the maximum number of transmission attempts for individual RADIUS stop-accounting requests.	**retry stop-accounting** *retries*	The default setting is 500.
5. Return to system view.	**quit**	N/A
6. Display information about buffered RADIUS stop-accounting requests to which no responses have been received.	**display stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time end-time* | **user-name** *user-name* }	N/A
7. Return to user view.	**quit**	N/A
8. Clear the buffered RADIUS stop-accounting requests to which no responses have been received.	**reset stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time end-time* | **user-name** *user-name* }	N/A

Command reference

display stop-accounting-buffer (for RADIUS)

Use **display stop-accounting-buffer** to display information about buffered RADIUS stop-accounting requests to which no responses have been received.

Syntax

display stop-accounting-buffer { **radius-scheme** *radius-scheme-name* **|** **session-id** *session-id* **|** **time-range** *start-time end-time* **|** **user-name** *user-name* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

session-id *session-id*: Specifies a session by its ID. The *session-id* argument is a string of 1 to 64 characters and cannot contain a letter. A session ID uniquely identifies an online user for a RADIUS scheme.

time-range *start-time end-time*: Specifies a time range. The start time and end time must be in the format of hh:mm:ss-MM/DD/YYYY or hh:mm:ss-YYYY/MM/DD.

user-name *user-name*: Specifies a user by its name, a case-sensitive string of 1 to 255 characters. Whether the *user-name* argument should include the domain name depends on the setting configured by the **user-name-format** command for the RADIUS scheme.

Examples

Display information about nonresponded RADIUS stop-accounting requests buffered for user **abc**.

```
<Sysname> display stop-accounting-buffer user-name abc
Total entries: 2
Scheme     Session ID          Username    First sending time   Attempts
rad1       1000326232325010    abc         23:27:16-08/31/2015  19
aaa        1000326232326010    abc         23:33:01-08/31/2015  20
```

Table 2 Command output

Field	Description
First sending time	Time when the stop-accounting request was first sent.
Attempts	Number of attempts that the stop-accounting request has been sent.

Related commands

reset stop-accounting-buffer (for RADIUS)

retry

retry stop-accounting (RADIUS scheme view)

stop-accounting-buffer enable (RADIUS scheme view)

user-name-format (RADIUS scheme view)

reset stop-accounting-buffer (for RADIUS)

Use **reset stop-accounting-buffer** to clear buffered RADIUS stop-accounting requests to which no responses have been received.

Syntax

reset stop-accounting-buffer { **radius-scheme** *radius-scheme-name* **|** **session-id** *session-id* **|** **time-range** *start-time end-time* **|** **user-name** *user-name* }

Views

User view

Predefined user roles

network-admin

Parameters

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

session-id *session-id*: Specifies a session by its ID. The *session-id* argument is a string of 1 to 64 characters and cannot contain a letter. A session ID uniquely identifies an online user for a RADIUS scheme.

time-range *start-time end-time*: Specifies a time range. The start time and end time must be in the format of hh:mm:ss-MM/DD/YYYY or hh:mm:ss-YYYY/MM/DD.

user-name *user-name*: Specifies a user by its name, a case-sensitive string of 1 to 255 characters. Whether the *user-name* argument should include the domain name depends on the setting configured by the **user-name-format** command for the RADIUS scheme.

Examples

Clear nonresponded RADIUS stop-accounting requests buffered for user **user0001@test**.

```
<Sysname> reset stop-accounting-buffer user-name user0001@test
```

Clear nonresponded RADIUS stop-accounting requests buffered from 0:0:0 to 23:59:59 on August 31, 2015.

```
<Sysname> reset stop-accounting-buffer time-range 00:00:00-08/31/2015
23:59:59-08/31/2015
```

Related commands

display stop-accounting-buffer (for RADIUS)

stop-accounting-buffer enable (RADIUS scheme view)

retry stop-accounting (RADIUS scheme view)

Use **retry stop-accounting** to set the maximum number of transmission attempts for individual RADIUS stop-accounting requests.

Use **undo retry stop-accounting** to restore the default.

Syntax

retry stop-accounting *retries*

undo retry stop-accounting

Default

The maximum number of transmission attempts is 500 for individual RADIUS stop-accounting requests.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

retries: Specifies the maximum number of transmission attempts. The value range is 10 to 65535.

Usage guidelines

The maximum number of stop-accounting request transmission attempts controls the transmission of stop-accounting requests together with the following parameters:

- RADIUS server response timeout timer (set by using the **timer response-timeout** command).
- Maximum number of times to transmit a RADIUS packet per round (set by using the **retry** command).

For example, the following settings exist:

- The RADIUS server response timeout timer is 3 seconds.
- The maximum number of times to transmit a RADIUS packet per round is five.
- The maximum number of stop-accounting request transmission attempts is 20.

A stop-accounting request is retransmitted if the device does not receive a response within 3 seconds. When all five transmission attempts in this round are used, the device buffers the request and starts another round of retransmission. If 20 consecutive rounds of attempts fail, the device discards the request.

Examples

Set the maximum number of stop-accounting request transmission attempts to 1000 for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry stop-accounting 1000
```

Related commands

display stop-accounting-buffer (for RADIUS)

retry

timer response-timeout (RADIUS scheme view)

stop-accounting-buffer enable (RADIUS scheme view)

Use **stop-accounting-buffer enable** to enable buffering of RADIUS stop-accounting requests to which no responses have been received.

Use **undo stop-accounting-buffer enable** to disable the buffering feature.

Syntax

stop-accounting-buffer enable

undo stop-accounting-buffer enable

Default

The device buffers the RADIUS stop-accounting requests to which no responses have been received.

Views

RADIUS scheme view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to buffer a RADIUS stop-accounting request to which no response is received after the maximum transmission times (set by using the **retry** command) are made. The device resends the buffered request until it receives a server response or when the number of stop-accounting request transmission attempts reaches the upper limit. If no more attempts are available, the device discards the request. However, if you have removed an accounting server, stop-accounting requests destined for the server are not buffered.

Examples

Enable buffering of RADIUS stop-accounting requests to which no responses have been received.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] stop-accounting-buffer enable
```

Related commands

display stop-accounting-buffer (for RADIUS)

reset stop-accounting-buffer (for RADIUS)

New feature: HWTACACS stop-accounting packet buffering

Configuring HWTACACS stop-accounting packet buffering

The device sends HWTACACS stop-accounting requests when it receives connection teardown requests from hosts or connection teardown commands from an administrator. However, the device might fail to receive a response for a stop-accounting request in a single transmission.

Enable the device to buffer HWTACACS stop-accounting requests that have not received responses from the accounting server. The device will resend the requests until responses are received.

To limit the transmission times, set a maximum number of attempts that can be made for transmitting individual HWTACACS stop-accounting requests. When the maximum attempts are made for a request, the device discards the buffered request.

To configure HWTACACS stop-accounting packet buffering:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter HWTACACS scheme view.	**hwtacacs scheme** *hwtacacs-scheme-name*	N/A
3. Enable buffering of HWTACACS stop-accounting requests to which no responses have been	**stop-accounting-buffer enable**	By default, the buffering feature is enabled.

Step	Command	Remarks
received.		
4. Set the maximum number of transmission attempts for individual HWTACACS stop-accounting requests.	**retry stop-accounting** *retries*	The default setting is 100.
5. Return to system view.	**quit**	N/A
6. Display information about buffered HWTACACS stop-accounting requests to which no responses have been received.	**display stop-accounting-buffer hwtacacs-scheme** *hwtacacs-scheme-name*	N/A
7. Return to user view.	**quit**	N/A
8. Clear the buffered HWTACACS stop-accounting requests to which no responses have been received.	**reset stop-accounting-buffer hwtacacs-scheme** *hwtacacs-scheme-name*	N/A

Command reference

display stop-accounting-buffer (for HWTACACS)

Use **display stop-accounting-buffer** to display information about buffered HWTACACS stop-accounting requests to which no responses have been received.

Syntax

display stop-accounting-buffer hwtacacs-scheme *hwtacacs-scheme-name*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

Examples

Display information about nonresponded stop-accounting requests buffered for HWTACACS scheme **hwt1**.

```
<Sysname> display stop-accounting-buffer hwtacacs-scheme hwt1
Total entries: 2
Scheme    IP address        Username      First sending time      Attempts
hwt1      192.168.100.1     abc           23:27:16-08/31/2015     19
hwt1      192.168.90.6      bob           23:33:01-08/31/2015     20
```

Table 10 Command output

Field	Description
First sending time	Time when the stop-accounting request was first sent.
Attempts	Number of attempts that the stop-accounting request has been sent.

Related commands

reset stop-accounting-buffer (for HWTACACS)

retry stop-accounting (HWTACACS scheme view)

stop-accounting-buffer enable (HWTACACS scheme view)

user-name-format (HWTACACS scheme view)

reset stop-accounting-buffer (for HWTACACS)

Use **reset stop-accounting-buffer** to clear buffered HWTACACS stop-accounting requests to which no responses have been received.

Syntax

reset stop-accounting-buffer hwtacacs-scheme *hwtacacs-scheme-name*

Views

User view

Predefined user roles

network-admin

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

Examples

Clear nonresponded stop-accounting requests buffered for HWTACACS scheme **hwt1**.

```
<Sysname> reset stop-accounting-buffer hwtacacs-scheme hwt1
```

Related commands

display stop-accounting-buffer (for HWTACACS)

stop-accounting-buffer enable (HWTACACS scheme view)

retry stop-accounting (HWTACACS scheme view)

Use **retry stop-accounting** to set the maximum number of transmission attempts for individual HWTACACS stop-accounting requests.

Use **undo retry stop-accounting** to restore the default.

Syntax

retry stop-accounting *retries*

undo retry stop-accounting

Default

The maximum number of transmission attempts for individual HWTACACS stop-accounting requests is 100.

Views

HWTACACS scheme view

Predefined user roles

network-admin

Parameters

retries: Specifies the maximum number of transmission attempts for HWTACACS stop-accounting requests. The value range is 1 to 300.

Examples

In HWTACACS scheme **hwt1**, set the maximum number of HWTACACS stop-accounting attempts to 300.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] retry stop-accounting 300
```

Related commands

display stop-accounting-buffer (for HWTACACS)

timer response-timeout (HWTACACS scheme view)

stop-accounting-buffer enable (HWTACACS scheme view)

Use **stop-accounting-buffer enable** to enable buffering of HWTACACS stop-accounting requests to which no responses are received.

Use **undo stop-accounting-buffer enable** to disable buffering of HWTACACS stop-accounting requests to which no responses are received.

Syntax

stop-accounting-buffer enable

undo stop-accounting-buffer enable

Default

The device buffers HWTACACS stop-accounting requests to which no responses have been received.

Views

HWTACACS scheme view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to buffer an HWTACACS stop-accounting request to which no response has been received. The device resends the buffered request until it receives a server response or when the number of transmission attempts reaches the maximum (set by using the **retry stop-accounting** command). If no more attempts are available, the device discards the request. However, if you have removed an accounting server, stop-accounting requests destined for the server are not buffered.

Examples

Enable buffering of HWTACACS stop-accounting requests to which no responses have been received.

```
<Sysname> system-view
```

```
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] stop-accounting-buffer enable
```

Related commands

display stop-accounting-buffer (for HWTACACS)

reset stop-accounting-buffer (for HWTACACS)

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 mac-binding** *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. If users in the 802.1X MAC address binding entries perform 802.1X authentication on another port, they cannot pass authentication.

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.
- To delete an 802.1X MAC address binding entry, you must use the **undo dot1x mac-binding** *mac-address* command. 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 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Enable the 802.1X MAC address binding feature.	**dot1x mac-binding enable**	By default, the feature is disabled.
4. (Optional.) Manually configure 802.1X MAC address binding entries.	**dot1x mac-binding** *mac-address*	By default, no 802.1X MAC address binding entries are configured on a port.

Command reference

dot1x mac-binding enable

Use **dot1x mac-binding enable** to enable the 802.1X MAC address binding feature.

Use **undo dot1x mac-binding enable** to disable the 802.1X MAC address binding feature.

Syntax

dot1x mac-binding enable

undo dot1x mac-binding enable

Default

The 802.1X MAC address binding feature is disabled.

Views

Ethernet interface view

Predefined user roles

network-admin

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 mac-binding** *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 Ten-GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] dot1x mac-binding enable
```

Related commands

dot1x

dot1x mac-binding

dot1x port-method

dot1x mac-binding

Use **dot1x mac-binding** to configure an 802.1X MAC address binding entry.

Use **undo dot1x mac-binding** to delete the specified 802.1X MAC address binding entries.

Syntax

dot1x mac-binding *mac-address*

undo dot1x mac-binding { *mac-address* **| all** }

Default

No 802.1X MAC address binding entries are configured on a port.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a MAC address, in the format of H-H-H, excluding broadcast, multicast, and all-zero MAC addresses.

all: Specifies all MAC addresses that are bound to a port.

Usage guidelines

This command takes effect only when 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 mac-binding** *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 Ten-GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] dot1x mac-binding 000a-eb29-75f1
```

New feature: Support of 802.1X for redirect URL assignment

The device supports the URL attribute assigned by a RADIUS server when the 802.1X-enabled port performs MAC-based access control and the port authorization state is **auto**. During authentication, an 802.1X user is redirected to the Web interface specified by the server-assigned URL attribute. After the user passes the Web authentication, the RADIUS server records the MAC address of the Web user and uses a DM (Disconnect Message) to log off the Web user. When the user initiates 802.1X authentication again, it will pass the authentication and come online successfully.

This feature must work with ACL assignment. The ACL must contain a rule that allows packets from the URL-specified server.

This feature is exclusive with the EAD assistant feature.

New feature: Support of MAC authentication for redirect URL assignment

The device supports the URL attribute assigned by a RADIUS server. During MAC authentication, a user is redirected to the Web interface specified by the server-assigned URL attribute. After the user passes the Web authentication, the RADIUS server records the MAC address of the Web user and uses a DM (Disconnect Message) to log off the Web user. When the user initiates MAC authentication again, it will pass the authentication and come online successfully.

This feature must work with ACL assignment. The ACL must contain a rule that allows packets from the URL-specified server.

New feature: Support of port security for redirect URL assignment in specific modes

The device supports the URL attribute assigned by a RADIUS server in the following port security modes:

- **mac-authentication**.
- **mac-else-userlogin-secure.**
- **mac-else-userlogin-secure-ext**.
- **userlogin-secure.**
- **userlogin-secure-ext**.
- **userlogin-secure-or-mac.**
- **userlogin-secure-or-mac-ext**.
- **userlogin-withoui**.

During authentication, a user is redirected to the Web interface specified by the server-assigned URL attribute. After the user passes the Web authentication, the RADIUS server records the MAC address of the Web user and uses a DM (Disconnect Message) to log off the Web user. When the user initiates 802.1X or MAC authentication again, it will pass the authentication and come online successfully.

New feature: Specifying ITU channel numbers for transceiver modules

This feature is supported on interfaces installed with HPE X130 10G SFP+ LC LH80 tunable Transceiver (JL250A) modules.

Specifying ITU channel numbers for transceiver modules

ITU defines a set of optical signal specifications by frequency and wavelength. These specifications are identified by channel numbers. In scenarios where Denseness Wavelength Division Multiplexing (DWDM) is used, you must specify ITU channel numbers for transceiver modules.

To specify an ITU channel number for a transceiver module:

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 ITU channel number for the transceiver module.	**itu-channel** *channel-number*	By default, the ITU channel number is 1 for a transceiver module.
4. Display ITU channel information for transceiver modules.	**display transceiver itu-channel interface** [*interface-type interface-number* [**supported-channel**]]	This command is available in any view.

Command reference

itu-channel

Use **itu-channel** to specify an ITU channel number for a transceiver module.

Use **undo itu-channel** to restore the default.

Syntax

itu-channel *channel-number*

undo itu-channel

Default

The ITU channel number is 1 for a transceiver module.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

channel-number: Specifies the ITU channel number for the transceiver module.

Usage guidelines

The device saves the ITU channel number to an internal register on the transceiver module. It does not save the number to a configuration file.

Examples

Set the ITU channel number to 2 for the transceiver module in Ten-GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] itu-channel 2
Changing the channel number causes the service to be down for a while. Continue? [Y/N]:Y
```

display transceiver itu-channel interface

Use **display transceiver itu-channel interface** to display ITU channel information for transceiver modules.

Syntax

display transceiver itu-channel interface [*interface-type interface-number* [**supported-channel**]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this option, the command displays the current ITU channel information for all transceiver modules.

supported-channel: Displays the supported ITU channel numbers and the ITU channel information. If you do not specify this option, the command displays the current ITU channel information.

Examples

Display current ITU channel information for all transceiver modules.

```
<Sysname> display transceiver itu-channel interface
Interface                          Channel        WaveLength(nm)  Frequency(THz)
XGE1/0/1                           1              1566.72           191.35
XGE1/0/2                           -              -                 -
XGE1/0/3                           3              1565.90           191.45
```

...

Display current ITU channel information for the transceiver module in Ten-GigabitEthernet 1/0/1.

```
<Sysname> display transceiver itu-channel interface ten-gigabitethernet 1/0/1
Interface                          Channel        WaveLength(nm)  Frequency(THz)
XGE1/0/1                           1              1566.72           191.35
```

Display the supported ITU channel numbers and the ITU channel information for the transceiver module in Ten-GigabitEthernet 1/0/1.

```
<Sysname> display transceiver itu-channel interface ten-gigabitethernet 1/0/1
supported-channel
ITU channel settings supported on Ten-GigabitEthernet1/0/1 :
Channel    WaveLength(nm)    Frequency(THz)
1          1566.72           191.35
2          1566.31           191.40
3          1565.90           191.45
```

```
4          1565.50          191.50
5          1565.09          191.55
6          1564.68          191.60
7          1564.27          191.65
8          1563.86          191.70
...
```

Table 3 Command output

Field	Description
Interface	Type and number of the Interface in which the transceiver module is installed.
Channel	ITU channel number.
WaveLength(nm)	Wavelength for the channel, in nm. The value is accurate to 0.01 nm.
Frequency(THz)	Frequency for the channel, in THz. The value is accurate to 0.01 THz.
-	This value is displayed if there is not ITU channel information to display for the Channel, WaveLength(nm), and Frequency(THz) fields. The reasons include: • No transceiver module is installed in the interface. • The transceiver module installed in the interface does not support ITU channel configuration. • The command failed to obtain the ITU channel information. • The device does not support the ITU channel number stored on the transceiver module.

New feature: Setting the MAC address for a Layer 3 Ethernet interface or Layer 3 aggregate interface

Setting the MAC address for a Layer 3 Ethernet interface or Layer 3 aggregate interface

This feature is available in this version and later versions.

To set the MAC address for a Layer 3 Ethernet interface or Layer 3 aggregate interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	• Enter Layer 3 Ethernet interface view: **interface** *interface-type interface-number* • Enter Layer 3 aggregate interface view: **interface route-aggregation** *interface-number*	N/A
3. Set the MAC address for the Layer 3 Ethernet	**mac-address** *mac-address*	By default, the MAC address of a Layer 3 Ethernet interface or Layer

Step	Command	Remarks
interface or Layer 3 aggregate interface.		3 aggregate interface is the bridge MAC address of the device.

Command reference

mac-address

Use **mac-address** to set the MAC address of a Layer 3 Ethernet interface or Layer 3 aggregate interface.

Use **undo mac-address** to restore the default.

Syntax

mac-address *mac-address*

undo mac-address

Default

The MAC address of a Layer 3 Ethernet interface or Layer 3 aggregate interface is the bridge MAC address of the device.

Views

Layer 3 Ethernet interface view

Layer 3 aggregate interface view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a MAC address in the format of H-H-H.

Examples

Set the MAC address of Ten-GigabitEthernet 1/0/1 to 0001-0001-0001.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] mac-address 1-1-1
```

New feature: Configuring the DHCP smart relay feature

Configuring the DHCP smart relay feature

The DHCP smart relay feature allows the DHCP relay agent to pad secondary IP addresses when the DHCP server does not reply the DHCP-OFFER message.

The relay agent initially pads its primary IP address to the **giaddr** field before forwarding a request to the DHCP server. If no DHCP-OFFER is received, the relay agent allows the client to send a maximum of two requests to the DHCP server by using the primary IP address. If no DHCP-OFFER is returned after two retries, the relay agent switches to a secondary IP address. If the DHCP server still does not respond, the next secondary IP address is used. After the secondary IP addresses are all tried and the DHCP server does not respond, the relay agent repeats the process by starting from the primary IP address.

Without this feature, the relay agent only pads the primary IP address to the **giaddr** field of all requests.

On a relay agent where DHCP address pools and gateway addresses are configured, the smart relay feature starts the process from the first gateway address.

To configure the DHCP smart relay feature for a common network:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Enable the DHCP relay agent.	**dhcp select relay**	By default, an interface operates in the DHCP server mode when DHCP is enabled.
4. Assign primary and secondary IP addresses to the DHCP relay agent.	**ip address** *ip-address* { *mask-length* | *mask* } [**sub**]	By default, the DHCP relay agent does not have any IP addresses.
5. Return to system view.	**quit**	N/A
6. Enable the DHCP smart relay feature.	**dhcp smart-relay enable**	By default, the DHCP smart relay feature is disabled.

Command reference

dhcp smart-relay enable

Use **dhcp smart-relay enable** to enable the DHCP smart relay feature.

Use **undo dhcp smart-relay enable** to disable the DHCP smart relay feature.

Syntax

dhcp smart-relay enable

undo dhcp smart-relay enable

Default

The DHCP smart relay feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the smart relay feature on interfaces that are configured as the relay agent on the device.

The smart relay feature allows the relay agent to use secondary IP addresses as the gateway address when the DHCP server does not reply the DHCP-OFFER message. The relay agent initially pads its primary IP address to the **giaddr** field before forwarding a request to the DHCP server. If no DHCP-OFFER is returned after two retries, the relay agent switches to secondary IP addresses.

Without this feature, the relay agent always uses the primary IP address as the gateway address.

Examples

Enable the DHCP smart relay feature.

```
<Sysname> system-view
[Sysname] dhcp smart-relay enable
```

New feature: Configuring a description for a network access user

Configuring a description for a network access user

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter network access user view.	**local-user** *user-name* **class network**	N/A
3. Configure a description for the network access user.	**description** *text*	By default, a network access user does not have a description.

Command reference

description

Use **description** to configure a description for a network access user.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

A network access user does not have a description.

Views

Network access user view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 255 characters.

Examples

Configure the description as **Manager of MSC company** for network access user **123**.

```
<Sysname> system-view
```

```
[Sysname] local-user 123 class network
[Sysname-luser-network-123] description Manager of MSC company
```

Related commands

display local-user

New feature: Configuring the validity period for a network access user

Configuring the validity period for a network access user

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter network access user view.	**local-user** *user-name* **class network**	N/A
3. Configure the validity period for the network access user.	**validity-datetime** { **from** *start-date start-time* **to** *expiration-date expiration-time* | **from** *start-date start-time* | **to** *expiration-date expiration-time* }	By default, a network access user does not expire. Expired network access user accounts cannot be used for authentication.

Command reference

validity-datetime

Use **validity-datetime** to configure the validity period for a network access user.

Use **undo validity-datetime** to restore the default.

Syntax

validity-datetime { **from** *start-date start-time* **to** *expiration-date expiration-time* | **from** *start-date start-time* | **to** *expiration-date expiration-time* }

undo validity-datetime

Default

A network access user does not expire.

Views

Network access user view

Predefined user roles

network-admin

Parameters

from: Specifies the start date and time of the validity period. If you do not specify this keyword, the command only limits the expiration date and time of the network access user.

start-date: Specifies the date from which the network access user takes effect. The date is in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for the MM argument is 1 to 12. The value range for the DD argument varies with the specified month. The value range for the YYYY argument is 2000 to 2035.

start-time: Specifies the time from which the network access user takes effect. The time is in the format of hh:mm:ss. The value range for the hh argument is 0 to 23. The value range for the mm and ss arguments is 0 to 59. The mm and ss arguments are optional. For example, enter 1 to indicate 1:00:00. A value of 0 indicates 00:00:00.

to: Specifies the expiration date and time of the validity period. If you do not specify this keyword, the command only limits the start date and time of the network access user.

expiration-date: Specifies the expiration date in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for the MM argument is 1 to 12. The value range for the DD argument varies with the specified month. The value range for the YYYY argument is 2000 to 2035.

expiration-time: Specifies the expiration time in the format of hh:mm:ss. The value range for the hh argument is 0 to 23. The value range for the mm and ss arguments is 0 to 59. The mm and ss arguments are optional. For example, enter 1 to indicate 1:00:00. A value of 0 indicates 00:00:00.

Usage guidelines

Expired network access user accounts cannot be used for authentication.

If you specify both the start time and expiration time, the expiration time must be later than the start time.

If you specify only the start time, the network access user takes effect after the specified time.

If you specify only the expiration time, the network access user takes effect before the time expires.

Examples

Configure network access user **123** to take effect from 2014/10/01 00:00:00 to 2015/10/02 12:00:00.

```
<Sysname> system-view
[Sysname] local-user 123 class network
[Sysname-luser-network-123] validity-datetime from 2014/10/01 00:00:00 to 2015/10/02
12:00:00
```

Related commands

display local-user

New feature: Enabling the auto-delete feature for expired local user accounts

Enabling the auto-delete feature for expired local user accounts

The device regularly checks the validity status of each local user and automatically deletes expired local user accounts.

To enable the auto-delete feature:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Enable the auto-delete feature for expired local user accounts.	**local-user auto-delete enable**	By default, the auto-delete feature is disabled.

Command reference

local-user auto-delete enable

Use **local-user auto-delete enable** to enable the auto-delete feature for expired local user accounts.

Use **undo local-user auto-delete enable** to restore the default.

Syntax

local-user auto-delete enable

undo local-user auto-delete enable

Default

The auto-delete feature is disabled for expired local user accounts.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to automatically delete the local user accounts when they expire.

Examples

Enable the auto-delete feature for expired local user accounts.

```
<Sysname> system-view
[Sysname] local-user auto-delete enable
```

New feature: Configuring periodic MAC reauthentication

Configuring periodic MAC reauthentication

The device reauthenticates online MAC authentication users on a port at the periodic reauthentication interval if the port is enabled with periodic MAC reauthentication. Periodic MAC reauthentication 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 reauthentication interval either in system view or in interface view by using the **mac-authentication timer reauth-period** command. A change to the periodic reauthentication timer applies to online users only after the old timer expires.

The device selects a periodic reauthentication timer for MAC reauthentication in the following order:

1. Server-assigned reauthentication timer.

2. Port-specific reauthentication timer.
3. Global reauthentication timer.
4. Default reauthentication timer.

To configure periodic MAC reauthentication:

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

Command reference

mac-authentication timer reauth-period (system view)

Use **mac-authentication timer reauth-period** to set the global periodic MAC reauthentication 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 reauthentication timer is 3600 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

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

Usage guidelines

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

A change to the global periodic reauthentication timer applies to online users only after the old timer expires.

The device selects a periodic reauthentication timer for MAC reauthentication in the following order:

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

Examples

Set the global periodic MAC reauthentication timer to 150 seconds.

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

mac-authentication re-authenticate

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

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

Syntax

mac-authentication re-authenticate

undo mac-authentication re-authenticate

Default

The periodic MAC reauthentication feature is disabled on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

Periodic MAC reauthentication 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 reauthentication interval, use the **mac-authentication timer reauth-period** command.

Examples

Enable the periodic MAC reauthentication feature on Ten-GigabitEthernet 1/0/1 and set the global periodic reauthentication interval to 1800 seconds.

```
<Sysname> system-view
[Sysname] mac-authentication timer reauth-period 1800
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] mac-authentication re-authenticate
```

mac-authentication timer reauth-period (interface view)

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

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

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

Usage guidelines

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

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

The device selects a periodic reauthentication timer for MAC reauthentication in the following order:

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

Examples

Set the periodic MAC reauthentication timer to 90 seconds on Ten-GigabitEthernet 1/0/1.

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

New feature: Enabling preprovisioning

Enabling preprovisioning

If a module is removed before you save the configuration and reboot all devices in an IRF fabric, the configuration on the module cannot be restored when it comes online. Modules include IRF member devices and subcards. To solve the problem, you can perform the <config-provisioned> operation to enable preprovisioning before the module goes offline. With preprovisioning, you can continue to view and edit the existing configuration on the module after the module goes offline. After you save the configuration and reboot all devices in the IRF fabric, the final configuration applies when the module comes online again.

Follow these restrictions and guidelines when you perform the <config-provisioned> operation:

- Preprovisioning is available for commands in the view of an interface on an IRF member device or a subcard, and for commands in the view of a slot. It is also available for the packet statistics feature (configured by the **qos traffic-counter** command).

- Only IRF member devices and subcards in **Normal** state support preprovisioning.
- After an IRF member device or a subcard is removed, you can only use the CLI to view and edit the existing configuration on the member device or subcard.

Configuration procedure

Copy the following text to the client to enable preprovisioning:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <config-provisioned>
  </config-provisioned>
</rpc>
```

Verifying the configuration

If the client receives the following text, the operation is successful:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <ok/>
</rpc-reply>
```

New feature: Enabling SNMP notifications for RRPP

Enabling SNMP notifications for RRPP

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable SNMP notifications for RRPP.	**snmp-agent trap enable rrpp** [**major-fault** | **multi-master** | **ring-fail** | **ring-recover**] *	By default, SNMP notifications are disabled for RRPP.

Command reference

snmp-agent trap enable rrpp

Use **snmp-agent trap enable rrpp** to enable SNMP notifications for RRPP.

Use **undo snmp-agent trap enable rrpp** to disable SNMP notifications for RRPP.

Syntax

snmp-agent trap enable rrpp [**major-fault** | **multi-master** | **ring-fail** | **ring-recover**] *

undo snmp-agent trap enable rrpp [**major-fault** | **multi-master** | **ring-fail** | **ring-recover**] *

Default

SNMP notifications are disabled for RRPP.

Views

System view

Predefined user roles

network-admin

Parameters

major-fault: Sends an SNMP notification when an SRPT between assistant edge node and edge node is disconnected.

multi-master: Sends an SNMP notification when multiple master nodes are configured on the RRPP ring.

ring-fail: Sends an SNMP notification when the RRPP ring state changes from Health to Disconnect.

ring-recover: Sends an SNMP notification when the RRPP ring state changes from Disconnect to Health.

Usage guidelines

To report critical RRPP events to an NMS, enable SNMP notifications for RRPP. For SNMP notifications to be sent correctly, you must also configure the notification sending parameters as required. For more information about SNMP notifications, see *Network Management and Monitoring Configuration Guide*.

If no optional parameters are specified, this command or its **undo** form enables or disables all SNMP notifications supported by the device.

Examples

Enable the device to send SNMP notifications when the RRPP ring state changes from Disconnect to Health.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable rrpp ring-recover
```

Modified feature: Displaying PBR configuration

Feature change description

The command output was changed.

Command changes

Modified command: display ip policy-based-route setup

Syntax

display ip policy-based-route setup

Views

Any view

Change description

Before modification: The command output does not include the **Type** field.

```
<Sysname> display ip policy-based-route setup
Policy Name              Interface Name
pr01                     Vlan-interface2
```

After modification: The command output includes the **Type** field, which indicates the type of the PBR.

```
<Sysname> display ip policy-based-route setup
Policy name              Type              Interface
pr01                     Forward           Ten-gigabitethernet1/0/1
pro2                     Egress            Tunnel0
pro3                     Local             N/A
```

Modified feature: Displaying MAC address table information for VSIs

Feature change description

In this release, the command output of the **display l2vpn mac-address** command displays the outgoing interface name of the MAC address entry.

Command changes

Modified command: display l2vpn mac-address

Syntax

display l2vpn mac-address [**vsi** *vsi-name*] [**dynamic**] [**count**]

Views

Any view

Change description

Before modification: The **Link ID/Name** field in the command output displays the outgoing link ID of the MAC address entry.

```
<Sysname> display l2vpn mac-address
MAC Address      State    VSI Name                          Link ID/Name  Aging
0000-0000-000a   dynamic  vpn1                              1             Aging
0000-0000-0009   dynamic  vpn1                              2             Aging
--- 2 mac address(es) found  ---
```

After modification: The **Link ID/Name** field in the command output displays the outgoing interface name of the MAC address entry.

```
<Sysname> display l2vpn mac-address
MAC Address    State    VSI Name                        Link ID/Name    Aging
0016-1600-0017 Openflow SDN_VSI_2028                    Tunnel257       NotAging
0050-56a1-1c4b Dynamic  SDN_VSI_2028                    FGE1/0/1        Aging
--- 2 mac address(es) found  ---
```

Modified feature: Enabling the BFD echo packet mode

Feature change description

The **receive** and **send** keywords were added to the **bfd echo enable** command to enable the echo packet receiving and sending capabilities.

Command changes

Modified command: bfd echo enable

Old syntax

bfd echo enable

undo bfd echo enable

New syntax

bfd echo [**receive** | **send**] **enable**

undo bfd echo [**receive** | **send**] **enable**

Views

Interface view

Change description

Before modification: The **receive** and **send** keywords are not supported. The **bfd echo enable** command enables only the echo packet sending capability.

After modification: The **receive** and **send** keywords are supported. The **bfd echo receive enable** command enables only the echo packet receiving capability. The **bfd echo send enable** command enables only the echo packet sending capability. The **bfd echo enable** command enables both the echo packet receiving and sending capabilities.

Modified feature: NTP authentication

Feature change description

Before modification: Only the MD5 algorithm is supported.

After modification: The HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 algorithms are supported.

Command changes

Modified command: ntp-service authentication-keyid

Old syntax

ntp-service authentication-keyid *keyid* **authentication-mode md5** { **cipher** | **simple** } *string*

New syntax

ntp-service authentication-keyid *keyid* **authentication-mode** { **hmac-sha-1** | **hmac-sha-256** | **hmac-sha-384** | **hmac-sha-512** | **md5** } { **cipher** | **simple** } *string*

Views

System view

Change description

The **hmac-sha-1**, **hmac-sha-256**, **hmac-sha-384**, and **hmac-sha-512** keywords were added.

- **hmac-sha-1**: Specifies the HMAC-SHA-1 algorithm.
- **hmac-sha-256**: Specifies the HMAC-SHA-256 algorithm.
- **hmac-sha-384**: Specifies the HMAC-SHA-384 algorithm.
- **hmac-sha-512**: Specifies the HMAC-SHA-512 algorithm.

Modified command: sntp authentication-keyid

Old syntax

sntp authentication-keyid *keyid* **authentication-mode md5** { **cipher** | **simple** } *string*

New syntax

sntp authentication-keyid *keyid* **authentication-mode** { **hmac-sha-1** | **hmac-sha-256** | **hmac-sha-384** | **hmac-sha-512** | **md5** } { **cipher** | **simple** } *string*

Views

System view

Change description

The **hmac-sha-1**, **hmac-sha-256**, **hmac-sha-384**, and **hmac-sha-512** keywords were added.

- **hmac-sha-1**: Specifies the HMAC-SHA-1 algorithm.
- **hmac-sha-256**: Specifies the HMAC-SHA-256 algorithm.
- **hmac-sha-384**: Specifies the HMAC-SHA-384 algorithm.
- **hmac-sha-512**: Specifies the HMAC-SHA-512 algorithm.

Modified feature: Displaying MAC address move records

Feature change description

In this release, the device can display a maximum of 200 MAC address move records.

Command changes

None.

Modified feature: MAC address move notifications

Feature change description

Before modification: Within a detection interval, the device can generate a maximum of 20 MAC address move logs. The most recent log will override the oldest one.

After modification: Within a detection interval, the device can record MAC address move logs for a maximum of 20 MAC addresses. The logs are ranked in descending order of MAC move count. When the MAC move count of a new log is higher than the MAC move count of any existing log, the device performs the following operations:

- Discards the log that has the lowest MAC move count.
- Ranks the MAC address move logs in descending order of MAC move count.

Then in the next detection interval, the device discards all MAC address move logs generated in the previous detection interval and starts another round of MAC address move log generation.

Command changes

None.

Modified feature: Displaying detailed information about UDP connections and RawIP connections

Feature change description

Before modification: The command output for UDP connections and RawIP connections does not include number of packets dropped in the receiving buffer.

After modification: The command output for UDP connections and RawIP connections includes number of packets dropped in the receiving buffer.

Command changes

Modified commands: display rawip verbose and display udp verbose

Syntax

display rawip verbose

display udp verbose

Views

Any view

Change description

Before modification: The command output about the receiving buffer is "`Receiving buffer(cc/hiwat/lowat/state): 0 / 1048576 / 1 / 0 / N/A`." The information does not include the number of packets dropped in the receiving buffer.

After modification: The command output about the receiving buffer is "`Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 1048576 / 1 / 0 / N/A`." The information includes the number of packets dropped in the receiving buffer.

Modified feature: Displaying detailed information about IPv6 UDP connections and IPv6 RawIP connections

Feature change description

Before modification: The command output for IPv6 UDP connections and IPv6 RawIP connections does not include number of packets dropped in the receiving buffer.

After modification: The command output for IPv6 UDP connections and IPv6 RawIP connections includes number of packets dropped in the receiving buffer.

Command changes

Modified commands: display ipv6 rawip verbose and display ipv6 udp verbose

Syntax

display ipv6 rawip verbose

display ipv6 udp verbose

Views

Any view

Change description

Before modification: The command output about the receiving buffer is "`Receiving buffer(cc/hiwat/lowat/state): 0 / 1048576 / 1 / 0 / N/A`." The information does not include the number of packets dropped in the receiving buffer.

After modification: The command output about the receiving buffer is "`Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 1048576 / 1 / 0 / N/A`." The information includes the number of packets dropped in the receiving buffer.

Modified feature: Default size of the TCP receive and send buffer

Feature change description

Before modification: The default size of the TCP receive and send buffer is 64 KB.

After modification: The default size of the TCP receive and send buffer is 63 KB.

Command changes

Modified command: tcp window

Syntax

tcp window *window-size*

undo tcp window

Views

System view

Change description

Before modification: The default value for the *window-size* argument was 64 KB.

After modification: The default value for the *window-size* argument is 63 KB.

Modified feature: Displaying MPLS LSP statistics

Feature change description

Before modification: The **display mpls lsp statistics** command displays IPv4 LSP statistics and IPv6 LSP statistics at the same time.

After modification: The **display mpls lsp statistics** command displays IPv4 LSP statistics and IPv6 LSP statistics separately.

Command changes

Modified command: display mpls lsp statistics

Old syntax

display mpls lsp statistics

New syntax

display mpls lsp statistics [**ipv6**]

Views

Any view

Change description

The **ipv6** keyword was added to display IPv6 LSP statistics. If you do not specify this keyword, the command displays IPv4 LSP statistics.

Modified feature: Configuring BGP route summarization

Feature change description

BGP route summarization configuration was supported in BGP-VPN IPv6 unicast address family view.

Command changes

Modified command: aggregate

Syntax

aggregate *ipv6-address prefix-length* [**as-set** | **attribute-policy** *route-policy-name* | **detail-suppressed** | **origin-policy** *route-policy-name* | **suppress-policy** *route-policy-name*] *

undo aggregate *ipv6-address prefix-length*

Views

BGP IPv6 unicast address family view, BGP-VPN IPv6 unicast address family view

Change description

Before modification: The **aggregate** command was not available in BGP-VPN IPv6 unicast address family view.

After modification: The **aggregate** command is available in BGP-VPN IPv6 unicast address family view.

Modified feature: Displaying OSI connection information

Feature change description

The information about dropped packets in the receiving buffer was added to the OSI connection information.

Command changes

Modified command: display osi

Syntax

display osi

Views

Any view

Change description

Before modification: The command output `Receiving buffer(cc/hiwat/lowat/state): 0 / 1048576 / 1 / 0 / N/A` does not contain the information about dropped packets.

After modification: The command output `Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 1048576 / 1 / 0 / N/A` contains the information about dropped packets.

F2426

This release has the following changes:

- New feature: Transceiver module alarm suppression
- New feature: IP unnumbered on an interface
- New feature: Setting the packet sending mode for IPv4 VRRPv3
- New feature: Enabling periodic sending of gratuitous ARP packets for IPv4 VRRP
- New feature: Enabling periodic sending of ND packets for IPv6 VRRP
- New feature: Configuring a subordinate IPv4 VRRP group to follow a master IPv4 VRRP group
- New feature: Configuring a subordinate IPv6 VRRP group to follow a master IPv6 VRRP group
- New feature: Displaying master-to-subordinate IPv4 VRRP group bindings
- New feature: Displaying master-to-subordinate IPv6 VRRP group bindings
- New feature: Configuring the threshold for triggering monitor link group state switchover
- New feature: ACL application to NETCONF over SOAP traffic
- New feature: Allowing link aggregation member ports to be in the deployed flow tables
- New feature: Enabling OpenFlow connection backup
- New feature: Port-specific 802.1X periodic reauthentication timer
- New feature: Manual reauthentication for all online 802.1X users on a port
- New feature: Enabling SNMP notifications for port security
- New feature: DSCP value for OpenFlow packets
- Modified feature: SSH support for Suite B
- Modified feature: Configuring the CDP-compatible operating mode for LLDP
- Modified feature: Configuring a traffic policing action

New feature: Transceiver module alarm suppression

Disabling alarm traps for transceiver modules

If you install a transceiver module whose vendor name is not **HPE**, the system repeatedly outputs traps and logs to notify you to replace the module. If the transceiver module is manufactured or customized by HPE, you can disable alarm traps so the system stops outputting alarm traps.

Command reference

Use **transceiver phony-alarm-disable** to disable alarm traps for transceiver modules.

Use **undo transceiver phony-alarm-disable** to restore the default.

transceiver phony-alarm-disable

Syntax

transceiver phony-alarm-disable

undo transceiver phony-alarm-disable

Default

Alarm traps are enabled for transceiver modules.

Views

System view

Predefined user roles

network-admin

Usage guidelines

If you install a transceiver module whose vendor name is not **HPE**, the system repeatedly outputs traps and logs to notify you to replace the module. If the transceiver module is manufactured or customized by HPE, you can disable alarm traps so the system stops outputting alarm traps.

Examples

Disable alarm traps for transceiver modules.

```
<Sysname> system-view
[Sysname] transceiver phony-alarm-disable
```

New feature: IP unnumbered on an interface

Configuring IP unnumbered on an interface

Overview

Typically, you assign an IP address to an interface either manually or through DHCP. If the IP addresses are not enough, or the interface is used only occasionally, you can configure an interface to borrow an IP address from other interfaces. This is called IP unnumbered, and the interface borrowing the IP address is called IP unnumbered interface.

You can use IP unnumbered to save IP addresses either when available IP addresses are inadequate or when an interface is brought up only for occasional use.

Configuration guidelines

Follow these guidelines when you configure IP unnumbered:

- Loopback interfaces cannot borrow IP addresses of other interfaces, but other interfaces can borrow IP addresses of loopback interfaces.
- An interface cannot borrow an IP address from an unnumbered interface.
- Multiple interfaces can use the same unnumbered IP address.
- If an interface has multiple manually configured IP addresses, only the manually configured primary IP address can be borrowed.

- A dynamic routing protocol cannot be enabled on the interface where IP unnumbered is configured. To enable the interface to communicate with other devices, configure a static route to the peer device on the interface.

Configuration prerequisites

Assign an IP address to the interface from which you want to borrow the IP address. Alternatively, you can configure the interface to obtain one through BOOTP, DHCP, or PPP address negotiation.

Configuration procedure

To configure IP unnumbered on an interface:

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 interface to borrow the IP address of the specified interface.	**ip address unnumbered interface** *interface-type interface-number*	By default, the interface does not borrow IP addresses from other interfaces.

Command reference

ip address unnumbered

Use **ip address unnumbered** to configure the current interface as IP unnumbered to borrow an IP address from the specified interface.

Use **undo ip address unnumbered** to restore the default.

Syntax

ip address unnumbered interface *interface-type interface-number*

undo ip address unnumbered

Default

The interface does not borrow IP addresses from other interfaces.

Views

Interface view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface from which the current interface can borrow an IP address.

Usage guidelines

Typically, you assign an IP address to an interface either manually or through DHCP. If the IP addresses are not enough, or the interface is used only occasionally, you can configure an interface to borrow an IP address from other interfaces. This is called IP unnumbered, and the interface borrowing the IP address is called IP unnumbered interface.

Loopback interfaces cannot borrow IP addresses of other interfaces, but other interfaces can borrow IP addresses of loopback interfaces.

Multiple interfaces can use the same unnumbered IP address. If an interface has multiple manually configured IP addresses, only the primary IP address manually configured can be borrowed.

You cannot enable a dynamic routing protocol on the interface that has no IP address configured. To enable the interface to communicate with other devices, you must configure a static route to the peer device on the interface.

Examples

Configure the interface Tunnel 0 to borrow the IP address of VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface tunnel 0 mode gre
[Sysname-Tunnel0] ip address unnumbered interface vlan-interface 100
```

New feature: Setting the packet sending mode for IPv4 VRRPv3

Setting the packet sending mode for IPv4 VRRPv3

A router configured with VRRPv3 can process incoming VRRPv2 packets, but a router configured with VRRPv2 cannot process incoming VRRPv3 packets. When the VRRP version of the routers in a VRRP group is changed from VRRPv2 to VRRPv3, multiple masters might be elected in the VRRP group. To resolve the problem, you can set the packet sending mode for IPv4 VRRPv3. This task enables a router configured with VRRPv3 to send VRRPv2 packets and communicate with routers configured with VRRPv2.

When you set the packet sending mode for IPv4 VRRPv3, follow these restrictions and guidelines:

- The packet sending mode for IPv4 VRRPv3 takes effect only on outgoing VRRP packets. A router configured with VRRPv3 can process incoming VRRPv2 and VRRPv3 packets.
- If you set the packet sending mode for IPv4 VRRPv3 and configure VRRP packet authentication, authentication information will be carried in outgoing VRRPv2 packets but not in VRRPv3 packets.
- The VRRP advertisement interval is set in centiseconds by using the **vrrp vrid timer advertise** command. The VRRP advertisement interval carried in VRRPv2 packets sent from routers configured with VRRPv3 might be different from the configured value. For information about the VRRP advertisement interval, see the **vrrp vrid timer advertise** command in *High Availability Command Reference*.

To set the packet sending mode for IPv4 VRRPv3:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Set the packet sending mode for IPv4 VRRPv3.	**vrrp vrid** *virtual-router-id* **vrrpv3-send-packet** { **v2-only** | **v2v3-both** }	By default, a router configured with VRRPv3 sends only VRRPv3 packets.

Command reference

vrrp vrid vrrpv3-send-packet

Use **vrrp vrid vrrpv3-send-packet** to set the packet sending mode for IPv4 VRRPv3.

Use **undo vrrp vrid vrrpv3-send-packet** to restore the default.

Syntax

vrrp vrid *virtual-router-id* **vrrpv3-send-packet** { **v2-only** | **v2v3-both** }

undo vrrp vrid *virtual-router-id* **vrrpv3-send-packet**

Default

A router configured with VRRPv3 sends only VRRPv3 packets.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

v2-only: Sends VRRPv2 packets only.

v2v3-both: Sends both VRRPv2 and VRRPv3 packets.

Usage guidelines

This command takes effect only on IPv4 VRRPv3.

The packet sending mode for IPv4 VRRPv3 takes effect only on outgoing VRRP packets. A router configured with VRRPv3 can process incoming VRRPv2 and VRRPv3 packets.

If you set the packet sending mode for IPv4 VRRPv3 and configure VRRP packet authentication, authentication information will be carried in outgoing VRRPv2 packets but not in VRRPv3 packets.

The VRRP advertisement interval is set in centiseconds by using the **vrrp vrid timer advertise** command. The VRRP advertisement interval carried in VRRPv2 packets sent from routers configured with VRRPv3 might be different from the configured value. For information about the VRRP advertisement interval, see the **vrrp vrid timer advertise** command in *High Availability Command Reference*.

Examples

Configure VRRP group 1 to send both VRRPv2 and VRRPv3 packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 vrrpv3-send-packet v2v3-both
```

Related commands

display vrrp

vrrp vrid timer advertise

New feature: Enabling periodic sending of gratuitous ARP packets for IPv4 VRRP

Enabling periodic sending of gratuitous ARP packets for IPv4 VRRP

This feature enables the master router in a VRRP group to periodically send gratuitous ARP packets. Then the downstream devices can update the MAC address entry for the virtual MAC address of the VRRP group in a timely manner.

When you enable periodic sending of gratuitous ARP packets for IPv4 VRRP, follow these restrictions and guidelines:

- This feature takes effect only in VRRP standard mode.
- If you change the sending interval for gratuitous ARP packets, the configuration takes effect at the next sending interval.
- The master sends the first gratuitous ARP packet at a random time in the second half of the set interval after you execute the **vrrp send-gratuitous-arp** command. This prevents too many gratuitous ARP packets from being sent at the same time.
- The sending interval for gratuitous ARP packets might be much longer than the set interval when the following conditions are met:
  - Multiple VRRP groups exist on the device.
  - A short sending interval is set.

To enable periodic sending of gratuitous ARP packets for IPv4 VRRP:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable periodic sending of gratuitous ARP packets for IPv4 VRRP.	**vrrp send-gratuitous-arp** [**interval** *interval*]	By default, periodic sending of gratuitous ARP packets is disabled for IPv4 VRRP.

Command reference

vrrp send-gratuitous-arp

Use **vrrp send-gratuitous-arp** to enable periodic sending of gratuitous ARP packets for IPv4 VRRP.

Use **undo vrrp send-gratuitous-arp** to restore the default.

Syntax

vrrp send-gratuitous-arp [**interval** *interval*]

undo vrrp send-gratuitous-arp

Default

Periodic sending of gratuitous ARP packets is disabled for IPv4 VRRP.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the sending interval in the range of 30 to 1200 seconds. The default value is 120 seconds.

Usage guidelines

This command ensures that the MAC address entry for the virtual MAC address of a VRRP group can be updated on downstream devices in a timely manner.

This command takes effect only in VRRP standard mode.

The master sends the first gratuitous ARP packet at a random time in the second half of the set interval after you execute the **vrrp send-gratuitous-arp** command. This prevents too many gratuitous ARP packets from being sent at the same time.

The sending interval for gratuitous ARP packets might be much longer than the set interval when the following conditions are met:

- Multiple VRRP groups exist on the device.
- A short sending interval is set.

If you change the sending interval for gratuitous ARP packets, the configuration takes effect at the next sending interval.

Examples

Enable periodic sending of gratuitous ARP packets for IPv4 VRRP and set the sending interval to 200 seconds.

```
<Sysname> system-view
[Sysname] vrrp send-gratuitous-arp interval 200
```

New feature: Enabling periodic sending of ND packets for IPv6 VRRP

Enabling periodic sending of ND packets for IPv6 VRRP

This feature enables the master router in an IPv6 VRRP group to periodically send ND packets. Then the downstream devices can update the MAC address entry for the virtual MAC address of the IPv6 VRRP group in a timely manner.

When you enable periodic sending of ND packets for IPv6 VRRP, follow these restrictions and guidelines:

- This feature takes effect only in VRRP standard mode.
- If you change the sending interval for ND packets, the configuration takes effect at the next sending interval.
- The master sends the first ND packet at a random time in the second half of the set interval after you execute the **vrrp ipv6 send-nd** command. This prevents too many ND packets from being sent at the same time.
- The sending interval for ND packets might be much longer than the set interval when the following conditions are met:
  - Multiple IPv6 VRRP groups exist on the device.

- A short sending interval is set.

To enable periodic sending of ND packets for IPv6 VRRP:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable periodic sending of ND packets for IPv6 VRRP.	**vrrp ipv6 send-nd** [**interval** *interval*]	By default, periodic sending of ND packets is disabled for IPv6 VRRP.

Command reference

vrrp ipv6 send-nd

Use **vrrp ipv6 send-nd** to enable periodic sending of ND packets for IPv6 VRRP.

Use **undo vrrp ipv6 send-nd** to restore the default.

Syntax

vrrp ipv6 send-nd [**interval** *interval*]

undo vrrp ipv6 send-nd

Default

Periodic sending of ND packets is disabled for IPv6 VRRP.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the sending interval in the range of 30 to 1200 seconds. The default value is 120 seconds.

Usage guidelines

This command ensures that the MAC address entry for the virtual MAC address of an IPv6 VRRP group can be updated on downstream devices in a timely manner.

This command takes effect only in VRRP standard mode.

The master sends the first ND packet at a random time in the second half of the set interval after you execute the **vrrp ipv6 send-nd** command. This prevents too many ND packets from being sent at the same time.

The sending interval for ND packets might be much longer than the set interval when the following conditions are met:

- Multiple IPv6 VRRP groups exist on the device.
- A short sending interval is set.

If you change the sending interval for ND packets, the configuration takes effect at the next sending interval.

Examples

Enable periodic sending of ND packets for IPv6 VRRP and set the sending interval to 200 seconds.

```
<Sysname> system-view
```

```
[Sysname] vrrp ipv6 send-nd interval 200
```

New feature: Configuring a subordinate IPv4 VRRP group to follow a master IPv4 VRRP group

Configuring a subordinate IPv4 VRRP group to follow a master IPv4 VRRP group

Each VRRP group determines the device role (master or backup) by exchanging VRRP packets among member devices, which might consume excessive bandwidth and CPU resources. To reduce the number of VRRP packets in the network, you can configure a subordinate VRRP group to follow a master VRRP group.

A master VRRP group determines the device role through exchanging VRRP packets among member devices. A VRRP group that follows a master group, called a subordinate VRRP group, does not exchange VRRP packets among its member devices. The state of the subordinate VRRP group follows the state of the master group.

Configuration restrictions and guidelines

When you configure a subordinate IPv4 VRRP group to follow a master IPv4 VRRP group, follow these restrictions and guidelines:

- You can configure a subordinate VRRP group to follow a master VRRP group in both VRRP standard and load balancing modes. The configuration takes effect only in VRRP standard mode.
- An IPv4 VRRP group cannot be both a master group and a subordinate group.
- An IPv4 VRRP group stays in **Inactive** state if it is configured to follow a nonexistent master group.
- If an IPv4 VRRP group in **Inactive** or **Initialize** state follows a master group that is not in **Inactive** state, the state of the VRRP group does not change.
- A subordinate IPv4 VRRP group does not exchange VRRP packets, which might cause the MAC address entry for its virtual MAC address not to be updated on downstream devices. As a best practice, enable periodic sending of gratuitous ARP packets for IPv4 VRRP by using the **vrrp send-gratuitous-arp** command.

To configure a subordinate IPv4 VRRP group to follow a master IPv4 VRRP group:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Assign a master group name to an IPv4 VRRP group.	**vrrp vrid** *virtual-router-id* **name** *name*	By default, an IPv4 VRRP group is not assigned a master group name.
4. Configure an IPv4 VRRP group to follow a master group.	**vrrp vrid** *virtual-router-id* **follow** *name*	By default, an IPv4 VRRP group does not follow a master VRRP group.

Command reference

vrrp vrid name

Use **vrrp vrid name** to configure an IPv4 VRRP group as a master group and assign a name to it.

Use **undo vrrp vrid name** to remove the configuration.

Syntax

vrrp vrid *virtual-router-id* **name** *name*

undo vrrp vrid *virtual-router-id* **name**

Default

An IPv4 VRRP group does not act as a master group.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

name: Specifies a master IPv4 VRRP group name, a case-sensitive string of 1 to 20 characters.

Usage guidelines

This command configures an IPv4 VRRP group as a master group by assigning a master group name to it. A VRRP group that follows the master group is a subordinate VRRP group. The master VRRP group exchanges VRRP packets among member devices. The subordinate VRRP group does not exchange VRRP packets and follows the state of the master group. Both the master and subordinate VRRP groups can forward service traffic.

You cannot assign the same master VRRP group name to different VRRP groups on a device.

An IPv4 VRRP group cannot be both a master group and a subordinate group. The **vrrp vrid name** and **vrrp vrid follow** commands are mutually exclusive.

Examples

Configure IPv4 VRRP group 1 as a master group and assign master group name **abc** to it.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 name abc
```

Related commands

display vrrp binding

vrrp vrid follow

vrrp vrid follow

Use **vrrp vrid follow** to configure an IPv4 VRRP group to follow a master group.

Use **undo vrrp vrid follow** to remove the configuration.

Syntax

vrrp vrid *virtual-router-id* **follow** *name*

undo vrrp vrid *virtual-router-id* **follow**

Default

An IPv4 VRRP group does not follow a master group.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

name: Specifies a master IPv4 VRRP group by its name, a case-sensitive string of 1 to 20 characters.

Usage guidelines

This command configures an IPv4 VRRP group as a subordinate VRRP group to follow a master group. A subordinate VRRP group can forward service traffic.

An IPv4 VRRP group cannot be both a master group and a subordinate group. The **vrrp vrid name** and **vrrp vrid follow** commands are mutually exclusive.

An IPv4 VRRP group stays in **Inactive** state if it is configured to follow a nonexistent master VRRP group.

If an IPv4 VRRP group in **Inactive** or **Initialize** state follows a master group that is not in **Inactive** state, the state of the VRRP group does not change.

Examples

Configure IPv4 VRRP group 1 to follow master group **abc**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 follow abc
```

Related commands

display vrrp binding

vrrp vrid name

New feature: Configuring a subordinate IPv6 VRRP group to follow a master IPv6 VRRP group

Configuring a subordinate IPv6 VRRP group to follow a master IPv6 VRRP group

Each IPv6 VRRP group determines the device role (master or backup) by exchanging VRRP packets among member devices, which might consume excessive bandwidth and CPU resources. To reduce the number of VRRP packets in the network, you can configure a subordinate IPv6 VRRP group to follow a master IPv6 VRRP group.

A master IPv6 VRRP group determines the device role through exchanging VRRP packets among member devices. An IPv6 VRRP group that follows a master group, called a subordinate VRRP group, does not exchange VRRP packets among its member devices. The state of the subordinate VRRP group follows the state of the master group.

Configuration restrictions and guidelines

When you configure a subordinate IPv6 VRRP group to follow a master IPv6 VRRP group, follow these restrictions and guidelines:

- You can configure a subordinate IPv6 VRRP group to follow a master IPv6 VRRP group in both VRRP standard and load balancing modes. The configuration takes effect only in VRRP standard mode.
- An IPv6 VRRP group cannot be both a master group and a subordinate group.
- An IPv6 VRRP group stays in **Inactive** state if it is configured to follow a nonexistent master IPv6 VRRP group.
- If an IPv6 VRRP group in **Inactive** or **Initialize** state follows a master group that is not in **Inactive** state, the state of the VRRP group does not change.
- A subordinate IPv6 VRRP group does not exchange VRRP packets, which might cause the MAC address entry for its virtual MAC address not to be updated on downstream devices. As a best practice, enable periodic sending of ND packets for IPv6 VRRP by using the **vrrp ipv6 send-nd** command.

To configure a subordinate IPv6 VRRP group to follow a master IPv6 VRRP group:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Assign a master group name to an IPv6 VRRP group.	**vrrp ipv6 vrid** *virtual-router-id* **name** *name*	By default, an IPv6 VRRP group is not assigned a master group name.
4. Configure an IPv6 VRRP group to follow a master group.	**vrrp ipv6 vrid** *virtual-router-id* **follow** *name*	By default, an IPv6 VRRP group does not follow a master VRRP group.

Command reference

vrrp ipv6 vrid name

Use **vrrp ipv6 vrid name** to configure an IPv6 VRRP group as a master group and assign a name to it.

Use **undo vrrp ipv6 vrid name** to remove the configuration.

Syntax

vrrp ipv6 vrid *virtual-router-id* **name** *name*

undo vrrp ipv6 vrid *virtual-router-id* **name**

Default

An IPv6 VRRP group does not act as a master group.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

name: Specifies a master IPv6 VRRP group name, a case-sensitive string of 1 to 20 characters.

Usage guidelines

This command configures an IPv6 VRRP group as a master group through assigning a master group name to it. An IPv6 VRRP group that follows the master group is a subordinate VRRP group. The master VRRP group exchanges VRRP packets among member devices. The subordinate group does not exchange VRRP packets and follows the state of the master group. Both the master and subordinate VRRP groups can forward service traffic.

You cannot assign the same master VRRP group name to different IPv6 VRRP groups on a device.

An IPv6 VRRP group cannot be both a master group and a subordinate group. The **vrrp ipv6 vrid name** and **vrrp ipv6 vrid follow** commands are mutually exclusive.

Examples

Configure IPv6 VRRP group 1 as a master VRRP group and assign master group name **abc** to it.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 name abc
```

Related commands

display vrrp ipv6 binding

vrrp ipv6 vrid follow

vrrp ipv6 vrid follow

Use **vrrp ipv6 vrid follow** to configure an IPv6 VRRP group to follow a master group.

Use **undo vrrp ipv6 vrid follow** to remove the configuration.

Syntax

vrrp ipv6 vrid *virtual-router-id* **follow** *name*

undo vrrp ipv6 vrid *virtual-router-id* **follow**

Default

An IPv6 VRRP group does not follow a master group.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

name: Specifies a master IPv6 VRRP group by its name, a case-sensitive string of 1 to 20 characters.

Usage guidelines

This command configures an IPv6 VRRP group as a subordinate VRRP group to follow a master group. A subordinate IPv6 VRRP group can forward service traffic.

An IPv6 VRRP group cannot be both a master group and a subordinate group. The **vrrp ipv6 vrid name** and **vrrp ipv6 vrid follow** commands are mutually exclusive.

An IPv6 VRRP group stays in **Inactive** state if it is configured to follow a nonexistent master VRRP group.

If an IPv6 VRRP group in **Inactive** or **Initialize** state follows a master group that is not in **Inactive** state, the state of the VRRP group does not change.

Examples

Configure IPv6 VRRP group 1 to follow master group **abc**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 follow abc
```

Related commands

display vrrp ipv6 binding

vrrp ipv6 vrid name

New feature: Displaying master-to-subordinate IPv4 VRRP group bindings

Displaying master-to-subordinate IPv4 VRRP group bindings

Execute **display** commands in any view.

Task	Command
Display master-to-subordinate IPv4 VRRP group bindings.	**display vrrp binding** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*] | **name** *name*]

Command reference

display vrrp binding

Use **display vrrp binding** to display master-to-subordinate IPv4 VRRP group bindings.

Syntax

display vrrp binding [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*] | **name** *name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The interface must be an interface to which master IPv4 VRRP groups belong.

vrid *virtual-router-id*: Specifies a master IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

name *name*: Specifies a master IPv4 VRRP group by its name, a case-sensitive string of 1 to 20 characters.

Usage guidelines

If you do not specify any parameters, this command displays all IPv4 VRRP group bindings.

If you specify an interface but do not specify the virtual router ID of a master VRRP group, this command displays all master-to-subordinate VRRP group bindings on the specified interface.

If you specify an interface and the virtual router ID of a master VRRP group, this command displays the binding information about the specified master VRRP group on the specified interface.

Examples

Display master-to-subordinate IPv4 VRRP group bindings.

```
[Sysname] display vrrp binding
IPv4 virtual router binding information:
  Total number of master virtual routers           : 1
  Total number of subordinate virtual routers      : 2
  Interface : Vlan2                    Master VRID : 1
  Name      : a                        Status      : Backup
  Subordinate virtual routers : 1
    Interface : Vlan2                  VRID        : 4

  Interface : --                       Master VRID : --
  Name      : c                        Status      : --
  Subordinate virtual routers : 1
    Interface : Vlan2                  VRID        : 5
```

Table 1 Command output

Field	Description
Total number of master virtual routers	Total number of master VRRP groups.
Total number of subordinate virtual routers	Total number of subordinate VRRP groups.
Interface	Interface to which the master VRRP group belongs. If the master VRRP group does not exist, this field displays two hyphens (**--**).
Master VRID	Virtual router ID of the master VRRP group. If the master VRRP group does not exist, this field displays two hyphens (**--**).
Name	Name of the master VRRP group.
Status	Status of the router in the master VRRP group: • **Master**. • **Backup**.

Field	Description
	• **Initialize**. • **Inactive**. If the master VRRP group does not exist, this field displays two hyphens (**--**).
Subordinate virtual routers	Number of subordinate VRRP groups.
Interface	Interface to which the subordinate VRRP group belongs.
VRID	Virtual router ID of the subordinate VRRP group.

Related commands

vrrp vrid follow

vrrp vrid name

New feature: Displaying master-to-subordinate IPv6 VRRP group bindings

Displaying master-to-subordinate IPv6 VRRP group bindings

Execute **display** commands in any view.

Task	Command
Display master-to-subordinate IPv6 VRRP group bindings.	**display vrrp ipv6 binding** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*] | **name** *name*]

Command reference

display vrrp ipv6 binding

Use **display vrrp ipv6 binding** to display master-to-subordinate IPv6 VRRP group bindings.

Syntax

display vrrp ipv6 binding [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*] | **name** *name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The interface must be an interface to which master IPv6 VRRP groups belong.

vrid *virtual-router-id*: Specifies a master IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

name *name*: Specifies a master IPv6 VRRP group by its name, a case-sensitive string of 1 to 20 characters.

Usage guidelines

If you do not specify any parameters, this command displays all IPv6 VRRP group bindings.

If you specify an interface but do not specify the virtual router ID of a master IPv6 VRRP group, this command displays all master-to-subordinate IPv6 VRRP group bindings on the specified interface.

If you specify an interface and the virtual router ID of a master IPv6 VRRP group, this command displays the binding information about the specified master VRRP group on the specified interface.

Examples

Display master-to-subordinate IPv6 VRRP group bindings.

```
[Sysname] display vrrp ipv6 binding
IPv6 virtual router binding information:
  Total number of master virtual routers            : 1
  Total number of subordinate virtual routers       : 2
  Interface : Vlan2                       Master VRID : 1
  Name      : a                           Status      : Backup
  Subordinate virtual routers : 1
    Interface : Vlan2                     VRID        : 4

  Interface : --                          Master VRID : --
  Name      : c                           Status      : --
  Subordinate virtual routers : 1
    Interface : Vlan2                     VRID        : 5
```

Table 2 Command output

Field	Description
Total number of master virtual routers	Total number of master IPv6 VRRP groups.
Total number of subordinate virtual routers	Total number of subordinate IPv6 VRRP groups.
Interface	Interface to which the master IPv6 VRRP group belongs. If the master IPv6 VRRP group does not exist, this field displays two hyphens (**--**).
Master VRID	Virtual router ID of the master IPv6 VRRP group. If the master IPv6 VRRP group does not exist, this field displays two hyphens (**--**).
Name	Name of the master IPv6 VRRP group.
Status	Status of the device in the master IPv6 VRRP group: • **Master**. • **Backup**. • **Initialize**. • **Inactive**. If the master IPv6 VRRP group does not exist, this field displays two hyphens (**--**).

Field	Description
Subordinate virtual routers	Number of subordinate IPv6 VRRP groups.
Interface	Interface to which the subordinate IPv6 VRRP group belongs.
VRID	Virtual router ID of the subordinate IPv6 VRRP group.

Related commands

vrrp ipv6 vrid follow

vrrp ipv6 vrid name

New feature: Configuring the threshold for triggering monitor link group state switchover

Configuring the threshold for triggering monitor link group state switchover

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter monitor link group view.	**monitor-link group** *group-id*	N/A
3. Configure the threshold for triggering monitor link group state switchover.	**uplink up-port-threshold** *number-of-port*	By default, the threshold for triggering monitor link group state switchover is 1.

Command reference

uplink up-port-threshold

Use **uplink up-port-threshold** to configure the threshold for triggering monitor link group state switchover.

Use **undo uplink up-port-threshold** to restore the default.

Syntax

uplink up-port-threshold *number-of-port*

undo uplink up-port-threshold

Default

The threshold for triggering monitor link group state switchover is 1.

Views

Monitor link group view

Predefined user roles

network-admin

Parameters

number-of-port: Specifies the threshold for triggering monitor link group state switchover, in the range of 1 to 1024.

Usage guidelines

When the number of uplink interfaces in up state in a monitor link group is less than the specified threshold, the monitor link group goes down and shuts down its downlink interfaces. When the number of uplink interfaces in up state reaches the threshold, the monitor link group comes up and brings up all its downlink interfaces.

As a best practice, use the **display monitor-link group** command to get known the total number of uplink interfaces before executing the **uplink up-port-threshold** command. If you set the threshold to be greater than the total number of the uplink interfaces, the monitor link group cannot come up and data will be lost.

Examples

Set the threshold for triggering monitor link group state switchover to 5.

```
<Sysname> system-view
[Sysname] monitor-link group 1
[Sysname-mtlk-group1] uplink up-port-threshold 5
```

Related commands

display monitor-link group

New feature: ACL application to NETCONF over SOAP traffic

Applying an ACL to NETCONF over SOAP traffic

Step	Command	Remark
1. Enter system view.	**system-view**	N/A
2. Apply an ACL to NETCONF over SOAP traffic.	• Apply an ACL to NETCONF over SOAP over HTTP traffic (not available in FIPS mode): **netconf soap http acl** { *acl-number* | **name** *acl-name* } • Apply an ACL to NETCONF over SOAP over HTTPS traffic: **netconf soap https acl** { *acl-number* | **name** *acl-name* }	By default, no ACL is applied to NETCONF over SOAP traffic.

Command reference

netconf soap http acl

Use **netconf soap http acl** to apply an ACL to NETCONF over SOAP over HTTP traffic.

Use **undo netconf soap http acl** to restore the default.

Syntax

netconf soap http acl { *acl-number* **|** **name** *acl-name* }

undo netconf soap http acl

Default

No ACL is applied to NETCONF over SOAP over HTTP traffic.

Views

System view

Predefined user roles

network-admin

Parameters

acl-number: Specifies an ACL by its number in the range of 2000 to 2999.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**. The specified ACL must be an IPv4 basic ACL that has already been created.

Usage guidelines

This command is not available in FIPS mode.

Only NETCONF clients permitted by the applied ACL can access the device through SOAP over HTTP.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Use ACL 2001 to allow only NETCONF clients in the subnet 10.10.0.0/16 to access the device through SOAP over HTTP.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] netconf soap http acl 2001
```

netconf soap https acl

Use **netconf soap https acl** to apply an ACL to NETCONF over SOAP over HTTPS traffic.

Use **undo netconf soap https acl** to restore the default.

Syntax

netconf soap https acl { *acl-number* **|** **name** *acl-name* }

undo netconf soap https acl

Default

No ACL is applied to NETCONF over SOAP over HTTPS traffic.

Views

System view

Predefined user roles

network-admin

Parameters

acl-number: Specifies an ACL by its number in the range of 2000 to 2999.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**. The specified ACL must be an IPv4 basic ACL that has already been created.

Usage guidelines

Only NETCONF clients permitted by the applied ACL can access the device through SOAP over HTTPS.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Use ACL 2001 to allow only NETCONF clients in the subnet 10.10.0.0/16 to access the device through SOAP over HTTPS.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] netconf soap https acl 2001
```

New feature: Allowing link aggregation member ports to be in the deployed flow tables

Allowing link aggregation member ports to be in the deployed flow tables

To allow link aggregation member ports to be in the deployed flow tables:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter OpenFlow instance view.	**openflow instance** *instance-id*	N/A
3. Allow link aggregation member ports to be in the deployed flow tables.	**permit-port-type member-port**	By default, link aggregation member ports are not allowed to be in the deployed flow tables.

Command reference

permit-port-type member-port

Use **permit-port-type member-port** to allow link aggregation member ports to be in the deployed flow tables.

Use **undo permit-port-type** to disable link aggregation member ports to be in the deployed flow tables.

Syntax

permit-port-type member-port

undo permit-port-type

Default

Link aggregation member ports are not allowed to be in the deployed flow tables.

Views

OpenFlow instance view

Predefined user roles

network-admin

Examples

Configure OpenFlow instance 1 to allow link aggregation member ports to be in the deployed flow tables.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] permit-port-type member-port
```

New feature: Enabling OpenFlow connection backup

Enabling OpenFlow connection backup

By default, an OpenFlow instance backs up OpenFlow connections established over TCP on the subordinate device. This prevents connection interruption when a master/subordinate switchover occurs. For OpenFlow packets to be processed correctly when too many connections are backed up, you can disable OpenFlow connection backup.

To enable OpenFlow connection backup:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter OpenFlow instance view.	**openflow instance** *instance-id*	N/A
3. Enable OpenFlow connection backup.	**tcp-connection backup**	By default, OpenFlow connection backup is enabled.

Command reference

tcp-connection backup

Use **tcp-connection backup** to enable OpenFlow connection backup.

Use **undo tcp-connection backup** to disable OpenFlow connection backup.

Syntax

tcp-connection backup

undo tcp-connection backup

Default

OpenFlow connection backup is enabled.

Views

OpenFlow instance view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only on OpenFlow connections that the OpenFlow instance establishes with controllers through TCP.

By default, an OpenFlow instance backs up OpenFlow connections established over TCP on the subordinate device. This prevents connection interruption when a master/subordinate switchover occurs.

Examples

Enable OpenFlow connection backup for OpenFlow instance 1.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] tcp-connection backup
```

New feature: Port-specific 802.1X periodic reauthentication timer

Setting the 802.1X periodic reauthentication timer on a port

The device reauthenticates online 802.1X users on a port at the specified periodic reauthentication interval if the port is enabled with periodic online user reauthentication. To enable periodic online user reauthentication on a port, use the **dot1x re-authenticate** command.

A change to the periodic reauthentication timer applies to online users only after the old timer expires.

The port-specific periodic reauthentication timer has higher priority than the global periodic reauthentication timer.

To set the 802.1X periodic reauthentication timer 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. Set the 802.1X periodic reauthentication timer on the port.	**dot1x timer reauth-period** *reauth-period-value*	The default setting is 3600 seconds.

Command reference

dot1x timer reauth-period

Use **dot1x timer reauth-period** to set the 802.1X periodic reauthentication timer on a port.

Use **undo dot1x timer reauth-period** to restore the default.

Syntax

dot1x timer reauth-period *reauth-period-value*

undo dot1x timer reauth-period

Default

The 802.1X periodic reauthentication timer on a port is 3600 seconds.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

reauth-period-value: Specifies the 802.1X periodic reauthentication timer in seconds. The value range for the *reauth-period-value* argument is 60 to 7200.

Usage guidelines

The device reauthenticates online 802.1X users on a port at the specified periodic reauthentication interval if the port is enabled with periodic online user reauthentication. To enable periodic online user reauthentication on a port, use the **dot1x re-authenticate** command.

A change to the periodic reauthentication timer applies to online users only after the old timer expires.

The device selects a periodic reauthentication timer for 802.1X reauthentication in the following order:

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

Examples

Set the 802.1X periodic reauthentication timer to 60 seconds on Ten-GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] dot1x timer reauth-period 60
```

Related commands

- **dot1x re-authenticate**
- **dot1x timer**

New feature: Manual reauthentication for all online 802.1X users on a port

Manually reauthenticating all online 802.1X users on a port

This feature reauthenticates all online 802.1X users on a port after the **dot1x re-authenticate manual** command is executed. The feature is independent of the server-assigned reauthentication attribute and the periodic reauthentication feature.

When no server is reachable for reauthentication, the device keeps users online or logs off users, depending on the keep-online feature configuration on the port.

To manually reauthenticate all online 802.1X users on a port:

Step	Command
1. Enter system view.	**system-view**
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*
3. Manually reauthenticate all online 802.1X users on the port.	**dot1x re-authenticate manual**

Command reference

dot1x re-authenticate manual

Use **dot1x re-authenticate manual** to manually reauthenticate all online 802.1X users on a port.

Syntax

dot1x re-authenticate manual

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Examples

Manually reauthenticate all online 802.1X users on Ten-GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] dot1x re-authenticate manual
```

Related commands

dot1x re-authenticate

New feature: Enabling SNMP notifications for port security

Enabling SNMP notifications for port security

This feature allows port security to generate SNMP notifications to report important events. The generated notifications are delivered to the SNMP module. The SNMP module determines the notification output attributes based on the SNMP settings. For more information about SNMP notifications, see *Network Management and Monitoring Configuration Guide*.

To enable SNMP notifications for port security:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable SNMP notifications for port security.	**snmp-agent trap enable port-security** [**address-learned** | **dot1x-failure** | **dot1x-logoff** | **dot1x-logon** | **intrusion** | **mac-auth-failure** | **mac-auth-logoff** | **mac-auth-logon**] *	By default, SNMP notifications are disabled for port security.

Command reference

snmp-agent trap enable port-security

Use **snmp-agent trap enable port-security** to enable SNMP notifications for port security.

Use **undo snmp-agent trap enable port-security** to disable SNMP notifications for port security.

Syntax

snmp-agent trap enable port-security [**address-learned** | **dot1x-failure** | **dot1x-logoff** | **dot1x-logon** | **intrusion** | **mac-auth-failure** | **mac-auth-logoff** | **mac-auth-logon**] *

undo snmp-agent trap enable port-security [**address-learned** | **dot1x-failure** | **dot1x-logoff** | **dot1x-logon** | **intrusion** | **mac-auth-failure** | **mac-auth-logoff** | **mac-auth-logon**] *

Default

Port security SNMP notifications are disabled.

Views

System view

Predefined user roles

network-admin

network-operator

Parameters

address-learned: Sends an SNMP notification when a new MAC address is learned.

dot1x-failure: Sends an SNMP notification when a user fails 802.1X authentication.

dot1x-logoff: Sends an SNMP notification when an 802.1X user is logged off.

dot1x-logon: Sends an SNMP notification when a user passes 802.1X authentication.

intrusion: Sends an SNMP notification when an illegal frame is detected.

mac-auth-failure: Sends an SNMP notification when a user fails MAC authentication.

mac-auth-logoff: Sends an SNMP notification when a MAC authentication user is logged off.

mac-auth-logon: Sends an SNMP notification when a uses passes MAC authentication.

Usage guidelines

If you do not specify any keywords, this command controls the enabling status of all SNMP notifications for port security.

This command allows the port security module to generate SNMP notifications to report important events. The generated notifications are delivered to the SNMP module. The SNMP module determines the notification output attributes based on the SNMP settings. For more information about SNMP notifications, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable the device to send SNMP notifications when new MAC addresses are learned.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable port-security address-learned
```

Related commands

- **display port-security**
- **port-security enable**

New feature: DSCP value for OpenFlow packets

Setting a DSCP value for OpenFlow packets

Step	Command	Remarks
1. Enter system view	**system-view**	N/A
2. Enter OpenFlow instance view.	**openflow instance** *instance-id*	N/A
3. Set a DSCP value for OpenFlow packets.	**tcp dscp** *dscp-value*	By default, the DSCP value for OpenFlow packets is 16. This configuration takes effect only on OpenFlow packets over the main connection that the OpenFlow instance establishes with a controller through TCP.

Command reference

tcp dscp

Use **tcp dscp** to set a DSCP value for OpenFlow packets.

Use **undo tcp dscp** to restore the default.

Syntax

tcp dscp *dscp-value*

undo tcp dscp

Default

The DSCP value for OpenFlow packets is 16.

Views

OpenFlow instance view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value for OpenFlow packets, in the range of 0 to 63.

Examples

Set the DSCP value to 63 for OpenFlow packets.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] tcp dscp 63
```

Modified feature: SSH support for Suite B

Feature change description

The order of keywords was modified in the command for establishing a connection to an IPv6 Stelnet server based on Suite B algorithms.

Command changes

Modified command: ssh2 ipv6 suite-b

Old syntax

ssh2 ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**-i** *interface-type interface-number*] [**prefer-compress zlib**] [**dscp** *dscp-value* | **escape** *character* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

New syntax

ssh2 ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**dscp** *dscp-value* | **escape** *character* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

Views

User view

Change description

Before modification: When you specify an interface to connect to an IPv6 Stelnet server, specify the **-i** *interface-type interface-number* option after you specify Suite B algorithms.

After modification: When you specify an interface to connect to an IPv6 Stelnet server, specify the **-i** *interface-type interface-number* option before you specify Suite B algorithms.

Modified feature: Configuring the CDP-compatible operating mode for LLDP

Feature change description

LLDP support for the **rx** operating mode was added. In **rx** mode, the LLDP-enabled device can receive CDP packets but cannot transmit CDP packets.

Command changes

Modified command: lldp compliance admin-status cdp

Old syntax

lldp compliance admin-status cdp { **disable** | **txrx** }

New syntax

lldp compliance admin-status cdp { **disable** | **rx** | **txrx** }

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Management Ethernet interface view

Change description

The **rx** keyword was added. In **rx** operating mode, the LLDP-enabled device can receive CDP packets but cannot transmit CDP packets.

Modified feature: Configuring a traffic policing action

Feature change description

The **pps** keyword was added for the **cir** *committed-information-rate* and **pir** *peak-information-rate* options in the **car** command. The CIR and PIR can be specified in packets per second (pps).

Command changes

Modified command: car

Old syntax

car cir *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**green** *action* **|** **red** *action* **|** **yellow** *action*] *

car cir *committed-information-rate* [**cbs** *committed-burst-size*] **pir** *peak-information-rate* [**ebs** *excess-burst-size*] [**green** *action* **|** **red** *action* **|** **yellow** *action*] *

New syntax

car cir [**pps**] *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**green** *action* **|** **red** *action* **|** **yellow** *action*] *

car cir [**pps**] *committed-information-rate* [**cbs** *committed-burst-size*] **pir** [**pps**] *peak-information-rate* [**ebs** *excess-burst-size*] [**green** *action* **|** **red** *action* **|** **yellow** *action*] *

Views

Traffic behavior view

Change description

Before modification, the CIR and PIR can be specified only in kbps.

After modification, the CIR and PIR can be specified in either kbps or pps. However, they must use the same unit.

Release 2423

This release has the following changes:

New feature: DHCP address pool application to a VPN instance

Applying a DHCP address pool to a VPN instance

If a DHCP address pool is applied to a VPN instance, the DHCP server assigns IP addresses in the address pool to clients in the VPN instance. Addresses in the address pool will not be assigned to clients on the public network or in other VPN instances.

The DHCP server can obtain the VPN instance to which a DHCP client belongs from the following information:

- The client's VPN information stored in authentication modules, such as IPoE.
- The VPN information of the DHCP server's interface that receives DHCP packets from the client.

The VPN information from authentication modules takes precedence over the VPN information of the receiving interface.

To apply a DHCP address pool to a VPN instance:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a DHCP address pool and enter its view.	**dhcp server ip-pool** *pool-name*	By default, no DHCP address pool exists.
3. Apply the address pool to a VPN instance.	**vpn-instance** *vpn-instance-name*	By default, a DHCP address pool is not applied to any VPN instance.

Command reference

New command: vpn-instance

Use **vpn-instance** to apply a DHCP address pool to a VPN instance.

Use **undo vpn-instance** to restore the default.

Syntax

vpn-instance *vpn-instance-name*

undo vpn-instance

Default

A DHCP address pool is not applied to any VPN instance.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

vpn-instance-name: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

If a DHCP address pool is applied to a VPN instance, the DHCP server assigns IP addresses in the address pool to clients in the VPN instance. Addresses in the address pool will not be assigned to clients on the public network or in other VPN instances.

The DHCP server identifies the VPN instance to which a DHCP client belongs according to the following information:

- The client's VPN information stored in authentication modules.
- The VPN information of the DHCP server's interface that receives DHCP packets from the client.

The VPN information from authentication modules takes precedence over the VPN information of the receiving interface.

Examples

Apply the address pool 0 to the VPN instance **abc**.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] vpn-instance abc
```

Modified commands: Commands for displaying the DHCP server

Old syntax

display dhcp server conflict [**ip** *ip-address*]

display dhcp server expired [**ip** *ip-address* **|** **pool** *pool-name*]

display dhcp server free-ip [**pool** *pool-name*]

display dhcp server ip-in-use [**ip** *ip-address* **|** **pool** *pool-name*]

display dhcp server pool [*pool-name*]

display dhcp server statistics [**pool** *pool-name*]

New syntax

display dhcp server conflict [**ip** *ip-address*] [**vpn-instance** *vpn-instance-name*]

display dhcp server expired [[**ip** *ip-address*] [**vpn-instance** *vpn-instance-name*] **|** **pool** *pool-name*]

display dhcp server free-ip [**pool** *pool-name* **|** **vpn-instance** *vpn-instance-name*]

display dhcp server ip-in-use [[**ip** *ip-address*] [**vpn-instance** *vpn-instance-name*] **|** **pool** *pool-name*]

display dhcp server pool [*pool-name* **|** **vpn-instance** *vpn-instance-name*]

display dhcp server statistics [**pool** *pool-name* **|** **vpn-instance** *vpn-instance-name*]

Views

Any view

Change description

Before modification: The commands do not support the **vpn-instance** *vpn-instance-name* option.

After modification: The commands support the **vpn-instance** *vpn-instance-name* option.

Modified command: dhcp server forbidden-ip

Old syntax

dhcp server forbidden-ip *start-ip-address* [*end-ip-address*]

New syntax

dhcp server forbidden-ip *start-ip-address* [*end-ip-address*] [**vpn-instance** *vpn-instance-name*]

Views

System view

Change description

Before modification: The command does not support the **vpn-instance** *vpn-instance-name* option.

After modification: The commands supports the **vpn-instance** *vpn-instance-name* option.

Modified commands: Commands for maintaining the DHCP server

Old syntax

reset dhcp server conflict [**ip** *ip-address*]

reset dhcp server expired [**ip** *ip-address* **|** **pool** *pool-name*]

reset dhcp server ip-in-use [**ip** *ip-address* **|** **pool** *pool-name*]

reset dhcp server statistics

New syntax

reset dhcp server conflict [**ip** *ip-address*] [**vpn-instance** *vpn-instance-name*]

reset dhcp server expired [[**ip** *ip-address*] [**vpn-instance** *vpn-instance-name*] **|** **pool** *pool-name*]

reset dhcp server ip-in-use [[**ip** *ip-address*] [**vpn-instance** *vpn-instance-name*] **|** **pool** *pool-name*]

reset dhcp server statistics [**vpn-instance** *vpn-instance-name*]

Views

User view

Change description

Before modification: The commands do not support the **vpn-instance** *vpn-instance-name* option.

After modification: The commands support the **vpn-instance** *vpn-instance-name* option.

New feature: RADIUS server status detection

Configuring a test profile for RADIUS server status detection

Use a test profile to detect whether a RADIUS authentication server is reachable at a detection interval. To detect the RADIUS server status, you must configure the RADIUS server to use this test profile in a RADIUS scheme.

With the test profile specified, the device sends a detection packet to the RADIUS server within each detection interval. The detection packet is a simulated authentication request that includes the specified user name in the test profile.

- If the device receives a response from the server within the interval, it sets the server to the active state.
- If the device does not receive any response from the server within the interval, it sets the server to the blocked state.

The device refreshes the RADIUS server status at each detection interval according to the detection result.

The device stops detecting the status of the RADIUS server when one of the following operations is performed:

- The RADIUS server is removed from the RADIUS scheme.

- The test profile configuration is removed for the RADIUS server in RADIUS scheme view.
- The test profile is deleted.
- The RADIUS server is manually set to the blocked state.
- The RADIUS scheme is deleted.

To configure a test profile for RADIUS server status detection:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure a test profile for detecting the status of RADIUS authentication servers.	**radius-server test-profile** *profile-name* **username** *name* [**interval** *interval*]	By default, no test profiles exist. You can configure multiple test profiles in the system.

Command reference

radius-server test-profile

Use **radius-server test-profile** to configure a test profile for detecting the RADIUS server status.

Use **undo radius-server test-profile** to delete a RADIUS test profile.

Syntax

radius-server test-profile *profile-name* **username** *name* [**interval** *interval*]

undo radius-server test-profile *profile-name*

Default

No test profiles exist.

Views

System view

Predefined user roles

network-admin

Parameters

profile-name: Specifies the name of the test profile, which is a case-sensitive string of 1 to 31 characters.

username *name*: Specifies the username in the detection packets. The *name* argument is a case-sensitive string of 1 to 253 characters.

interval *interval*: Specifies the interval for sending a detection packet, in minutes. The value range for the *interval* argument is 1 to 3600, and the default value is 60.

Usage guidelines

You can execute this command multiple times to configure multiple test profiles.

If you specify a nonexistent test profile for a RADIUS server, the device does not detect the status of the server until you create the test profile on the device.

When you delete a test profile, the device stops detecting the status of the RADIUS servers that use the test profile.

Examples

Configure a test profile named **abc** for RADIUS server status detection. The detection packet uses **admin** as the username and is sent every 10 minutes.

```
<Sysname> system-view
[Sysname] radius-server test-profile abc username admin interval 10
```

New feature: RADIUS server load sharing

Enabling the RADIUS server load sharing feature

By default, the device communicates with RADIUS servers based on the server roles. It first attempts to communicate with the primary server, and, if the primary server is unavailable, it then searches for the secondary servers in the order they are configured. The first secondary server in active state is used for communication. In this process, the workload is always placed on the active server.

Use the RADIUS server load sharing feature to dynamically distribute the workload over multiple servers regardless of their server roles. The device forwards an AAA request to the most appropriate server of all active servers in the scheme after it compares the weight values and numbers of currently served users. Specify a weight value for each RADIUS server based on the AAA capacity of the server. A larger weight value indicates a higher AAA capacity.

In RADIUS server load sharing, once the device sends a start-accounting request to a server for a user, it forwards all subsequent accounting requests of the user to the same server. If the accounting server is unreachable, the device returns an accounting failure message rather than searching for another active accounting server.

To enable the RADIUS server load sharing feature:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter RADIUS scheme view.	**radius scheme** *radius-scheme-name*	N/A
3. Enable the RADIUS server load sharing feature.	**algorithm loading-share enable**	By default, this feature is disabled.

Command reference

algorithm loading-share enable

Use **algorithm loading-share enable** to enable the RADIUS server load sharing feature.

Use **undo algorithm loading-share enable** to disable the RADIUS server load sharing feature.

Syntax

algorithm loading-share enable

undo algorithm loading-share enable

Default

The RADIUS server load sharing feature is disabled.

Views

RADIUS scheme view

Predefined user roles

network-admin

Usage guidelines

Use the RADIUS server load sharing feature to dynamically distribute the workload over multiple servers regardless of their server roles. The device forwards an AAA request to the most appropriate server of all active servers in the scheme after it compares the weight values and numbers of currently served users. Specify a weight value for each RADIUS server based on the AAA capacity of the server. A larger weight value indicates a higher AAA capacity.

In RADIUS server load sharing, once a server starts accounting for a user, it forwards all subsequent accounting requests of the user to the same server. If the accounting server is unreachable, the device returns an accounting failure message rather than searching for another active accounting server.

Examples

Enable the RADIUS server load sharing feature for the RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] algorithm loading-share enable
```

New feature: IP address pool authorization by AAA

Configuring the IP address pool authorization attribute

The IP address pool assigned to users as an authorization attribute provides address allocation. Authenticated users obtain IPv4 or IPv6 addresses from the authorized address pool.

To configure the IP address pool authorization attribute for an ISP domain:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter ISP domain view.	**domain** *isp-name*	N/A
3. Configure the IP address pool authorization attribute.	**authorization-attribute** { **ip-pool** *pool-name* | **ipv6-pool** *ipv6-pool-name* }	By default, no authorization attribute is configured for an ISP domain.

To configure the IP address pool authorization attribute for a local user:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter local user view.	**local-user** *user-name* [**class** { **manage** | **network** }]	N/A
3. Configure the IP address pool authorization attribute.	**authorization-attribute** { **ip-pool** *pool-name* | **ipv6-pool** *ipv6-pool-name* } *	By default, no authorization attribute is configured for a local user.

To configure the IP address pool authorization attribute for a user group:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter user group view.	**user-group** *group-name*	N/A
3. Configure the IP address pool authorization attribute.	**authorization-attribute** { **ip-pool** *pool-name* | **ipv6-pool** *ipv6-pool-name* } *	By default, no authorization attribute is configured for a user group.

Command reference

authorization-attribute (ISP domain view)

Use **authorization-attribute** { **ip-pool** | **ipv6-pool** } to configure the IP address pool authorization attribute.

Use **undo authorization-attribute** { **ip-pool** | **ipv6-pool** } to delete the IP address pool authorization attribute.

Syntax

authorization-attribute { **ip-pool** *pool-name* | **ipv6-pool** *ipv6-pool-name* }

undo authorization-attribute { **ip-pool** | **ipv6-pool** }

Default

No authorization attribute is configured.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

ip-pool *pool-name*: Specifies an IPv4 address pool for users. The *pool-name* argument is a case-insensitive string of 1 to 63 characters.

ipv6-pool *ipv6-pool-name*: Specifies an IPv6 address pool for users. The *ipv6-pool-name* argument is a case-insensitive string of 1 to 63 characters.

Examples

Configure the authorization IPv4 address pool named **pool1** for ISP domain **test**.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization-attribute ip-pool pool1
```

authorization-attribute (local user view/user group view)

Use **authorization-attribute** { **ip-pool** | **ipv6-pool** } * to configure the IP address pool authorization attribute.

Use **undo authorization-attribute** { **ip-pool** | **ipv6-pool** } * to delete the IP address pool authorization attribute.

Syntax

authorization-attribute { **ip-pool** *pool-name* **| ipv6-pool** *ipv6-pool-name* } *

undo authorization-attribute { **ip-pool | ipv6-pool** } *

Default

No authorization attribute is configured.

Views

Local user view

User group view

Predefined user roles

network-admin

Parameters

ip-pool *pool-name*: Specifies an IPv4 address pool for users. The *pool-name* argument is a case-insensitive string of 1 to 63 characters.

ipv6-pool *ipv6-pool-name*: Specifies an IPv6 address pool for users. The *ipv6-pool-name* argument is a case-insensitive string of 1 to 63 characters.

Examples

Configure the authorization IPv4 address pool named **pool1** for network access user **abc**.

```
<Sysname> system-view
[Sysname] local-user abc class network
[Sysname-luser-network-abc] authorization-attribute ip-pool pool1
```

Configure the authorization IPv4 address pool named **pool2** for user group **abc**.

```
<Sysname> system-view
[Sysname] user-group abc
[Sysname-ugroup-abc] authorization-attribute ip-pool pool2
```

New feature: 802.1X guest VLAN assignment delay

Enabling 802.1X guest VLAN assignment delay

This feature delays assigning an 802.1X-enabled port to the 802.1X guest VLAN when 802.1X authentication is triggered on the port.

This feature applies only to situations where 802.1X authentication is triggered by EAPOL-Start packets from 802.1X clients or packets from unknown MAC addresses.

To use this feature, the 802.1X-enabled port must perform MAC-based access control. If 802.1X authentication is triggered by packets from unknown MAC addresses, the port must be also configured with unicast trigger.

When 802.1X authentication is triggered on a port the device performs the following operations:

1. Sends a unicast EAP-Request/Identity packet to the MAC address.
2. Retransmits the packet if no response has been received within the username request timeout interval set by using the **dot1x timer tx-period** command.
3. Assigns the port the 802.1X guest VLAN after the maximum number of request attempts set by using the **dot1x retry** command is reached.

To enable 802.1X guest VLAN assignment delay 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.	Enable 802.1X guest VLAN assignment delay on the port.	**dot1x guest-vlan-delay** { **eapol** | **new-mac** }	By default, 802.1X guest VLAN assignment delay is disabled on a port.

Command reference

dot1x guest-vlan-delay

Use **dot1x guest-vlan-delay** to enable 802.1X guest VLAN assignment delay on a port.

Use **undo dot1x guest-vlan-delay** to disable the specified 802.1X guest VLAN assignment delay on a port.

Syntax

dot1x guest-vlan-delay { **eapol** | **new-mac** }

undo dot1x guest-vlan-delay [**eapol** | **new-mac**]

Default

802.1X guest VLAN assignment delay is disabled on a port.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

eapol: Specifies EAPOL-triggered 802.1X guest VLAN assignment delay. This keyword takes effect if 802.1X authentication is triggered by EAPOL-Start packets.

new-mac: Specifies new MAC-triggered 802.1X guest VLAN assignment delay. This keyword takes effect if 802.1X authentication is triggered by packets from unknown MAC addresses.

Usage guidelines

The **undo** form of the command disables both EAPOL packets and packets from unknown MAC addresses from triggering 802.1X guest VLAN assignment delay if you do not specify any keyword.

Examples

Enable EAPOL-triggered 802.1X guest VLAN assignment delay on Ten-GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] dot1x guest-vlan-delay eapol
```

New feature: Sending 802.1X protocol packets without VLAN tags

Sending 802.1X protocol packets out of a port without VLAN tags

By default, the device sends 802.1X protocol packets with VLAN tags out of an 802.1X-enabled port. This feature enables the device to send 802.1X protocol packets without VLAN tags. It prevents terminal devices connected to the port from failing 802.1X authentication because they cannot identify VLAN tags.

This feature is not available for Ethernet ports whose link type is access.

To enable the device to send 802.1X protocol packets out of a port without VLAN tags:

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 device to send 802.1X protocol packets out of the port without VLAN tags.	**dot1x eapol untag**	By default, 802.1X protocol packets are sent out of a port with VLAN tags.

Command reference

dot1x eapol untag

Use **dot1x eapol untag** to enable the device to send 802.1X protocol packets out of a port without VLAN tags.

Use **undo dot1x eapol untag** to enable the device to send 802.1X protocol packets out of a port with VLAN tags.

Syntax

dot1x eapol untag

undo dot1x eapol untag

Default

The device sends 802.1X protocol packets out of a port with VLAN tags.

Views

Ethernet interface view

Predefined user roles

network-admin

Examples

Enable the device to send 802.1X protocol packets out of Ten-GigabitEthernet 1/0/1 without VLAN tags.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] dot1x eapol untag
```

New feature: 802.1X critical voice VLAN

Enabling 802.1X critical voice VLAN

The 802.1X critical voice VLAN on a port accommodates 802.1X voice users who have failed authentication because none of the RADIUS servers in their ISP domain are reachable.

The critical voice VLAN feature takes effect when 802.1X authentication is performed only through RADIUS servers.

With the 802.1X critical voice VLAN enabled, the access device handles VLANs on an 802.1X-enabled port as follows:

Authentication status	VLAN manipulation
A voice user that has not been assigned to any VLAN fails 802.1X authentication because all the RADIUS servers are unreachable.	The device assigns the port to the 802.1X critical voice VLAN.
A voice user in the 802.1X Auth-Fail VLAN fails authentication because all the RADIUS servers are unreachable.	The port is still in the 802.1X Auth-Fail VLAN.
A voice user in the 802.1X guest VLAN fails authentication because all the RADIUS servers are unreachable.	The device removes the port from the 802.1X guest VLAN and assigns the port to the 802.1X critical voice VLAN.

When a reachable RADIUS server is detected, the device performs the following operations:

- If MAC-based access control is used, the device removes 802.1X voice users from the critical voice VLAN. The port sends a unicast EAP-Request/Identity packet to each 802.1X voice user that was assigned to the critical voice VLAN to trigger authentication.
- If port-based access control is used, the device removes the port from the critical voice VLAN. The port sends a multicast EAP-Request/Identity packet to all 802.1X voice users on the port to trigger authentication.

Configuration prerequisites

Before you enable the 802.1X critical voice VLAN on a port, complete the following tasks:

- Enable LLDP both globally and on the port.

  The device uses LLDP to identify voice users. For information about LLDP, see *Layer 2—LAN Switching Configuration Guide*.
- Enable voice VLAN on the port.

Configuration procedure

To enable the 802.1X critical voice VLAN feature on a port:

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

Step	Command	Remarks
view.	*interface-number*	
3. Enable the 802.1X critical voice VLAN feature on a port.	**dot1x critical-voice-vlan**	By default, the 802.1X critical voice VLAN feature is disabled on the port.

Command reference

dot1x critical-voice-vlan

Use **dot1x critical-voice-vlan** to enable the 802.1X critical voice VLAN on a port.

Use **undo dot1x critical-voice-vlan** to restore the default.

Syntax

dot1x critical-voice-vlan

undo dot1x critical-voice-vlan

Default

The 802.1X critical voice VLAN is disabled on a port.

Views

Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

The 802.1X critical voice VLAN on a port accommodates 802.1X voice users who have failed authentication because none of the RADIUS servers in their ISP domain are reachable.

Before you enable the 802.1X critical voice VLAN on the port, make sure the following requirements are met:

- The port is configured with the voice VLAN.

  To configure a voice VLAN on a port, use the **voice-vlan enable** command (see *Layer 2—LAN Switching Command Reference*).
- LLDP is enabled both globally and on the port.

  The device uses LLDP to identify voice users. For information about LLDP commands, see *Layer 2—LAN Switching Command Reference*.

Examples

Enable the 802.1X critical voice VLAN on Ten-GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] dot1x critical-voice-vlan
```

Related commands

- **display dot1x**
- **lldp enable** (*Layer 2—LAN Switching Command Reference*)
- **lldp global enable** (*Layer 2—LAN Switching Command Reference*)
- **voice-vlan enable** *(Layer 2—LAN Switching Command Reference)*

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).

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 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

New command: 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 Ten-GigabitEthernet 1/0/1 to send EAP-Success packets to 802.1X users in the critical VLAN.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] dot1x critical eapol
```

New feature: MAC authentication critical voice VLAN

Enabling MAC authentication critical voice VLAN

The MAC authentication critical voice VLAN on a port accommodates MAC authentication voice users who have failed authentication because none of the RADIUS servers in their ISP domain are reachable.

Configuration prerequisites

Before you enable the MAC authentication critical voice VLAN on a port, complete the following tasks:

- Enable LLDP both globally and on the port.

  The device uses LLDP to identify voice users. For information about LLDP, see *Layer 2—LAN Switching Configuration Guide*.
- Enable voice VLAN on the port.

Configuration procedure

To enable the MAC authentication critical voice VLAN feature 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. Enable the MAC authentication critical voice VLAN feature on a port.	**mac-authentication critical-voice-vlan**	By default, the MAC authentication critical voice VLAN feature is disabled on the port.

Command reference

mac-authentication critical-voice-vlan

Use **mac-authentication critical-voice-vlan** to enable the MAC authentication critical voice VLAN on a port.

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

Syntax

mac-authentication critical-voice-vlan

undo mac-authentication critical-voice-vlan

Default

The MAC authentication critical voice VLAN is disabled on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

The MAC authentication critical voice VLAN on a port accommodates MAC authentication voice users who have failed authentication because none of the RADIUS servers in their ISP domain are reachable.

Before you enable the MAC authentication critical voice VLAN on the port, make sure the following requirements are met:

- The port is configured with the voice VLAN.

  To configure a voice VLAN on a port, use the **voice-vlan enable** command (see *Layer 2—LAN Switching Command Reference*).
- LLDP is enabled both globally and on the port.

  The device uses LLDP to identify voice users. For information about LLDP commands, see *Layer 2—LAN Switching Command Reference*.

Examples

Enable the MAC authentication critical voice VLAN on Ten-GigabitEthernet 1/0/1.

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

Related commands

- **display mac-authentication**
- **lldp enable** (*Layer 2—LAN Switching Command Reference*)
- **lldp global enable** (*Layer 2—LAN Switching Command Reference*)
- **voice-vlan enable** (*Layer 2—LAN Switching Command Reference*)

reset mac-authentication critical-voice-vlan

Use **reset mac-authentication critical-voice-vlan** to remove MAC authentication users from the MAC authentication critical voice VLAN on a port.

Syntax

reset mac-authentication critical-voice-vlan interface *interface-type interface-number* [**mac-address** *mac-address*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

mac-address *mac-address*: Specifies a user by its MAC address. If you do not specify this option, the command removes all users from the MAC authentication critical voice VLAN on the port.

Examples

Remove the user with MAC address **1-1-1** from the MAC authentication critical voice VLAN on Ten-GigabitEthernet 1/0/1.

```
<Sysname> reset mac-authentication critical-voice-vlan interface ten-gigabitethernet
1/0/1 mac-address 1-1-1
```

Related commands

- **display mac-authentication**
- **mac-authentication critical-voice-vlan**

New feature: Parallel processing of MAC authentication and 802.1X authentication

Enabling parallel processing of MAC authentication and 802.1X authentication

Use this feature to enable a port to process MAC authentication and 802.1X authentication in a parallel manner if the port performs MAC authentication after 802.1X authentication is complete. When the port receives a packet from an unknown MAC address, it sends a unicast EAP-Request/Identity packet to the MAC address. After that, the port immediately processes MAC authentication without waiting for the 802.1X authentication result.

For a port to perform MAC authentication before it is assigned to the 802.1X guest VLAN, enable this feature and 802.1X guest VLAN assignment delay. After MAC authentication succeeds, the device will assign the port to the authorization VLAN.

For information about 802.1X guest VLAN assignment delay, see "New feature: 802.1X guest VLAN assignment delay."

This feature applies to the following situations where a port that is enabled with 802.1X unicast trigger uses both 802.1X authentication and MAC authentication:

- A port is enabled with both 802.1X and MAC authentications, and the port performs MAC-based access control for 802.1X authentication.
- A port is enabled with port security, and the port security mode is **userlogin-secure-or-mac** or **userlogin-secure-or-mac-ext**.

  For information about port security mode configuration, see port security in S*ecurity Command Reference*.

To ensure that this feature can function correctly, do not enable MAC authentication delay on the port. This operation will delay MAC authentication after 802.1X authentication is triggered.

To enable parallel processing of MAC authentication and 802.1X authentication 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. Enable parallel processing of MAC authentication and 802.1X authentication on the port.	**mac-authentication parallel-with-dot1x**	By default, this feature is disabled.

Command reference

mac-authentication parallel-with-dot1x

Use **mac-authentication parallel-with-dot1x** to enable parallel processing of MAC authentication and 802.1X authentication on a port.

Use **undo mac-authentication parallel-with-dot1x** to restore the default.

Syntax

mac-authentication parallel-with-dot1x

undo mac-authentication parallel-with-dot1x

Default

Parallel processing of MAC authentication and 802.1X authentication is disabled on a port.

Views

Ethernet interface view

Predefined user roles

network-admin

Examples

Enable parallel processing of MAC authentication and 802.1X authentication on Ten-GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] mac-authentication parallel-with-dot1x
```

New feature: IPsec support for Suite B

Suite B contains a set of encryption and authentication algorithms that meet high security requirements. IPsec and IKEv2 provide stronger protection by supporting Suite B.

Overview

Internet Key Exchange version 2 (IKEv2) is an enhanced version of IKEv1. The same as IKEv1, IKEv2 has a set of self-protection mechanisms and can be used on insecure networks for reliable identity authentication, key distribution, and IPsec SA negotiation. IKEv2 provides stronger protection against attacks and higher key exchange ability and needs less message exchanges than IKEv1.

IKEv2 negotiation process

Compared with IKEv1, IKEv2 simplifies the negotiation process and is much more efficient.

IKEv2 defines three types of exchanges: initial exchanges, CREATE_CHILD_SA exchange, and INFORMATIONAL exchange.

As shown in Figure 6, IKEv2 uses two exchanges during the initial exchange process: IKE_SA_INIT and IKE_AUTH, each with two messages.

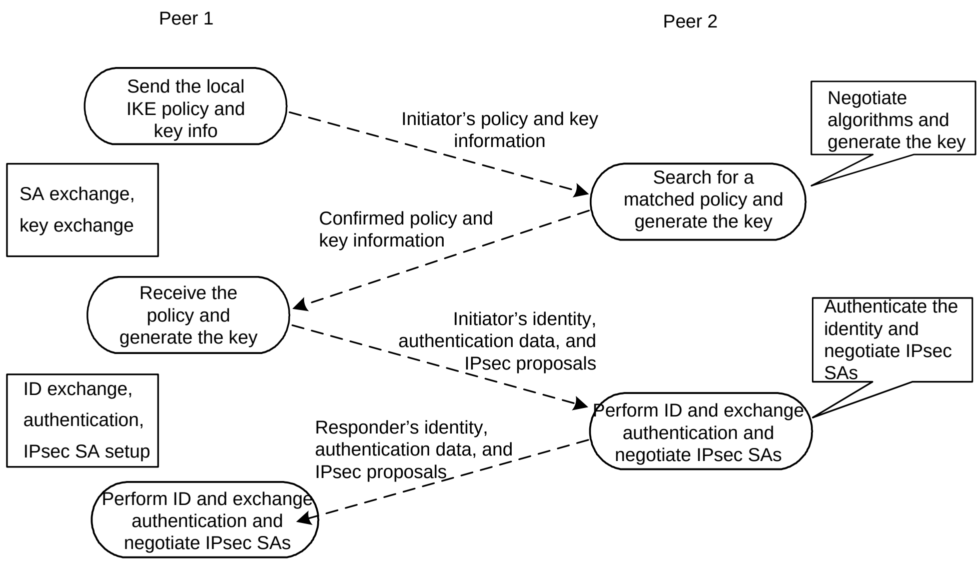
- **IKE_SA_INIT exchange**—Negotiates IKE SA parameters and exchanges keys.
- **IKE_AUTH exchange**—Authenticates the identity of the peer and establishes IPsec SAs.

After the four-message initial exchanges, IKEv2 sets up one IKE SA and one pair of IPsec SAs. For IKEv1 to set up one IKE SA and one pair of IPsec SAs, it must go through two phases that use a minimum of six messages.

To set up one more pair of IPsec SAs within the IKE SA, IKEv2 goes on to perform an additional two-message exchange—the CREATE_CHILD_SA exchange. One CREATE_CHILD_SA exchange creates one pair of IPsec SAs. IKEv2 also uses the CREATE_CHILD_SA exchange to rekey IKE SAs and Child SAs.

IKEv2 uses the INFORMATIONAL exchange to convey control messages about errors and notifications.

Figure 6 IKEv2 Initial exchange process



New features in IKEv2

DH guessing

In the IKE_SA_INIT exchange, the initiator guesses the DH group that the responder is most likely to use and sends it in an IKE_SA_INIT request message. If the initiator's guess is correct, the responder responds with an IKE_SA_INIT response message and the IKE_SA_INIT exchange is finished. If the guess is wrong, the responder responds with an INVALID_KE_PAYLOAD message that contains the DH group that it wants to use. The initiator then uses the DH group selected by the responder to reinitiate the IKE_SA_INIT exchange. The DH guessing mechanism allows for more flexible DH group configuration and enables the initiator to adapt to different responders.

Cookie challenging

Messages for the IKE_SA_INIT exchange are in plain text. An IKEv1 responder cannot confirm the validity of the initiators and must maintain half-open IKE SAs, which makes the responder susceptible to DoS attacks. An attacker can send a large number of IKE_SA_INIT requests with forged source IP addresses to the responder, exhausting the responder's system resources.

IKEv2 introduces the cookie challenging mechanism to prevent such DoS attacks. When an IKEv2 responder maintains a threshold number of half-open IKE SAs, it starts the cookie challenging mechanism. The responder generates a cookie and includes it in the response sent to the initiator. If the initiator initiates a new IKE_SA_INIT request that carries the correct cookie, the responder considers the initiator valid and proceeds with the negotiation. If the carried cookie is incorrect, the responder terminates the negotiation.

The cookie challenging mechanism automatically stops working when the number of half-open IKE SAs drops below the threshold.

IKEv2 SA rekeying

For security purposes, both IKE SAs and IPsec SAs have a lifetime and must be rekeyed when the lifetime expires. An IKEv1 SA lifetime is negotiated. An IKEv2 SA lifetime, in contrast, is configured. If two peers are configured with different lifetimes, the peer with the shorter lifetime always initiates the SA rekeying. This mechanism reduces the possibility that two peers will simultaneously initiate a rekeying. Simultaneous rekeying results in redundant SAs and SA status inconsistency on the two peers.

IKEv2 message retransmission

Unlike IKEv1 messages, IKEv2 messages appear in request/response pairs. IKEv2 uses the Message ID field in the message header to identify the request/response pair. If an initiator sends a request but receives no response with the same Message ID value within a specific period of time, the initiator retransmits the request.

It is always the IKEv2 initiator that initiates the retransmission, and the retransmitted message must use the same Message ID value.

Protocols and standards

- RFC 2408, Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 4306, Internet Key Exchange (IKEv2) Protocol
- RFC 4718, IKEv2 Clarifications and Implementation Guidelines
- RFC 2412, The OAKLEY Key Determination Protocol
- RFC 5996, Internet Key Exchange Protocol Version 2 (IKEv2)

IKEv2 configuration task list

Determine the following parameters prior to IKEv2 configuration:

- The strength of the algorithms for IKEv2 negotiation, including the encryption algorithms, integrity protection algorithms, PRF algorithms, and DH groups. Different algorithms provide different levels of protection. A stronger algorithm means better resistance to decryption of protected data but requires more resources. Typically, the longer the key, the stronger the algorithm.
- The local and remote identity authentication methods.
  - To use the pre-shared key authentication method, you must determine the pre-shared key.
  - To use the RSA digital signature authentication method, you must determine the PKI domain for the local end to use. For information about PKI, see "Configuring PKI."

To configure IKEv2, perform the following tasks:

Tasks at a glance	Remarks
(Required.) Configuring an IKEv2 profile	N/A
(Required.) Configuring an IKEv2 policy	N/A
(Optional.) Configuring an IKEv2 proposal	If you specify an IKEv2 proposal in an IKEv2 policy, you must configure the IKEv2 proposal.
Configuring an IKEv2 keychain	Required when either end or both ends use the pre-shared key authentication method.
Configure global IKEv2 parameters • (Optional.) Enabling the cookie challenging feature • (Optional.) Configuring the IKEv2 DPD feature • (Optional.) Configuring the IKEv2 NAT keepalive feature	The cookie challenging feature takes effect only on IKEv2 responders.

Configuring an IKEv2 profile

An IKEv2 profile is intended to provide a set of parameters for IKEv2 negotiation. To configure an IKEv2 profile, perform the following tasks:

1. Specify the local and remote identity authentication methods.

   The local and remote identity authentication methods must both be specified and they can be different. You can specify only one local identity authentication method and multiple remote identity authentication methods.

2. Configure the IKEv2 keychain or PKI domain for the IKEv2 profile to use:
   - To use digital signature authentication, configure a PKI domain.
   - To use pre-shared key authentication, configure an IKEv2 keychain.

3. Configure the local ID, the ID that the device uses to identify itself to the peer during IKEv2 negotiation:
   - For digital signature authentication, the device can use an ID of any type. If the local ID is an IP address that is different from the IP address in the local certificate, the device uses the FQDN as the local ID. The FQDN is the device name configured by using the **sysname** command.
   - For pre-shared key authentication, the device can use an ID of any type other than the DN.

4. Configure peer IDs.

   The device compares the received peer ID with the peer IDs of its local IKEv2 profiles. If a match is found, it uses the IKEv2 profile with the matching peer ID for IKEv2 negotiation. IKEv2 profiles will be compared in descending order of their priorities.

5. Specify a local interface or IP address for the IKEv2 profile so the profile can be applied only to the specified interface or IP address. For this task, specify the local address configured in IPsec policy or IPsec policy template view (using the **local-address** command). If no local address is configured, specify the IP address of the interface that uses the IPsec policy.

6. Specify a priority number for the IKEv2 profile. To determine the priority of an IKEv2 profile:
   a. First, the device examines the existence of the **match local** command. An IKEv2 profile with the **match local** command configured has a higher priority.
   b. If a tie exists, the device compares the priority numbers. An IKEv2 profile with a smaller priority number has a higher priority.
   c. If a tie still exists, the device prefers an IKEv2 profile configured earlier.

7. Specify a VPN instance for the IKEv2 profile. The IKEv2 profile is used for IKEv2 negotiation only on the interfaces that belong to the VPN instance.
8. Configure the IKEv2 SA lifetime.

   The local and remote ends can use different IKEv2 SA lifetimes. They do not negotiate the lifetime. The end with a smaller SA lifetime will initiate an SA negotiation when the lifetime expires.
9. Configure IKEv2 DPD to detect dead IKEv2 peers. You can also configure this feature in system view. If you configure IKEv2 DPD in both views, the IKEv2 DPD settings in IKEv2 profile view apply. If you do not configure IKEv2 DPD in IKEv2 profile view, the IKEv2 DPD settings in system view apply.
10. Specify an inside VPN instance. This setting determines where the device should forward received IPsec packets after it de-encapsulates them. If you specify an inside VPN instance, the device looks for a route in the specified VPN instance to forward the packets. If you do not specify an inside VPN instance, the internal and external networks are in the same VPN instance. The device looks for a route in this VPN instance to forward the packets.
11. Configure the NAT keepalive interval.

    Configure this task when the device is behind a NAT gateway. The device sends NAT keepalive packets regularly to its peer to prevent the NAT session from being aged because of no matching traffic.
12. Enable the configuration exchange feature.

    The configuration exchange feature enables the local and remote ends to exchange configuration data, such as gateway address, internal IP address, and route. The exchange includes data request and response, and data push and response.

    This feature typically applies to scenarios where branches and the headquarters communicate through virtual tunnels.

    This feature enables the IPsec gateway at a branch to send IP address requests to the IPsec gateway at the headquarters. When the headquarters receives the request, it sends an IP address to the branch in the response packet. The headquarters can also actively push an IP address to the branch. The branch uses the allocated IP address as the IP address of the virtual tunnel to communicate with the headquarters.

To configure an IKEv2 profile:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create an IKEv2 profile and enter IKEv2 profile view.	**ikev2 profile** *profile-name*	By default, no IKEv2 profiles exist.
3. Configure the local and remote identity authentication methods.	**authentication-method** { **local** | **remote** } { **dsa-signature** | **ecdsa-signature** | **pre-share** | **rsa-signature** }	By default, no local or remote identity authentication method is configured.
4. Specify a keychain.	**keychain** *keychain-name*	By default, no keychain is specified for an IKEv2 profile. Perform this task when the pre-shared key authentication method is specified.
5. Specify a PKI domain.	**certificate domain** *domain-name* [**sign** | **verify**]	By default, the device uses PKI domains configured in system view. Perform this task when the digital signature authentication method is specified.
6. Configure the local ID.	**identity local** { **address**	By default, no local ID is configured,

Step	Command	Remarks
	{ *ipv4-address* | **ipv6** *ipv6-address* } | **dn** | **email** *email-string* | **fqdn** *fqdn-name* | **key-id** *key-id-string* }	and the device uses the IP address of the interface where the IPsec policy applies as the local ID.
7. Configure peer IDs.	**match remote** { **certificate** *policy-name* | **identity** { **address** { { *ipv4-address* [*mask* | *mask-length*] | **range** *low-ipv4-address* *high-ipv4-address* } | **ipv6** { *ipv6-address* [*prefix-length*] | **range** *low-ipv6-address* *high-ipv6-address* } } | **fqdn** *fqdn-name* | **email** *email-string* | **key-id** *key-id-string* } }	By default, no peer ID is configured. You must configure a minimum of one peer ID on each of the two peers.
8. (Optional.) Specify the local interface or IP address to which the IKEv2 profile can be applied.	**match local address** { *interface-type interface-number* | *ipv4-address* | **ipv6** *ipv6-address* }	By default, an IKEv2 profile can be applied to any local interface or IP address.
9. (Optional.) Specify a priority for the IKEv2 profile.	**priority** *priority*	By default, the priority of an IKEv2 profile is 100.
10. (Optional.) Specify a VPN instance for the IKEv2 profile.	**match vrf** { **name** *vrf-name* | **any** }	By default, an IKEv2 profile belongs to the public network.
11. (Optional.) Set the IKEv2 SA lifetime for the IKEv2 profile.	**sa duration** *seconds*	By default, the IKEv2 SA lifetime is 86400 seconds.
12. (Optional.) Configure the DPD feature for the IKEv2 profile.	**dpd interval** *interval* [**retry** *seconds*] { **on-demand** | **periodic** }	By default, DPD is disabled for an IKEv2 profile. The global DPD settings in system view are used. If DPD is also disabled in system view, the device does not perform DPD.
13. (Optional.) Specify an inside VPN instance for the IKEv2 profile.	**inside-vrf** *vrf-name*	By default, no inside VPN instance is specified for an IKEv2 profile. The internal and external networks are in the same VPN instance. The device forwards protected data to this VPN instance.
14. (Optional.) Set the IKEv2 NAT keepalive interval.	**nat-keepalive** *seconds*	By default, the global IKEv2 NAT keepalive setting is used.
15. (Optional.) Enable the configuration exchange feature.	**config-exchange** { **request** | **set** { **accept** | **send** } }	By default, all configuration exchange options are disabled.

Configuring an IKEv2 policy

During the IKE_SA_INIT exchange, each end tries to find a matching IKEv2 policy, using the IP address of the local security gateway as the matching criterion.

- If IKEv2 policies are configured, IKEv2 searches for an IKEv2 policy that uses the IP address of the local security gateway. If no IKEv2 policy uses the IP address or the policy is using an incomplete proposal, the IKE_SA_INIT exchange fails.
- If no IKEv2 policy is configured, IKEv2 uses the system default IKEv2 policy **default**.

The device matches IKEv2 policies in the descending order of their priorities. To determine the priority of an IKEv2 policy:

1. First, the device examines the existence of the **match local address** command. An IKEv2 policy with the **match local address** command configured has a higher priority.
2. If a tie exists, the device compares the priority numbers. An IKEv2 policy with a smaller priority number has a higher priority.
3. If a tie still exists, the device prefers an IKEv2 policy configured earlier.

To configure an IKEv2 policy:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create an IKEv2 policy and enter IKEv2 policy view.	**ikev2 policy** *policy-name*	By default, an IKEv2 policy named **default** exists.
3. Specify the local interface or address used for IKEv2 policy matching.	**match local address** { *interface-type interface-number* | *ipv4-address* | **ipv6** *ipv6-address* }	By default, no local interface or address is used for IKEv2 policy matching, and the policy matches any local interface or address.
4. Specify a VPN instance for IKEv2 policy matching.	**match vrf** { **name** *vrf-name* | **any** }	By default, no VPN instance is specified for IKEv2 policy matching. The IKEv2 policy matches all local addresses in the public network.
5. Specify an IKEv2 proposal for the IKEv2 policy.	**proposal** *proposal-name*	By default, no IKEv2 proposal is specified for an IKEv2 policy.
6. Specify a priority for the IKEv2 policy.	**priority** *priority*	By default, the priority of an IKEv2 policy is 100.

Configuring an IKEv2 proposal

An IKEv2 proposal contains security parameters used in IKE_SA_INIT exchanges, including the encryption algorithms, integrity protection algorithms, PRF algorithms, and DH groups. An algorithm specified earlier has a higher priority.

A complete IKEv2 proposal must have at least one set of security parameters, including one encryption algorithm, one integrity protection algorithm, one PRF algorithm, and one DH group.

You can specify multiple IKEv2 proposals for an IKEv2 policy. A proposal specified earlier has a higher priority.

To configure an IKEv2 proposal:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create an IKEv2 proposal and enter IKEv2 proposal view.	**ikev2 proposal** *proposal-name*	By default, an IKEv2 proposal named **default** exists. In non-FIPS mode, the default proposal uses the following settings: • Encryption algorithms AES-CBC-128 and 3DES. • Integrity protection algorithms HMAC-SHA1 and HMAC-MD5.

Step	Command	Remarks
		• PRF algorithms HMAC-SHA1 and HMAC-MD5. • DH groups 2 and 5. In FIPS mode, the default proposal uses the following settings: • Encryption algorithms AES-CBC-128 and AES-CTR-128. • Integrity protection algorithms HMAC-SHA1 and HMAC-SHA256. • PRF algorithms HMAC-SHA1 and HMAC-SHA256. • DH groups 14 and 19.
3. Specify the encryption algorithms.	In non-FIPS mode: **encryption** { **3des-cbc** | **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** | **aes-ctr-128** | **aes-ctr-192** | **aes-ctr-256** | **camellia-cbc-128** | **camellia-cbc-192** | **camellia-cbc-256** | **des-cbc** } * In FIPS mode: **encryption** { **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** | **aes-ctr-128** | **aes-ctr-192** | **aes-ctr-256** } *	By default, an IKEv2 proposal does not have any encryption algorithms.
4. Specify the integrity protection algorithms.	In non-FIPS mode: **integrity** { **aes-xcbc-mac** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** } * In FIPS mode: **integrity** { **sha1** | **sha256** | **sha384** | **sha512** } *	By default, an IKEv2 proposal does not have any integrity protection algorithms.
5. Specify the PRF algorithms.	In non-FIPS mode: **prf** { **aes-xcbc-mac** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** } * In FIPS mode: **prf** { **sha1** | **sha256** | **sha384** | **sha512** } *	By default, an IKEv2 proposal uses the integrity protection algorithms as the PRF algorithms.
6. Specify the DH groups.	In non-FIPS mode: **dh** { **group1** | **group14** | **group2** | **group24** | **group5** | **group19** | **group20** } * In FIPS mode: **dh** { **group14** | **group24** | **group19** | **group20** } *	By default, an IKEv2 proposal does not have any DH groups.

Configuring an IKEv2 keychain

An IKEv2 keychain specifies the pre-shared keys used for IKEv2 negotiation.

An IKEv2 keychain can have multiple IKEv2 peers. Each peer has a symmetric pre-shared key or an asymmetric pre-shared key pair, and information for identifying the peer (such as the peer's host name, IP address or address range, or ID).

An IKEv2 negotiation initiator uses the peer host name or IP address/address range as the matching criterion to search for a peer. A responder uses the peer host IP address/address range or ID as the matching criterion to search for a peer.

To configure an IKEv2 keychain:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create an IKEv2 keychain and enter IKEv2 keychain view.	**ikev2 keychain** *keychain-name*	By default, no IKEv2 keychains exist.
3. Create an IKEv2 peer and enter IKEv2 peer view.	**peer** *name*	By default, no IKEv2 peers exist.
4. Configure the information for identifying the IKEv2 peer.	• To configure a host name for the peer: **hostname** *host-name* • To configure a host IP address or address range for the peer: **address** { *ipv4-address* [*mask* | *mask-length*] | **ipv6** *ipv6-address* [*prefix-length*] } • To configure an ID for the peer: **identity** { **address** { *ipv4-address* | **ipv6** { *ipv6-address* } } | **fqdn** *fqdn-name* | **email** *email-string* | **key-id** *key-id-string* }	By default, no hostname, host IP address, address range, or identity information is configured for an IKEv2 peer. You must configure different IP addresses/address ranges for different peers.
5. Configure a pre-shared key for the peer.	**pre-shared-key** [**local** | **remote**] { **ciphertext** | **plaintext** } *string*	By default, an IKEv2 peer does not have a pre-shared key.

Configure global IKEv2 parameters

Enabling the cookie challenging feature

Enable cookie challenging on responders to protect them against DoS attacks that use a large number of source IP addresses to forge IKE_SA_INIT requests.

To enable cookie challenging:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable cookie challenging.	**ikev2 cookie-challenge** *number*	By default, IKEv2 cookie challenging is disabled.

Configuring the IKEv2 DPD feature

IKEv2 DPD detects dead IKEv2 peers in periodic or on-demand mode.

- **Periodic DPD**—Verifies the liveness of an IKEv2 peer by sending DPD messages at regular intervals.
- **On-demand DPD**—Verifies the liveness of an IKEv2 peer by sending DPD messages before sending data.
    - Before the device sends data, it identifies the time interval for which the last IPsec packet has been received from the peer. If the time interval exceeds the DPD interval, it sends a DPD message to the peer to detect its liveliness.
    - If the device has no data to send, it never sends DPD messages.

If you configure IKEv2 DPD in both IKEv2 profile view and system view, the IKEv2 DPD settings in IKEv2 profile view apply. If you do not configure IKEv2 DPD in IKEv2 profile view, the IKEv2 DPD settings in system view apply.

To configure global IKEv2 DPD:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure global IKEv2 DPD.	**ikev2 dpd interval** *interval* [**retry** *seconds*] { **on-demand** | **periodic** }	By default, global DPD is disabled.

Configuring the IKEv2 NAT keepalive feature

Configure this feature on the IKEv2 gateway behind the NAT device. The gateway then sends NAT keepalive packets regularly to its peer to keep the NAT session alive, so that the peer can access the device.

The NAT keepalive interval must be shorter than the NAT session lifetime.

This feature takes effect after the device detects the NAT device.

To configure the IKEv2 NAT keepalive feature:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the IKEv2 NAT keepalive interval.	**ikev2 nat-keepalive** *seconds*	By default, the IKEv2 NAT keepalive interval is 10 seconds.

Displaying and maintaining IKEv2

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display the IKEv2 proposal configuration.	**display ikev2 proposal** [*name* | **default**]
Display the IKEv2 policy configuration.	**display ikev2 policy** [*policy-name* | **default**]
Display the IKEv2 profile configuration.	**display ikev2 profile** [*profile-name*]
Display the IKEv2 SA information.	**display ikev2 sa** [**count** | [{ **local** | **remote** } { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance**

Task	Command
	vpn-instance-name]] [**verbose** [**tunnel** *tunnel-id*]]]
Display IKEv2 statistics.	**display ikev2 statistics**
Delete IKEv2 SAs and the child SAs negotiated through the IKEv2 SAs.	**reset ikev2 sa** [[{ **local** | **remote** } { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]] | **tunnel** *tunnel-id*] [**fast**]
Clear IKEv2 statistics.	**reset ikev2 statistics**

Command reference

New command: address

Use **address** to specify the IP address or IP address range of an IKEv2 peer.

Use **undo address** to restore the default.

Syntax

address { *ipv4-address* [*mask* **|** *mask-length*] **| ipv6** *ipv6-address* [*prefix-length*] }

undo address

Default

An IKEv2 peer's IP address or IP address range is not specified.

Views

IKEv2 peer view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies the IPv4 address of the IKEv2 peer.

mask: Specifies the subnet mask of the IPv4 address.

mask-length: Specifies the subnet mask length of the IPv4 address, in the range of 0 to 32.

ipv6 *ipv6-address*: Specifies the IPv6 address of the IKEv2 peer.

prefix-length: Specifies the prefix length of the IPv6 address, in the range of 0 to 128.

Usage guidelines

Both the initiator and the responder can look up an IKEv2 peer by IP address in IKEv2 negotiation.

The IP addresses of different IKEv2 peers in the same IKEv2 keychain cannot be the same.

Examples

Create an IKEv2 keychain named **key1**.

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
```

Create an IKEv2 peer named **peer1**.

```
[Sysname-ikev2-keychain-key1] peer peer1
```

Specify the IKEv2 peer's IP address 3.3.3.3 with the subnet mask 255.255.255.0.

```
[Sysname-ikev2-keychain-key1-peer-peer1] address 3.3.3.3 255.255.255.0
```

Related commands

- **ikev2 keychain**
- **peer**

New command: authentication-method

Use **authentication-method** to specify the local or remote identity authentication method.

Use **undo authentication-method** to remove the local or remote identity authentication method.

Syntax

authentication-method { **local** | **remote** } { **dsa-signature** | **ecdsa-signature** | **pre-share** | **rsa-signature** }

undo authentication-method local

undo authentication-method remote { **dsa-signature** | **ecdsa-signature** | **pre-share** | **rsa-signature** }

Default

No local or remote identity authentication method is specified.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

local: Specifies the local identity authentication method.

remote: Specifies the remote identity authentication method.

dsa-signature: Specifies the DSA signatures as the identity authentication method.

ecdsa-signature: Specifies the ECDSA signatures as the identity authentication method.

pre-share: Specifies the pre-shared key as the identity authentication method.

rsa-signature: Specifies the RSA signatures as the identity authentication method.

Usage guidelines

The local and remote identity authentication methods must both be specified and they can be different.

You can specify only one local identity authentication method. You can specify multiple remote identity authentication methods by executing this command multiple times when there are multiple remote ends whose authentication methods are unknown.

If you use RSA, DSA, or ECDSA signature authentication, you must specify PKI domains for obtaining certificates. You can specify PKI domains by using the **certificate domain** command in IKEv2 profile view. If you do not specify PKI domains in IKEv2 profile view, the PKI domains configured by the **pki domain** command in system view will be used.

If you specify the pre-shared key method, you must specify a pre-shared key for the IKEv2 peer in the keychain used by the IKEv2 profile.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Specify the pre-shared key and RSA signatures as the local and remote authentication methods, respectively.

```
[Sysname-ikev2-profile-profile1] authentication local pre-share
[Sysname-ikev2-profile-profile1] authentication remote rsa-signature
```

Specify the PKI domain **genl** as the PKI domain for obtaining certificates.

```
[Sysname-ikev2-profile-profile1] certificate domain genl
```

Specify the keychain **keychain1**.

```
[Sysname-ikev2-profile-profile1] keychain keychain1
```

Related commands

- **display ikev2 profile**
- **certificate domain** (IKEv2 profile view)
- **keychain** (IKEv2 profile view)

New command: certificate domain

Use **certificate domain** to specify a PKI domain for signature authentication in IKEv2 negotiation.

Use **undo certificate domain** to remove a PKI domain for signature authentication in IKEv2 negotiation.

Syntax

certificate domain *domain-name* [**sign** | **verify**]

undo certificate domain *domain-name*

Default

PKI domains configured in system view are used.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters.

sign: Uses the local certificate in the PKI domain to generate a signature.

verify: Uses the CA certificate in the PKI domain to verify the remote end's certificate.

Usage guidelines

If you do not specify the **sign** or **verify** keyword, the PKI domain is used for both **sign** and **verify** purposes. You can specify a PKI domain for each purpose by executing this command multiple times. If you specify the same PKI domain for both purposes, the later configuration takes effect. For example, if you execute **certificate domain abc sign** and **certificate domain abc verify** successively, the PKI domain **abc** will be used only for verification.

If the local end uses RSA, DSA, or ECDSA signature authentication, you must specify a PKI domain for signature generation. If the remote end uses RSA, DSA, or ECDSA signature authentication, you must specify a PKI domain for verifying the remote end's certificate. If you do not specify PKI domains, the PKI domains configured in system view will be used.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
```

```
[Sysname] ikev2 profile profile1
```

Specify the PKI domain **abc** for signature. Specify the PKI domain **def** for verification.

```
[Sysname-ikev2-profile-profile1] certificate domain abc sign
[Sysname-ikev2-profile-profile1] certificate domain def verify
```

Related commands

- **authentication-method**
- **pki domain**

New command: config-exchange

Use **config-exchange** to enable the configuration exchange feature.

Use **undo config-exchange** to disable the configuration exchange feature.

Syntax

config-exchange { **request** | **set** { **accept** | **send** } }

undo config-exchange { **request** | **set** { **accept** | **send** } }

Default

Configuration exchange is disabled.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

request: Enables the device to send request messages carrying the configuration request payload during the IKE_AUTH exchange.

set: Specifies the configuration set payload exchange.

accept: Enables the device to accept the configuration set payload carried in Info messages.

send: Enables the device to send Info messages carrying the configuration set payload.

Usage guidelines

The configuration exchange feature enables the local and remote ends to exchange configuration data, such as gateway address, internal IP address, and route. The exchange includes data request and response, and data push and response. The enterprise center can push IP addresses to branches. The branches can request IP addresses, but the requested IP addresses cannot be used.

You can specify both **request** and **set** for the device.

If you specify **request** for the local end, the remote end will respond if it can obtain the requested data through AAA authorization.

If you specify **set send** for the local end, you must specify **set accept** for the remote end.

The device with **set send** specified pushes an IP address after the IKEv2 SA is set up if it does not receive any configuration request from the peer.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Enable the local end to add the configuration request payload to the request message of IKE_AUTH exchange.

```
[Sysname-ikev2-profile-profile1] config-exchange request
```

Related commands

- **aaa authorization**
- **configuration policy**
- **display ikev2 profile**

New command: description

Use **description** to configure a description for an IKE proposal.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

An IKE proposal does not have a description.

Views

IKE proposal view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 80 characters.

Usage guidelines

If multiple IKE proposals exist, you can use this command to configure different descriptions for them to distinguish them.

Examples

Configure the description **test** for the IKE proposal 1.

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1] description test
```

New command: display ike statistics

Use **display ike statistics** to display IKE statistics.

Syntax

display ike statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display IKE statistics.

```
<Sysname> display ike statistics
IKE statistics:
  No matching proposal: 0
  Invalid ID information: 0
  Unavailable certificate: 0
  Unsupported DOI: 0
  Unsupported situation: 0
  Invalid proposal syntax: 0
  Invalid SPI: 0
  Invalid protocol ID: 0
  Invalid certificate: 0
  Authentication failure: 0
  Invalid flags: 0
  Invalid message id: 0
  Invalid cookie: 0
  Invalid transform ID: 0
  Malformed payload: 0
  Invalid key information: 0
  Invalid hash information: 0
  Unsupported attribute: 0
  Unsupported certificate type: 0
  Invalid certificate authority: 0
  Invalid signature: 0
  Unsupported exchange type: 0
  No available SA: 0
  Retransmit timeout: 0
  Not enough memory: 0
  Enqueue fails: 0
```

New command: display ikev2 policy

Use **display ikev2 policy** to display the IKEv2 policy configuration.

Syntax

display ikev2 policy [*policy-name* | **default**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

policy-name: Specifies an IKEv2 policy by its name, a case-insensitive string of 1 to 63 characters.

default: Specifies the default IKEv2 policy.

Usage guidelines

If you do not specify any parameters, this command displays the configuration of all IKEv2 policies.

Examples

Display the configuration of all IKEv2 policies.

```
<Sysname> display ikev2 policy
IKEv2 policy: 1
  Priority: 100
  Match local address: 1.1.1.1
  Match local address ipv6: 1:1::1:1
  Match VRF: vpn1
  Proposal: 1
  Proposal: 2
IKEv2 policy: default
  Match local address: Any
  Match VRF: Any
  Proposal: default
```

Table 11 Command output

Field	Description
IKEv2 policy	Name of the IKEv2 policy.
Priority	Priority of the IKEv2 policy.
Match local address	IPv4 address to which the IKEv2 policy can be applied.
Match local address ipv6	IPv6 address to which the IKEv2 policy can be applied.
Match VRF	VPN instance to which the IKEv2 policy can be applied.
Proposal	IKEv2 proposal that the IKEv2 policy uses.

Related commands

ikev2 policy

New command: display ikev2 profile

Use **display ikev2 profile** to display the IKEv2 profile configuration.

Syntax

display ikev2 profile [*profile-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

profile-name: Specifies an IKEv2 profile by its name, a case-insensitive string of 1 to 63 characters. If you do not specify an IKEv2 profile, this command displays the configuration of all IKEv2 profiles.

Examples

Display the configuration of all IKEv2 profiles.

```
<Sysname> display ikev2 profile
IKEv2 profile: 1
  Priority: 100
  Match criteria:
    Local address 1.1.1.1
    Local address 1:1::1:1
    Remote identity address 3.3.3.3/32
    VRF vrf1
  Local identity: address 1.1.1.1
  Local authentication method: pre-share
  Remote authentication methods: pre-share
  Keychain: Keychain1
  Sign certificate domain:
     Domain1
     abc
  Verify certificate domain:
     Domain2
     yy
  SA duration: 500 seconds
  DPD: Interval 32 secs, retry-interval 23 secs, periodic
  Config exchange: request, set accept, set send
  NAT keepalive: 10 seconds
  Inside VRF: vrf1
  AAA authorization: Domain domain1, username ikev2
```

Table 12 Command output

Field	Description
IKEv2 profile	Name of the IKEv2 profile.
Priority	Priority of the IKEv2 profile.
Match criteria	Criteria for looking up the IKEv2 profile.
Local identity	ID of the local end.
Local authentication method	Method that the local end uses for authentication.
Remote authentication methods	Methods that the remote end uses for authentication.
Keychain	IKEv2 keychain that the IKEv2 profile uses.
Sign certificate domain	PKI domain used for signature generation.
Verify certificate domain	PKI domain used for verifying the remote end's certificate.
SA duration	Lifetime of the IKEv2 SA.
DPD	DPD settings: • Detection interval in seconds. • Retry interval in seconds. • Detection mode, on demand or periodically. If DPD is disabled, this field displays **Disabled**.
Config exchange	Configuration exchange settings:

Field	Description
	• **request**—The local end sends request messages carrying the configuration request payload during the IKE_AUTH exchange. • **set accept**—The local end accepts the configuration set payload carried in Info messages. • **set send**—The local end sends Info messages carrying the configuration set payload.
NAT keepalive	NAT keepalive interval in seconds.
Inside vrf	Inside VPN instance.
AAA authorization	AAA authorization settings: • ISP domain name. • Username.

Related commands

ikev2 profile

New command: display ikev2 proposal

Use **display ikev2 proposal** to display the IKEv2 proposal configuration.

Syntax

display ikev2 proposal [*name* | **default**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name: Specifies an IKEv2 proposal by its name, a case-insensitive string of 1 to 63 characters.

default: Specifies the default IKEv2 proposal.

Usage guidelines

This command displays IKEv2 proposals in descending order of priorities. If you do not specify any parameters, this command displays the configuration of all IKEv2 proposals.

Examples

Display the configuration of all IKEv2 proposals.

```
<Sysname> display ikev2 proposal
IKEv2 proposal: 1
  Encryption: 3DES-CBC, AES-CBC-128, AES-CTR-192, CAMELLIA-CBC-128
  Integrity: MD5, SHA256, AES-XCBC
  PRF: MD5, SHA256, AES-XCBC
  DH group: MODP1024/Group 2, MODP1536/Group 5

IKEv2 proposal: default
  Encryption: AES-CBC-128, 3DES-CBC
  Integrity: SHA1, MD5
```

```
PRF: SHA1, MD5
DH group: MODP1536/Group 5, MODP1024/Group 2
```

Table 13 Command output

Field	Description
IKEv2 proposal	Name of the IKEv2 proposal.
Encryption	Encryption algorithms that the IKEv2 proposal uses.
Integrity	Integrity protection algorithms that the IKEv2 proposal uses.
PRF	PRF algorithms that the IKEv2 proposal uses.
DH group	DH groups that the IKEv2 proposal uses.

Related commands

ikev2 proposal

New command: display ikev2 sa

Use **display ikev2 sa** to display the IKEv2 SA information.

Syntax

display ikev2 sa [**count** | [{ **local** | **remote** } { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]] [**verbose** [**tunnel** *tunnel-id*]]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

count: Displays the number of IKEv2 SAs.

local: Displays IKEv2 SA information for a local IP address.

remote: Displays IKEv2 SA information for a remote IP address.

ipv4-address: Specifies a local or remote IPv4 address.

ipv6 *ipv6-address*: Specifies a local or remote IPv6 address.

vpn-instance *vpn-instance-name*: Displays information about the IKEv2 SAs in an MPLS L3VPN instance. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays information about IKEv2 SAs for the public network.

verbose: Displays detailed information. If you do not specify this keyword, the command displays the summary information.

tunnel *tunnel-id*: Displays detailed IKEv2 SA information for an IPsec tunnel. The *tunnel-id* argument specifies an IPsec tunnel by its ID in the range of 1 to 2000000000.

Usage guidelines

If you do not specify any parameters, this command displays summary information about all IKEv2 SAs.

Examples

Display summary information about all IKEv2 SAs.

```
<Sysname> display ikev2 sa
    Tunnel ID          Local              Remote             Status
  ---------------------------------------------------------------------
    1                  1.1.1.1/500        1.1.1.2/500        EST
    2                  2.2.2.1/500        2.2.2.2/500        EST
  Status:
  IN-NEGO: Negotiating, EST: Established, DEL: Deleting
```

Display summary IKEv2 SA information for the remote IP address 1.1.1.2.

```
<Sysname> display ikev2 sa remote 1.1.1.2
    Tunnel ID          Local              Remote             Status
  ---------------------------------------------------------------------
    1                  1.1.1.1/500        1.1.1.2/500        EST
  Status:
  IN-NEGO: Negotiating, EST: Established, DEL: Deleting
```

Table 14 Command output

Field	Description
Tunnel ID	ID of the IPsec tunnel to which the IKEv2 SA belongs.
Local	Local IP address of the IKEv2 SA.
Remote	Remote IP address of the IKEv2 SA.
Status	Status of the IKEv2 SA: • **IN-NEGO** (**Negotiating**)—The IKEv2 SA is under negotiation. • **EST** (**Established**)—The IKEv2 SA has been set up. • **DEL** (**Deleting**)—The IKEv2 SA is about to be deleted.

Display detailed information about all IKEv2 SAs.

```
<Sysname> display ikev2 sa verbose
  Tunnel ID: 1
  Local IP/Port: 1.1.1.1/500
  Remote IP/Port: 1.1.1.2/500
  Outside VRF: -
  Inside VRF: -
  Local SPI: 8f8af3dbf5023a00
  Remote SPI: 0131565b9b3155fa

  Local ID type: FQDN
  Local ID: router_a
  Remote ID type: FQDN
  Remote ID: router_b

  Auth sign method: Pre-shared key
  Auth verify method: Pre-shared key
  Integrity algorithm: HMAC_MD5
  PRF algorithm: HMAC_MD5
```

```
  Encryption algorithm: AES-CBC-192

  Life duration: 86400 secs
  Remaining key duration: 85604 secs
  Diffie-Hellman group: MODP1024/Group2
  NAT traversal: Not detected
  DPD: Interval 20 secs, retry interval 2 secs
  Transmitting entity: Initiator

  Local window: 1
  Remote window: 1
  Local request message ID: 2
  Remote request message ID:2
  Local next message ID: 0
  Remote next message ID: 0

  Pushed IP address: 192.168.1.5
  Assigned IP address: 192.168.2.24
```

Display detailed IKEv2 SA information for the remote IP address 1.1.1.2.

```
<Sysname> display ikev2 sa remote 1.1.1.2 verbose
  Tunnel ID: 1
  Local IP/Port: 1.1.1.1/500
  Remote IP/Port: 1.1.1.2/500
  Outside VRF: -
  Inside VRF: -
  Local SPI: 8f8af3dbf5023a00
  Remote SPI: 0131565b9b3155fa

  Local ID type: FQDN
  Local ID: router_a
  Remote ID type: FQDN
  Remote ID: router_b

  Auth sign method: Pre-shared key
  Auth verify method: Pre-shared key
  Integrity algorithm: HMAC_MD5
  PRF algorithm: HMAC_MD5
  Encryption algorithm: AES-CBC-192

  Life duration: 86400 secs
  Remaining key duration: 85604 secs
  Diffie-Hellman group: MODP1024/Group2
  NAT traversal: Not detected
  DPD: Interval 30 secs, retry 10 secs
  Transmitting entity: Initiator

  Local window: 1
```

```
Remote window: 1
Local request message ID: 2
Remote request message ID: 2
Local next message ID: 0
Remote next message ID: 0

Pushed IP address: 192.168.1.5
Assigned IP address: 192.168.2.24
```

Table 15 Command output

Field	Description
Tunnel ID	ID of the IPsec tunnel to which the IKEv2 SA belongs.
Local IP/Port	IP address and port number of the local security gateway.
Remote IP/Port	IP address and port number of the remote security gateway.
Outside VRF	Name of the VPN instance to which the protected outbound data flow belongs. If the protected outbound data flow belongs to the public network, this field displays a hyphen (**-**).
Inside VRF	Name of the VPN instance to which the protected inbound data flow belongs. If the protected inbound data flow belongs to the public network, this field displays a hyphen (**-**).
Local SPI	SPI that the local end uses.
Remote SPI	SPI that the remote end uses.
Local ID type	ID type of the local security gateway.
Local ID	ID of the local security gateway.
Remote ID type	ID type of the remote security gateway.
Remote ID	ID of the remote security gateway.
Auth sign method	Signature method that the IKEv2 proposal uses in authentication.
Auth verify method	Verification method that the IKEv2 proposal uses in authentication.
Integrity algorithm	Integrity protection algorithms that the IKEv2 proposal uses.
PRF algorithm	PRF algorithms that the IKEv2 proposal uses.
Encryption algorithm	Encryption algorithms that the IKEv2 proposal uses.
Life duration	Lifetime of the IKEv2 SA, in seconds.
Remaining key duration	Remaining lifetime of the IKEv2 SA, in seconds.
Diffie-Hellman group	DH groups used in IKEv2 key negotiation.
NAT traversal	Whether a NAT gateway is detected between the local and remote ends.
DPD	DPD settings: • Detection interval in seconds. • Retry interval in seconds. If DPD is disabled, this field displays **Disabled**.

Field	Description
Transmitting entity	Role of the local end in IKEv2 negotiation, initiator or responder.
Local window	Window size that the local end uses.
Remote window	Window size that the remote end uses.
Local request message ID	ID of the request message that the local end is about to send.
Remote request message ID	ID of the request message that the remote end is about to send.
Local next message ID	ID of the message that the local end expects to receive.
Remote next message ID	ID of the message that the remote end expects to receive.
Pushed IP address	IP address pushed to the local end by the remote end.
Assigned IP address	IP address assigned to the remote end by the local end .

New command: display ikev2 statistics

Use **display ikev2 statistics** to display IKEv2 statistics.

Syntax

display ikev2 statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display IKEv2 statistics.

```
<Sysname> display ikev2 statistics
IKEv2 statistics:
  Unsupported critical payload: 0
  Invalid IKE SPI: 0
  Invalid major version: 0
  Invalid syntax: 0
  Invalid message ID: 0
  Invalid SPI: 0
  No proposal chosen: 0
  Invalid KE payload: 0
  Authentication failed: 0
  Single pair required: 0
  TS unacceptable: 0
  Invalid selectors: 0
  Temporary failure: 0
  No child SA: 0
  Unknown other notify: 0
  No enough resource: 0
```

```
Enqueue error: 0
No IKEv2 SA: 0
Packet error: 0
Other error: 0
Retransmit timeout: 0
DPD detect error: 0
Del child for IPsec message: 0
Del child for deleting IKEv2 SA: 0
Del child for receiving delete message: 0
```

New command: dh

Use **dh** to specify DH groups to be used in IKEv2 key negotiation.

Use **undo group** to restore the default.

Syntax

In non-FIPS mode:

dh { **group1** | **group14** | **group2** | **group24** | **group5** | **group19** | **group20** } *

undo dh

In FIPS mode:

dh { **group14** | **group24** | **group19** | **group20** } *

undo dh

Default

No DH group is specified for an IKEv2 proposal.

Views

IKEv2 proposal view

Predefined user roles

network-admin

Parameters

group1: Uses the 768-bit Diffie-Hellman group.

group2: Uses the 1024-bit Diffie-Hellman group.

group5: Uses the 1536-bit Diffie-Hellman group.

group14: Uses the 2048-bit Diffie-Hellman group.

group24: Uses the 2048-bit Diffie-Hellman group with the 256-bit prime order subgroup.

group19: Uses the 256-bit ECP Diffie-Hellman group.

group20: Uses the 384-bit ECP Diffie-Hellman group.

Usage guidelines

A DH group with a higher group number provides higher security but needs more time for processing. To achieve the best trade-off between processing performance and security, choose proper DH groups for your network.

You must specify a minimum of one DH group for an IKEv2 proposal. Otherwise, the proposal is incomplete and useless.

You can specify multiple DH groups for an IKEv2 proposal. A group specified earlier has a higher priority.

Examples

Specify DH groups 1 for the IKEv2 proposal 1.

```
<Sysname> system-view
[Sysname] ikev2 proposal 1
[Sysname-ikev2-proposal-1] dh group1
```

Related commands

ikev2 proposal

New command: dpd

Use **dpd** to configure the IKEv2 DPD feature.

Use **undo dpd** to disable the IKEv2 DPD feature.

Syntax

dpd interval *interval* [**retry** *seconds*] { **on-demand** | **periodic** }

undo dpd interval

Default

IKEv2 DPD is disabled. The global IKEv2 DPD settings are used.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies a DPD triggering interval in the range of 10 to 3600 seconds.

retry *seconds*: Specifies the DPD retry interval in the range of 2 to 60 seconds. The default is 5 seconds.

on-demand: Triggers DPD on demand. The device triggers DPD if it has IPsec traffic to send and has not received any IPsec packets from the peer for the specified interval.

periodic: Triggers DPD at regular intervals. The device triggers DPD at the specified interval.

Usage guidelines

DPD is triggered periodically or on-demand. The on-demand mode is recommended when the device communicates with a large number of IKEv2 peers. For an earlier detection of dead peers, use the periodic triggering mode, which consumes more bandwidth and CPU.

The triggering interval must be longer than the retry interval, so that the device will not trigger a new round of DPD during a DPD retry.

Examples

Configure on-demand IKEv2 DPD. Set the DPD triggering interval to 10 seconds and the retry interval to 5 seconds.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
[Sysname-ikev2-profile-profile1] dpd interval 10 retry 5 on-demand
```

Related commands

ikev2 dpd

New command: encryption

Use **encryption** to specify encryption algorithms for an IKEv2 proposal.

Use **undo encryption** to restore the default.

Syntax

In non-FIPS mode:

encryption { **3des-cbc** | **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** | **aes-ctr-128** | **aes-ctr-192** | **aes-ctr-256** | **camellia-cbc-128** | **camellia-cbc-192** | **camellia-cbc-256** | **des-cbc** } *

undo encryption

In FIPS mode:

encryption { **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** | **aes-ctr-128** | **aes-ctr-192** | **aes-ctr-256** } *

undo encryption

Default

No encryption algorithm is specified for an IKEv2 proposal.

Views

IKEv2 proposal view

Predefined user roles

network-admin

Parameters

3des-cbc: Specifies the 3DES algorithm in CBC mode, which uses a 168-bit key.

aes-cbc-128: Specifies the AES algorithm in CBC mode, which uses a 128-bit key.

aes-cbc-192: Specifies the AES algorithm in CBC mode, which uses a 192-bit key.

aes-cbc-256: Specifies the AES algorithm in CBC mode, which uses a 256-bit key.

aes-ctr-128: Specifies the AES algorithm in CTR mode, which uses a 128-bit key.

aes-ctr-192: Specifies the AES algorithm in CTR mode, which uses a 192-bit key.

aes-ctr-256: Specifies the AES algorithm in CTR mode, which uses a 256-bit key.

camellia-cbc-128: Specifies the Camellia algorithm in CBC mode, which uses a 128-bit key.

camellia-cbc-192: Specifies the Camellia algorithm in CBC mode, which uses a 192-bit key.

camellia-cbc-256: Specifies the Camellia algorithm in CBC mode, which uses a 256-bit key.

des-cbc: Specifies the DES algorithm in CBC mode, which uses a 56-bit key.

Usage guidelines

You must specify a minimum of one encryption algorithm for an IKEv2 proposal. Otherwise, the proposal is incomplete and useless. You can specify multiple encryption algorithms for an IKEv2 proposal. An algorithm specified earlier has a higher priority.

Examples

Specify the 168-bit 3DES algorithm in CBC mode as the encryption algorithm for the IKE proposal **prop1**.

```
<Sysname> system-view
```

```
[Sysname] ikev2 proposal prop1
[Sysname-ikev2-proposal-prop1] encryption 3des-cbc
```

Related commands

ikev2 proposal

New command: hostname

Use **hostname** to specify the host name of an IKEv2 peer.

Use **undo hostname** to restore the default.

Syntax

hostname *name*

undo hostname

Default

An IKEv2 peer's host name is not specified.

Views

IKEv2 peer view

Predefined user roles

network-admin

Parameters

name: Specifies the host name of the IKEv2 peer, a case-insensitive string of 1 to 253 characters.

Usage guidelines

Only the initiator can look up an IKEv2 peer by host name in IKEv2 negotiation, and the initiator must use an IPsec policy rather than an IPsec profile.

Examples

Create an IKEv2 keychain named **key1**.

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
```

Create an IKEv2 peer named **peer1**.

```
[Sysname-ikev2-keychain-key1] peer peer1
```

Specify the host name **test** of the IKEv2 peer.

```
[Sysname-ikev2-keychain-key1-peer-peer1] hostname test
```

Related commands

- **ikev2 keychain**
- **peer**

New command: identity

Use **identity** to specify the ID of an IKEv2 peer.

Use **undo identity** to restore the default.

Syntax

identity { **address** { *ipv4-address* **| ipv6** { *ipv6-address* } } **| fqdn** *fqdn-name* **| email** *email-string* **| key-id** *key-id-string* }

undo identity

Default

An IKEv2 peer's ID is not specified.

Views

IKEv2 peer view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies the IPv4 address of the peer.

ipv6 *ipv6-address*: Specifies the IPv6 address of the peer.

fqdn *fqdn-name*: Specifies the FQDN of the peer. The *fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as www.test.com.

email *email-string*: Specifies the email address of the peer. The *email-string* argument is a case-sensitive string of 1 to 255 characters in the format defined by RFC 822, such as esec@test.com.

key-id *key-id-string*: Specifies the remote gateway's key ID. The *key-id-string* argument is a case-sensitive string of 1 to 255 characters, and is usually a vendor-specific string for doing proprietary types of identification.

Usage guidelines

Only the responder can look up an IKEv2 peer by ID in IKEv2 negotiation. The initiator does not know the peer ID when initiating the IKEv2 negotiation, so it cannot use an ID for IKEv2 peer lookup.

Examples

Create an IKEv2 keychain named **key1**.

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
```

Create an IKEv2 peer named **peer1**.

```
[Sysname-ikev2-keychain-key1] peer peer1
```

Specify the peer IPv4 address 1.1.1.2 as the ID of the IKEv2 peer.

```
[Sysname-ikev2-keychain-key1-peer-peer1] identity address 1.1.1.2
```

Related commands

- **ikev2 keychain**
- **peer**

New command: identity local

Use **identity local** to configure the local ID, the ID that the device uses to identify itself to the peer during IKEv2 negotiation..

Use **undo identity local** to restore the default.

Syntax

identity local { **address** { *ipv4-address* | **ipv6** *ipv6-address* } **| dn | email** *email-string* **| fqdn** *fqdn-name* **| key-id** *key-id-string* }

undo identity local

Default

No local ID is specified. The IP address of the interface to which the IPsec policy is applied is used as the local ID.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

address { *ipv4-address* **| ipv6** *ipv6-address* }: Uses an IPv4 or IPv6 address as the local ID.

dn: Uses the DN in the local certificate as the local ID.

email *email-string*: Uses an email address as the local ID. The *email-string* argument is a case-sensitive string of 1 to 255 characters in the format defined by RFC 822, such as sec@abc.com.

fqdn *fqdn-name*: Uses an FQDN as the local ID. The *fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as www.test.com.

key-id *key-id-string*: Uses the device's key ID as the local ID. The *key-id-string* argument is a case-sensitive string of 1 to 255 characters, and is usually a vendor-specific string for doing proprietary types of identification.

Usage guidelines

Peers exchange local IDs for identifying each other in negotiation.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Use the IP address 2.2.2.2 as the local ID.

```
[Sysname-ikev2-profile-profile1] identity local address 2.2.2.2
```

Related commands

peer

New command: ikev2 cookie-challenge

Use **ikev2 cookie-challenge** to enable the cookie challenging feature.

Use **undo ikev2 cookie-challenge** to disable the cookie challenging feature.

Syntax

ikev2 cookie-challenge *number*

undo ikev2 cookie-challenge

Default

The cookie challenging feature is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

number: Specifies the threshold for triggering the cookie challenging feature. The value range for this argument is 0 to 1000 half-open IKE SAs.

Usage guidelines

When an IKEv2 responder maintains a threshold number of half-open IKE SAs, it starts the cookie challenging mechanism. The responder generates a cookie and includes it in the response sent to the initiator. If the initiator initiates a new IKE_SA_INIT request that carries the correct cookie, the responder considers the initiator valid and proceeds with the negotiation. If the carried cookie is incorrect, the responder terminates the negotiation.

This feature can protect the responder against DoS attacks which aim to exhaust the responder's system resources by using a large number of IKE_SA_INIT requests with forged source IP addresses.

Examples

Enable the cookie challenging feature and set the threshold to 450.

```
<Sysname> system-view
[Sysname] ikev2 cookie-challenge 450
```

New command: ikev2 dpd

Use **ikev2 dpd** to configure the global IKEv2 DPD feature.

Use **undo ikev2 dpd** to disable the global IKEv2 DPD feature.

Syntax

ikev2 dpd interval *interval* [**retry** *seconds*] { **on-demand** | **periodic** }

undo ikev2 dpd interval

Default

The global IKEv2 DPD feature is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies a DPD triggering interval in the range of 10 to 3600 seconds.

retry *seconds*: Specifies the DPD retry interval in the range of 2 to 60 seconds. The default is 5 seconds.

on-demand: Triggers DPD on demand. The device triggers DPD if it has IPsec traffic to send and has not received any IPsec packets from the peer for the specified interval.

periodic: Triggers DPD at regular intervals. The device triggers DPD at the specified interval.

Usage guidelines

DPD is triggered periodically or on-demand. The on-demand mode is recommended when the device communicates with a large number of IKEv2 peers. For an earlier detection of dead peers, use the periodic triggering mode, which consumes more bandwidth and CPU.

The triggering interval must be longer than the retry interval, so that the device will not trigger a new round of DPD during a DPD retry.

You can configure IKEv2 DPD in both IKEv2 profile view and system view. The IKEv2 DPD settings in IKEv2 profile view apply. If you do not configure IKEv2 DPD in IKEv2 profile view, the IKEv2 DPD settings in system view apply.

Examples

Configure the device to trigger IKEv2 DPD if it has IPsec traffic to send and has not received any IPsec packets from the peer for 15 seconds.

```
<Sysname> system-view
[Sysname] ikev2 dpd interval 15 on-demand
```

Configure the device to trigger IKEv2 DPD every 15 seconds.

```
<Sysname> system-view
[Sysname] ikev2 dpd interval 15 periodic
```

Related commands

dpd (IKEv2 profile view)

New command: ikev2 keychain

Use **ikev2 keychain** to create an IKEv2 keychain and enter its view, or enter the view of an existing IKEv2 keychain.

Use **undo ikev2 keychain** to delete an IKEv2 keychain.

Syntax

ikev2 keychain *keychain-name*

undo ikev2 keychain *keychain-name*

Default

No IKEv2 keychains exist.

Views

System view

Predefined user roles

network-admin

Parameters

keychain-name: Specifies a name for the IKEv2 keychain. The keychain name is a case-insensitive string of 1 to 63 characters and cannot contain a hyphen (-).

Usage guidelines

An IKEv2 keychain is required on both ends if either end uses pre-shared key authentication. The pre-shared key configured on both ends must be the same.

You can configure multiple IKEv2 peers in an IKEv2 keychain.

Examples

Create an IKEv2 keychain named **key1** and enter IKEv2 keychain view.

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
[Sysname-ikev2-keychain-key1]
```

New command: ikev2 nat-keepalive

Use **ikev2 nat-keepalive** to set the NAT keepalive interval.

Use **undo ikev2 nat-keepalive** to restore the default.

Syntax

ikev2 nat-keepalive *seconds*

undo ikev2 nat-keepalive

Default

The NAT keepalive interval is 10 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

seconds: Specifies the NAT keepalive interval in seconds, in the range of 5 to 3600.

Usage guidelines

This command takes effect when the device resides in the private network behind a NAT device. The device must send NAT keepalive packets regularly to its peer to keep the NAT session alive, so that the peer can access the device.

The NAT keepalive interval must be shorter than the NAT session lifetime.

Examples

Set the NAT keepalive interval to 5 seconds.

```
<Sysname> system-view
[Sysname] ikev2 nat-keepalive 5
```

New command: ikev2 policy

Use **ikev2 policy** to create an IKEv2 policy and enter its view, or enter the view of an existing IKEv2 policy.

Use **undo ikev2 policy** to delete an IKEv2 policy.

Syntax

ikev2 policy *policy-name*

undo ikev2 policy *policy-name*

Default

An IKEv2 policy named **default** exists, which uses the default IKEv2 proposal and matches any local addresses.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a name for the IKEv2 policy. The policy name is a case-insensitive string of 1 to 63 characters.

Usage guidelines

Each end must have an IKEv2 policy for the IKE_SA_INIT exchange. The initiator looks up an IKEv2 policy by the IP address of the interface to which the IPsec policy is applied and the VPN instance to which the interface belongs. The responder looks up an IKEv2 policy by the IP address of the interface that receives the IKEv2 packet and the VPN instance to which the interface belongs. An IKEv2 policy uses IKEv2 proposals to define the encryption algorithms, integrity protection algorithms, PRF algorithms, and DH groups to be used for negotiation.

You can configure multiple IKEv2 policies. An IKEv2 policy must have a minimum of one IKEv2 proposal. Otherwise, the policy is incomplete.

If the initiator uses an IPsec policy that is bound to a source interface, the initiator looks up an IKEv2 policy by the IP address of the source interface.

You can set priorities to adjust the match order of IKEv2 policies that have the same match criteria.

If no IKEv2 policy is configured, the default IKEv2 policy is used. You cannot enter the view of the default IKEv2 policy, nor modify it.

Examples

Create an IKEv2 policy named **policy1** and enter IKEv2 policy view.

```
<Sysname> system-view
[Sysname] ikev2 policy policy1
[Sysname-ikev2-policy-policy1]
```

Related commands

display ikev2 policy

New command: ikev2 profile

Use **ikev2 profile** to create an IKEv2 profile and enter its view, or enter the view of an existing IKEv2 profile.

Use **undo ikev2 profile** to delete an IKEv2 profile.

Syntax

ikev2 profile *profile-name*

undo ikev2 profile *profile-name*

Default

No IKEv2 profiles exist.

Views

System view

Predefined user roles

network-admin

Parameters

profile-name: Specifies a name for the IKEv2 profile. The profile name is a case-insensitive string of 1 to 63 characters.

Usage guidelines

An IKEv2 profile contains the IKEv2 SA parameters that are not negotiated, such as the identity information and authentication methods of the peers, and the matching criteria for profile lookup.

Examples

Create an IKEv2 profile named **profile1** and enter IKEv2 profile view.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
[Sysname-ikev2-profile-profile1]
```

Related commands

display ikev2 profile

New command: ikev2 proposal

Use **ikev2 proposal** to create an IKEv2 proposal and enter its view, or enter the view of an existing IKEv2 proposal.

Use **undo ikev2 proposal** to delete an IKEv2 proposal.

Syntax

ikev2 proposal *proposal-name*

undo ikev2 proposal *proposal-name*

Default

An IKEv2 proposal named **default** exists, which has the lowest priority and uses the following settings:

- In non-FIPS mode:
  - **Encryption algorithm**—AES-CBC-128 and 3DES.
  - **Integrity protection algorithm**—HMAC-SHA1 and HMAC-MD5.
  - **PRF algorithm**—HMAC-SHA1 and HMAC-MD5.
  - **DH group**—Group 5 and group 2.
- In FIPS mode:
  - **Encryption algorithm**—AES-CBC-128 and AES-CTR-128.
  - **Integrity protection algorithm**—HMAC-SHA1 and HMAC-SHA256.
  - **PRF algorithm**—HMAC-SHA1 and HMAC-SHA256.
  - **DH group**—Group 14 and group 19.

Views

System view

Predefined user roles

network-admin

Parameters

proposal-name: Specifies a name for the IKEv2 proposal. The proposal name is a case-insensitive string of 1 to 63 characters and cannot be **default**.

Usage guidelines

An IKEv2 proposal contains security parameters used in IKE_SA_INIT exchanges, including the encryption algorithms, integrity protection algorithms, PRF algorithms, and DH groups.

An IKEv2 proposal must have a minimum of one set of security parameters, including one encryption algorithm, one integrity protection algorithm, one PRF algorithm, and one DH group.

In an IKEv2 proposal, you can specify multiple parameters of the same type. The parameters of different types combine and form multiple sets of security parameters. If you want to use only one set of security parameters, configure only one set of security parameters for the IKEv2 proposal.

Examples

Create an IKEv2 proposal named **prop1**. Specify the encryption algorithm AES-CBC-128, integrity protection algorithm SHA1, PRF algorithm SHA1, and DH group 2.

```
<Sysname> system-view
[Sysname] ikev2 proposal prop1
[Sysname-ikev2-proposal-prop1] encryption aes-cbc-128
[Sysname-ikev2-proposal-prop1] authentication sha1
[Sysname-ikev2-proposal-prop1] prf sha1
[Sysname-ikev2-proposal-prop1] dh group2
```

Related commands

- **encryption**
- **integrity**
- **prf**
- **dh**

New command: inside-vrf

Use **inside-vrf** to specify an inside VPN instance.

Use **undo inside-vrf** to restore the default.

Syntax

inside-vrf *vrf-name*

undo inside-vrf

Default

No inside VPN instance is specified. The internal and external networks are in the same VPN instance. The device forwards protected data to this VPN instance.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

vrf-name: Specifies the VPN instance to which the protected data belongs. The *vrf-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

This command determines where the device should forward received IPsec packets after it de-encapsulates them. If you configure this command, the device looks for a route in the specified VPN instance to forward the packets. If you do not configure this command, the internal and external networks are in the same VPN instance. The device looks for a route in this VPN instance to forward the packets.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Specify the inside VPN instance **vpn1**.

```
[Sysname-ikev2-profile-profile1] inside-vrf vpn1
```

New command: integrity

Use **integrity** to specify integrity protection algorithms for an IKEv2 proposal.

Use **undo integrity** to restore the default.

Syntax

In non-FIPS mode:

integrity { **aes-xcbc-mac** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** } *

undo integrity

In FIPS mode:

integrity { **sha1** | **sha256** | **sha384** | **sha512** } *

undo integrity

Default

No integrity protection algorithm is specified for an IKEv2 proposal.

Views

IKEv2 proposal view

Predefined user roles

network-admin

Parameters

aes-xcbc-mac: Uses the HMAC-AES-XCBC-MAC algorithm.

md5: Uses the HMAC-MD5 algorithm.

sha1: Uses the HMAC-SHA1 algorithm.

sha256: Uses the HMAC-SHA256 algorithm.

sha384: Uses the HMAC-SHA384 algorithm.

sha512: Uses the HMAC-SHA512 algorithm.

Usage guidelines

You must specify a minimum of one integrity protection algorithm for an IKEv2 proposal. Otherwise, the proposal is incomplete and useless. You can specify multiple integrity protection algorithms for an IKEv2 proposal. An algorithm specified earlier has a higher priority.

Examples

Create an IKEv2 proposal named **prop1**.

```
<Sysname> system-view
[Sysname] ikev2 proposal prop1
```

Specify HMAC-SHA1 and HMAC-MD5 as the integrity protection algorithms, with HMAC-SHA1 preferred.

```
[Sysname-ikev2-proposal-prop1] integrity sha1 md5
```

Related commands

ikev2 proposal

New command: keychain

Use **keychain** to specify an IKEv2 keychain for pre-shared key authentication.

Use **undo keychain** to restore the default.

Syntax

keychain *keychain-name*

undo keychain

Default

No IKEv2 keychain is specified for an IKEv2 profile.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

keychain-name: Specifies an IKEv2 keychain by its name. The keychain name is a case-insensitive string of 1 to 63 characters and cannot contain a hyphen (-).

Usage guidelines

An IKEv2 keychain is required on both ends if either end uses pre-shared key authentication. You can specify only one IKEv2 keychain for an IKEv2 profile.

You can specify the same IKEv2 keychain for different IKEv2 profiles.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Specify the IKEv2 keychain **keychain1**.

```
[Sysname-ikev2-profile-profile1] keychain keychain1
```

Related commands

- **display ikev2 profile**
- **ikev2 keychain**

New command: match local (IKEv2 profile view)

Use **match local** to specify a local interface or a local IP address to which an IKEv2 profile can be applied.

Use **undo match local** to remove a local interface or a local IP address to which an IKEv2 profile can be applied.

Syntax

match local address { *interface-type interface-number* **|** *ipv4-address* **| ipv6** *ipv6-address* }

undo match local address { *interface-type interface-number* **|** *ipv4-address* **| ipv6** *ipv6-address* }

Default

An IKEv2 profile can be applied to any local interface or IP address.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

address: Specifies a local interface or IP address to which an IKEv2 profile can be applied.

interface-type interface-number: Specifies a local interface by its type and number. It can be any Layer 3 interface.

ipv4-address: Specifies the IPv4 address of a local interface.

ipv6 *ipv6-address*: Specifies the IPv6 address of a local interface.

Usage guidelines

Use this command to specify which address or interface can use the IKEv2 profile for IKEv2 negotiation. The interface is the interface that receives IKEv2 packets. The IP address is the IP address of the interface that receives IKEv2 packets.

An IKEv2 profile configured earlier has a higher priority. To give an IKEv2 profile that is configured later a higher priority, you can configure the **priority** command or this command for the profile. For example, suppose you configured IKEv2 profile A before configuring IKEv2 profile B, and you configured the **match remote identity address range 2.2.2.1 2.2.2.100** command for IKEv2 profile A and the **match remote identity address range 2.2.2.1 2.2.2.10** command for IKEv2 profile B. For the local interface with the IP address 3.3.3.3 to negotiate with the peer 2.2.2.6, IKEv2 profile A is preferred because IKEv2 profile A was configured earlier. To use IKEv2 profile B, you can use this command to restrict the application scope of IKEv2 profile B to IPv4 address 3.3.3.3.

You can specify multiple applicable local interfaces or IP addresses for an IKEv2 profile.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Apply the IKEv2 profile **profile1** to the interface whose IP address is 2.2.2.2.

```
[Sysname-ikev2-profile-profile1] match local address 2.2.2.2
```

Related commands

match remote

New command: match local address (IKEv2 policy view)

Use **match local address** to specify a local interface or a local address that an IKEv2 policy matches.

Use **undo match local address** to remove a local interface or a local address that an IKEv2 policy matches.

Syntax

match local address { *interface-type interface-number* **|** *ipv4-address* **|** **ipv6** *ipv6-address* }

undo match local address { *interface-type interface-number* **|** *ipv4-address* **|** **ipv6** *ipv6-address* }

Default

No local interface or address is specified, and the IKEv2 policy matches any local interface or address.

Views

IKEv2 policy view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies a local interface by its type and number. It can be any Layer 3 interface.

ipv4-address: Specifies the IPv4 address of a local interface.

ipv6 *ipv6-address*: Specifies the IPv6 address of a local interface.

Usage guidelines

IKEv2 policies with this command configured are looked up before those that do not have this command configured.

Examples

Configure the IKEv2 policy **policy1** to match the local address 3.3.3.3.

```
<Sysname> system-view
[Sysname] ikev2 policy policy1
[Sysname-ikev2-policy-policy1] match local address 3.3.3.3
```

Related commands

- **display ikev2 policy**
- **match vrf**

New command: match remote

Use **match remote** to configure a peer ID that an IKEv2 profile matches.

Use **undo match remote** to delete a peer ID that an IKEv2 profile matches.

Syntax

match remote { **certificate** *policy-name* **|** **identity** { **address** { { *ipv4-address* [*mask* **|** *mask-length*] **|** **range** *low-ipv4-address high-ipv4-address* } **|** **ipv6** { *ipv6-address* [*prefix-length*] **|** **range** *low-ipv6-address high-ipv6-address* } } **|** **fqdn** *fqdn-name* **|** **email** *email-string* **|** **key-id** *key-id-string* } }

undo match remote { **certificate** *policy-name* **|** **identity** { **address** { { *ipv4-address* [*mask* **|***mask-length*] **|** **range** *low-ipv4-address high-ipv4-address* } **|** **ipv6** { *ipv6-address* [*prefix-length*] **|** **range** *low-ipv6-address high-ipv6-address* } } **|** **fqdn** *fqdn-name* **|** **email** *email-string* **|** **key-id** *key-id-string* } }

Default

No matching peer ID is configured for an IKEv2 profile.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

certificate *policy-name*: Uses the information in the peer's digital certificate as the peer ID for IKEv2 profile matching. The *policy-name* argument specifies a certificate-based access control policy by its name, a case-insensitive string of 1 to 31 characters.

identity: Uses the specified information as the peer ID for IKEv2 profile matching. The specified information is configured on the peer by using the **identity local** command.

- **address** *ipv4-address* [*mask* | *mask-length*]: Uses an IPv4 host address or an IPv4 subnet address as the peer ID for IKEv2 profile matching. The value range for the *mask-length* argument is 0 to 32.
- **address range** *low-ipv4-address high-ipv4-address*: Uses a range of IPv4 addresses as the peer ID for IKEv2 profile matching. The end address must be higher than the start address.
- **address ipv6** *ipv6-address* [*prefix-length*]: Uses an IPv6 host address or an IPv6 subnet address as the peer ID for IKEv2 profile matching. The value range for the *prefix-length* argument is 0 to 128.
- **address ipv6 range** *low-ipv6-address high-ipv6-address*: Uses a range of IPv6 addresses as the peer ID for IKEv2 profile matching. The end address must be higher than the start address.
- **fqdn** *fqdn-name*: Uses the peer's FQDN as the peer ID for IKEv2 profile matching. The *fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as www.test.com.
- **email** *email-string*: Uses peer's email address as the peer ID for IKEv2 profile matching. The *email-string* argument is a case-sensitive string of 1 to 255 characters in the format defined by RFC 822, such as sec@abc.com.
- **key-id** *key-id-string*: Uses the peer's key ID as the peer ID for IKEv2 profile matching. The *key-id-string* argument is a case-sensitive string of 1 to 255 characters, and is usually a vendor-specific string for doing proprietary types of identification.

Usage guidelines

The device compares the received peer ID with the peer IDs configured in local IKEv2 profiles. If a match is found, it uses the IKEv2 profile with the matching peer ID for IKEv2 negotiation. If you have configured the **match local address** and **match vrf** commands, the IKEv2 profile must also match the specified local interface or address and the specified VPN instance.

To make sure only one IKEv2 profile is matched for a peer, do not configure the same peer ID for two or more IKEv2 profiles. If you configure the same peer ID for two or more IKEv2 profiles, which IKEv2 profile is selected for IKEv2 negotiation is unpredictable.

You can configure an IKEv2 profile to match multiple peer IDs. A peer ID configured earlier has a higher priority.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Configure the IKEv2 profile to match the peer ID that is the FQDN name **www.test.com**.

```
[Sysname-ikev2-profile-profile1] match remote identity fqdn www.test.com
```

Configure the IKEv2 profile to match the peer ID that is the IP address 10.1.1.1.

```
[Sysname-ikev2-profile-profile1]match remote identity address 10.1.1.1
```

Related commands

- **identity local**
- **match local address**
- **match vrf**

New command: match vrf (IKEv2 policy view)

Use **match vrf** to specify a VPN instance that an IKEv2 policy matches.

Use **undo match vrf** to restore the default.

Syntax

match vrf { **name** *vrf-name* | **any** }

undo match vrf

Default

No VPN instance is specified, and the IKEv2 policy matches all local IP addresses in the public network.

Views

IKEv2 policy view

Predefined user roles

network-admin

Parameters

name *vrf-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters.

any: Specifies the public network and all VPN instances.

Usage guidelines

Each end must have an IKEv2 policy for the IKE_SA_INIT exchange. The initiator looks up an IKEv2 policy by the IP address of the interface to which the IPsec policy is applied and the VPN instance to which the interface belongs. The responder looks up an IKEv2 policy by the IP address of the interface that receives the IKEv2 packet and the VPN instance to which the interface belongs.

IKEv2 policies with this command configured are looked up before those that do not have this command configured.

Examples

Create an IKEv2 policy named **policy1**.

```
<Sysname> system-view
[Sysname] ikev2 policy policy1
```

Configure the IKEv2 policy to match the VPN instance **vpn1**.

```
[Sysname-ikev2-policy-policy1] match vrf name vpn1
```

Related commands

- **display ikev2 policy**
- **match local address**

New command: match vrf (IKEv2 profile view)

Use **match vrf** to specify a VPN instance for an IKEv2 profile.

Use **undo match vrf** to restore the default.

Syntax

match vrf { **name** *vrf-name* **|** **any** }

undo match vrf

Default

An IKEv2 profile belongs to the public network.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

name *vrf-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters.

any: Specifies the public network and all VPN instances.

Usage guidelines

If an IKEv2 profile belongs to a VPN instance, only interfaces in the VPN instance can use the IKEv2 profile for IKEv2 negotiation. The VPN instance is the VPN instance to which the interface that receives IKEv2 packets belongs. If you specify the **any** keyword, interfaces in any VPN instance can use the IKEv2 profile for IKEv2 negotiation.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Specify **vrf1** as the VPN instance that the IKEv2 profile belongs to.

```
[Sysname-ikev2-profile-profile1] match vrf name vrf1
```

Related commands

match remote

New command: nat-keepalive

Use **nat-keepalive** to set the NAT keepalive interval.

Use **ikev2 nat-keepalive** to restore the default.

Syntax

nat-keepalive *seconds*

undo nat-keepalive

Default

The NAT keepalive interval set in system view is used.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

seconds: Specifies the NAT keepalive interval in seconds, in the range of 5 to 3600.

Usage guidelines

This command takes effect when the device resides in the private network behind a NAT device. The device must send NAT keepalive packets regularly to its peer to keep the NAT session alive, so that the peer can access the device.

The NAT keepalive interval must be shorter than the NAT session lifetime.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Set the NAT keepalive interval to 1200 seconds.

```
[Sysname-ikev2-profile-profile1]nat-keepalive 1200
```

Related commands

- **display ikev2 profile**
- **ikev2 nat-keepalive**

New command: peer

Use **peer** to create an IKEv2 peer and enter its view, or enter the view of an existing IKEv2 peer.

Use **undo peer** to delete an IKEv2 peer.

Syntax

peer *name*

undo peer *name*

Default

No IKEv2 peers exist.

Views

IKEv2 keychain view

Predefined user roles

network-admin

Parameters

name: Specifies a name for the IKEv2 peer. The peer name is a case-insensitive string of 1 to 63 characters.

Usage guidelines

An IKEv2 peer contains a pre-shared key and the criteria for looking up the peer. The criteria for peer lookup include the peer's host name, IP address, IP address range, and ID. The IKEv2 negotiation initiator uses the peer's host name, IP address, or IP address range to look up its peer. The responder uses the peer's IP address, IP address range, or ID to look up its peer.

Examples

Create an IKEv2 keychain named **key1** and enter IKEv2 keychain view.

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
```

Create an IKEv2 peer named **peer1**.

```
[Sysname-ikev2-keychain-key1] peer peer1
```

Related commands

- **address**
- **hostname**
- **identity**
- **ikev2 keychain**

New command: pre-shared-key

Use **pre-shared-key** to configure a pre-shared key.

Use **undo pre-shared-key** to delete a pre-shared key.

Syntax

pre-shared-key [**local** | **remote**] { **ciphertext** | **plaintext** } *string*

undo pre-shared-key [**local** | **remote**]

Default

No pre-shared key exists.

Views

IKEv2 peer view

Predefined user roles

network-admin

Parameters

local: Specifies a pre-shared key for certificate signing.

remote: Specifies a pre-shared key for certificate authentication.

ciphertext: Specifies a pre-shared key in encrypted form.

plaintext: Specifies a pre-shared key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the pre-shared key. The key is case sensitive. In non-FIPS mode, its plaintext form is a string of 1 to 128 characters and its encrypted form is a string of 1 to 201 characters. In FIPS mode, its plaintext form is a string of 15 to 128 characters and its encrypted form is a string of 15 to 201 characters.

Usage guidelines

If you specify the **local** or **remote** keyword, you configure an asymmetric key. If you specify neither the **local** nor the **remote** keyword, you configure a symmetric key.

To delete a key by using the **undo** command, you must specify the correct key type. For example, if you configure a key by using the **pre-shared-key local** command, you cannot delete the key by using the **undo pre-shared-key** or **undo pre-shared-key remote** command.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

- On the initiator:

  # Create an IKEv2 keychain named **key1**.

  ```
  <Sysname> system-view
  [Sysname] ikev2 keychain key1
  ```

  # Create an IKEv2 peer named **peer1**.

  ```
  [Sysname-ikev2-keychain-key1] peer peer1
  ```

  # Configure the symmetric plaintext pre-shared key **111-key**.

  ```
  [Sysname-ikev2-keychain-key1-peer-peer1] pre-shared-key plaintext 111-key
  [Sysname-ikev2-keychain-key1-peer-peer1] quit
  ```

  # Create an IKEv2 peer named **peer2**.

  ```
  [Sysname-ikev2-keychain-key1] peer peer2
  ```

  # Configure asymmetric plaintext pre-shared keys. The key for certificate signing is **111-key-a** and the key for certificate authentication is **111-key-b**.

  ```
  [Sysname-ikev2-keychain-key1-peer-peer2] pre-shared-key local plaintext 111-key-a
  [Sysname-ikev2-keychain-key1-peer-peer2] pre-shared-key remote plaintext 111-key-b
  ```

- On the responder:

  # Create an IKEv2 keychain named **telecom**.

```
<Sysname> system-view
[Sysname] ikev2 keychain telecom
```

Create an IKEv2 peer named **peer1**.

```
[Sysname-ikev2-keychain-telecom] peer peer1
```

Configure the symmetric plaintext pre-shared key **111-key**.

```
[Sysname-ikev2-keychain-telecom-peer-peer1] pre-shared-key plaintext 111-key
[Sysname-ikev2-keychain-telecom-peer-peer1] quit
```

Create an IKEv2 peer named **peer2**.

```
[Sysname-ikev2-keychain-telecom] peer peer2
```

Configure asymmetric plaintext pre-shared keys. The key for certificate signing is **111-key-b** and the key for certificate authentication is **111-key-a**.

```
[Sysname-ikev2-keychain-telecom-peer-peer2] pre-shared-key local plaintext
111-key-b
[Sysname-ikev2-keychain-telecom-peer-peer2] pre-shared-key remote plaintext
111-key-a
```

Related commands

- **ikev2 keychain**
- **peer**

New command: prf

Use **prf** to specify pseudo-random function (PRF) algorithms for an IKEv2 proposal.

Use **undo prf** to restore the default.

Syntax

In non-FIPS mode:

prf { **aes-xcbc-mac** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** } *

undo prf

In FIPS mode:

prf { **sha1** | **sha256** | **sha384** | **sha512** } *

undo prf

Default

An IKEv2 proposal uses the integrity protection algorithms as the PRF algorithms.

Views

IKEv2 proposal view

Predefined user roles

network-admin

Parameters

aes-xcbc-mac: Uses the HMAC-AES-XCBC-MAC algorithm.

md5: Uses the HMAC-MD5 algorithm.

sha1: Uses the HMAC-SHA1 algorithm.

sha256: Uses the HMAC-SHA256 algorithm.

sha384: Uses the HMAC-SHA384 algorithm.

sha512: Uses the HMAC-SHA512 algorithm.

Usage guidelines

You can specify multiple PRF algorithms for an IKEv2 proposal. An algorithm specified earlier has a higher priority.

Examples

Create an IKEv2 proposal named **prop1**.

```
<Sysname> system-view
[Sysname] ikev2 proposal prop1
```

Specify HMAC-SHA1 and HMAC-MD5 as the PRF algorithms, with HMAC-SHA1 preferred.

```
[Sysname-ikev2-proposal-prop1] prf sha1 md5
```

Related commands

- **ikev2 proposal**
- **integrity**

New command: priority (IKEv2 policy view)

Use **priority** to set a priority for an IKEv2 policy.

Use **undo priority** to restore the default.

Syntax

priority *priority*

undo priority

Default

The priority of an IKEv2 policy is 100.

Views

IKEv2 policy view

Predefined user roles

network-admin

Parameters

priority: Specifies the priority of the IKEv2 policy, in the range of 1 to 65535. A smaller number represents a higher priority.

Usage guidelines

The priority set by this command can only be used to adjust the match order of IKEv2 policies.

Examples

Set the priority to 10 for the IKEv2 policy **policy1**.

```
<Sysname> system-view
[Sysname] ikev2 policy policy1
[Sysname-ikev2-policy-policy1] priority 10
```

Related commands

display ikev2 policy

New command: priority (IKEv2 profile view)

Use **priority** to set a priority for an IKEv2 profile.

Use **undo priority** to restore the default.

Syntax

priority *priority*

undo priority

Default

The priority of an IKEv2 profile is 100.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

priority: Specifies the priority of the IKEv2 profile, in the range of 1 to 65535. A smaller number represents a higher priority.

Usage guidelines

The priority set by this command can only be used to adjust the match order of IKEv2 profiles.

Examples

Set the priority to 10 for the IKEv2 profile **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
[Sysname-ikev2-profile-profile1] priority 10
```

New command: proposal

Use **proposal** to specify an IKEv2 proposal for an IKEv2 policy.

Use **undo proposal** to remove an IKEv2 proposal from an IKEv2 policy.

Syntax

proposal *proposal-name*

undo proposal *proposal-name*

Default

No IKEv2 proposal is specified for an IKEv2 policy.

Views

IKEv2 policy view

Predefined user roles

network-admin

Parameters

proposal-name: Specifies an IKEv2 proposal by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can specify multiple IKEv2 proposals for an IKEv2 policy. A proposal specified earlier has a higher priority.

Examples

Specify the IKEv2 proposal **proposal1** for the IKEv2 policy **policy1**.

```
<Sysname> system-view
[Sysname] ikev2 policy policy1
[Sysname-ikev2-policy-policy1] proposal proposal1
```

Related commands

- **display ikev2 policy**
- **ikev2 proposal**

New command: reset ikev2 sa

Use **reset ikev2 sa** to delete IKEv2 SAs.

Syntax

reset ikev2 sa [[{ **local** | **remote** } { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]] | **tunnel** *tunnel-id*] [**fast**]

Views

User view

Predefined user roles

network-admin

Parameters

local: Deletes IKEv2 SAs for a local IP address.

remote: Deletes IKEv2 SAs for a remote IP address.

ipv4-address: Specifies a local or remote IPv4 address.

ipv6 *ipv6-address*: Specifies a local or remote IPv6 address.

vpn-instance *vpn-instance-name*: Deletes IKEv2 SAs in an MPLS L3VPN instance. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes IKEv2 SAs for the public network.

tunnel *tunnel-id*: Deletes IKEv2 SAs for an IPsec tunnel. The *tunnel-id* argument specifies an IPsec tunnel by its ID in the range of 1 to 2000000000.

fast: Notifies the peers of the deletion and deletes IKEv2 SAs directly before receiving the peers' responses. If you do not specify this keyword, the device notifies the peers of the deletion and deletes IKEv2 SAs after it receives the peers' responses.

Usage guidelines

Deleting an IKEv2 SA will also delete the child SAs negotiated through the IKEv2 SA.

If you do not specify any parameters, this command deletes all IKEv2 SAs and the child SAs negotiated through the IKEv2 SAs.

Examples

Display information about IKEv2 SAs.

```
<Sysname> display ikev2 sa
    Tunnel ID          Local              Remote              Status
```

```
  ------------------------------------------------------------------
     1                 1.1.1.1/500       1.1.1.2/500        EST
     2                 2.2.2.1/500       2.2.2.2/500        EST
  Status:
  IN-NEGO: Negotiating EST: Established, DEL: Deleting
```

Delete the IKEv2 SA whose remote IP address is 1.1.1.2.

```
<Sysname> reset ikev2 sa remote 1.1.1.2
```

Display information about IKEv2 SAs again. Verify that the IKEv2 SA is deleted.

```
<Sysname> display ikev2 sa
     Tunnel ID          Local             Remote             Status
  ------------------------------------------------------------------
     2                 2.2.2.1/500       2.2.2.2/500        EST
  Status:
  IN-NEGO: Negotiating EST: Established, DEL: Deleting
```

Related commands

display ikev2 sa

New command: reset ikev2 statistics

Use **reset ikev2 statistics** to clear IKEv2 statistics.

Syntax

reset ikev2 statistics

Views

Any view

Predefined user roles

network-admin

Examples

Clear IKEv2 statistics.

```
<Sysname> reset ikev2 statistics
```

New command: sa duration

Use **sa duration** to set the IKEv2 SA lifetime.

Use **undo sa duration** to restore the default.

Syntax

sa duration *seconds*

undo sa duration

Default

The IKEv2 SA lifetime is 86400 seconds.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

seconds: Specifies the IKEv2 SA lifetime in seconds, in the range of 120 to 86400.

Usage guidelines

An IKEv2 SA can be used for subsequent IKEv2 negotiations before its lifetime expires, saving a lot of negotiation time. However, the longer the lifetime, the higher the possibility that attackers collect enough information and initiate attacks.

Two peers can have different IKEv2 SA lifetime settings, and they do not perform lifetime negotiation. The peer with a shorter lifetime always initiates the rekeying.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Set the IKEv2 SA lifetime to 1200 seconds.

```
[Sysname-ikev2-profile-profile1] sa duration 1200
```

Related commands

display ikev2 profile

New command: esn enable

Use **esn enable** to enable the Extended Sequence Number (ESN) feature.

Use **undo esn enable** to disable the ESN feature.

Syntax

esn enable [**both**]

undo esn enable

Default

ESN is disabled.

Views

IPsec transform set view

Predefined user roles

network-admin

Parameters

both: Specifies IPsec to support both extended sequence number and traditional sequence number. If you do not specify this keyword, IPsec only supports extended sequence number.

Usage guidelines

The ESN feature extends the sequence number length from 32 bits to 64 bits. This feature prevents the sequence number space from being exhausted when large volumes of data are transmitted at high speeds over an IPsec SA. If the sequence number space is not exhausted, the IPsec SA does not need to be renegotiated.

This feature must be enabled at both the initiator and the responder.

Examples

Enable the ESN feature in the IPsec transform set **tran1**.

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
```

```
[Sysname-ipsec-transform-set-tran1] esn enable
```

Related commands

display ipsec transform-set

New command: ikev2-profile

Use **ikev2-profile** to specify an IKEv2 profile for an IPsec policy or IPsec policy template.

Use **undo ikev2-profile** to restore the default.

Syntax

ikev2-profile *profile-name*

undo ikev2-profile

Default

No IKEv2 profile is specified.

Views

IPsec policy view, IPsec policy template view

Predefined user roles

network-admin

Parameters

profile-name: Specifies an IKEv2 profile by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

The IKEv2 profile specified for an IPsec policy or IPsec policy template defines the parameters used for IKEv2 negotiation.

You can specify only one IKEv2 profile for an IPsec policy or IPsec policy template. On the initiator, an IKEv2 profile is required. On the responder, an IKEv2 profile is optional. If you do not specify an IKEv2 profile, the responder can use any IKEv2 profile for negotiation.

Examples

Specify the IKEv2 profile **profile1** for the IPsec policy **policy1**.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 10 isakmp
[Sysname-ipsec-policy-isakmp-policy1-10] ikev2-profile profile1
```

Related commands

- **display ipsec ipv6-policy**
- **display ipsec policy**
- **ikev2 profile**

New command: tfc enable

Use **tfc enable** to enable the Traffic Flow Confidentiality (TFC) padding feature.

Use **undo tfc enable** to disable the TFC padding feature.

Syntax

tfc enable

undo tfc enable

Default

TFC padding is disabled.

Views

IPsec policy view, IPsec policy template view

Predefined user roles

network-admin

Usage guidelines

The TFC padding feature can hide the length of the original packet, and might affect the packet encapsulation and de-encapsulation performance. This feature takes effect on UDP packets encapsulated by ESP in transport mode and on original IP packets encapsulated by ESP in tunnel mode.

Examples

Enable TFC padding for the IPsec policy **policy1**.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 10 isakmp
[Sysname-ipsec-policy-isakmp-policy1-10] tfc enable
```

Related commands

- **display ipsec ipv6-policy**
- **display ipsec policy**

Modified command: ah authentication-algorithm

Old 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

New syntax

In non-FIPS mode:

ah authentication-algorithm { **aes-xcbc-mac** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** } *

undo ah authentication-algorithm

In FIPS mode:

ah authentication-algorithm { **sha1** | **sha256** | **sha384** | **sha512** } *

undo ah authentication-algorithm

Views

IPsec transform set view

Change description

The following keywords were added:

- **aes-xcbc-mac**: Specifies the HMAC-AES-XCBC-MAC algorithm.

- **sha256**: Specifies the HMAC-SHA256 algorithm.
- **sha384**: Specifies the HMAC-SHA384 algorithm.
- **sha512**: Specifies the HMAC-SHA512 algorithm.

Modified command: display ipsec { ipv6-policy | policy }

Syntax

display ipsec { **ipv6-policy | policy** } [*policy-name* [*seq-number*]]

Views

Any view

Change description

The following fields were added to the command output:

- **Traffic Flow Confidentiality**—Whether Traffic Flow Confidentiality (TFC) padding is enabled.
- **IKEv2 profile**—IKEv2 profile used by the IPsec policy.

Modified command: display ipsec { ipv6-policy-template | policy-template }

Syntax

display ipsec { **ipv6-policy-template | policy-template** } [*template-name* [*seq-number*]]

Views

Any view

Change description

The following fields were added to the command output:

- **Traffic Flow Confidentiality**—Whether Traffic Flow Confidentiality (TFC) padding is enabled.
- **Selector mode**—Data flow protection mode of the IPsec policy template.
- **Local address**—Local end IP address of the IPsec tunnel.
- **IKEv2 profile**—IKEv2 profile used by the IPsec policy template.
- **SA idle time**—Idle timeout of the IPsec SA, in seconds.

Modified command: display ipsec sa

Syntax

display ipsec sa [**brief | count | interface** *interface-type interface-number* **|** { **ipv6-policy | policy** } *policy-name* [*seq-number*] **| profile** *profile-name* **| remote** [**ipv6**] *ip-address*]

Views

Any view

Change description

The following fields were added to the command output:

- **Extended Sequence Number enable**—Whether Extended Sequence Number (ESN) is enabled.
- **Traffic Flow Confidentiality enable**—Whether Traffic Flow Confidentiality (TFC) padding is enabled.

- **Inside VRF**—VPN instance to which the protected data flow belongs.

The following values were added to the **Perfect Forward Secrecy** field:

- **dh-group19**—256-bit ECP Diffie-Hellman group.
- **dh-group20**—384-bit ECP Diffie-Hellman group.

Modified command: display ipsec transform-set

Syntax

display ipsec transform-set [*transform-set-name*]

Views

Any view

Change description

The following fields were added to the command output:

- **ESN**—Whether Extended Sequence Number (ESN) is enabled.
- **PFS**—Perfect Forward Secrecy (PFS) configuration.

Modified command: display ipsec tunnel

Syntax

display ipsec tunnel { **brief | count | tunnel-id** *tunnel-id* }

Views

Any view

Change description

The following values were added to the **Perfect Forward Secrecy** field of the command output:

- **dh-group19**—256-bit ECP Diffie-Hellman group.
- **dh-group20**—384-bit ECP Diffie-Hellman group.

Modified command: esp authentication-algorithm

Old 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

New syntax

In non-FIPS mode:

esp authentication-algorithm { **aes-xcbc-mac | md5 | sha1 | sha256 | sha384 | sha512** } *

undo esp authentication-algorithm

In FIPS mode:

esp authentication-algorithm { **sha1** | **sha256** | **sha384** | **sha512** } *

undo esp authentication-algorithm

Views

IPsec transform set view

Change description

The following keywords were added:

- **aes-xcbc-mac**: Specifies the HMAC-AES-XCBC-MAC algorithm.
- **sha256**: Specifies the HMAC-SHA256 algorithm.
- **sha384**: Specifies the HMAC-SHA384 algorithm.
- **sha512**: Specifies the HMAC-SHA512 algorithm.

Modified command: esp encryption-algorithm

Old syntax

In non-FIPS mode:

esp encryption-algorithm { **3des-cbc** | **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** | **des-cbc** | **null** } *

undo esp encryption-algorithm

In FIPS mode:

esp encryption-algorithm { **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** }*

undo esp encryption-algorithm

New syntax

In non-FIPS mode:

esp encryption-algorithm { **3des-cbc** | **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** | **aes-ctr-128** | **aes-ctr-192** | **aes-ctr-256** | **camellia-cbc-128** | **camellia-cbc-192** | **camellia-cbc-256** | **des-cbc** | **gmac-128** | **gmac-192** | **gmac-256** | **gcm-128** | **gcm-192** | **gcm-256** | **null** } *

undo esp encryption-algorithm

In FIPS mode:

esp encryption-algorithm { **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** | **aes-ctr-128** | **aes-ctr-192** | **aes-ctr-256** | **gmac-128** | **gmac-192** | **gmac-256** | **gcm-128** | **gcm-192** | **gcm-256** }*

undo esp encryption-algorithm

Views

IPsec transform set view

Change description

The following keywords were added:

- **aes-ctr-128**: Uses the AES algorithm with a 128-bit key in CTR mode. This keyword is available only for IKEv2.
- **aes-ctr-192**: Uses the AES algorithm with a 192-bit key in CTR mode. This keyword is available only for IKEv2.
- **aes-ctr-256**: Uses the AES algorithm with a 256-bit key in CTR mode. This keyword is available only for IKEv2.
- **camellia-cbc-128**: Uses the Camellia algorithm with a 128-bit key in CBC mode. This keyword is available only for IKEv2.

- **camellia-cbc-192**: Uses the Camellia algorithm with a 192-bit key in CBC mode. This keyword is available only for IKEv2.
- **camellia-cbc-256**: Uses the Camellia algorithm with a 256-bit key in CBC mode. This keyword is available only for IKEv2.
- **gmac-128**: Uses the GMAC algorithm with a 128-bit key. This keyword is available only for IKEv2.
- **gmac-192**: Uses the GMAC algorithm with a 192-bit key. This keyword is available only for IKEv2.
- **gmac-256**: Uses the GMAC algorithm with a 256-bit key. This keyword is available only for IKEv2.
- **gcm-128**: Uses the GCM algorithm with a 128-bit key. This keyword is available only for IKEv2.
- **gcm-192**: Uses the GCM algorithm with a 192-bit key. This keyword is available only for IKEv2.
- **gcm-256**: Uses the GCM algorithm with a 256-bit key. This keyword is available only for IKEv2.

Modified command: pfs

Old syntax

In non-FIPS mode:

pfs { **dh-group1 | dh-group2 | dh-group5 | dh-group14 | dh-group24** }

undo pfs

In FIPS mode:

pfs dh-group14

undo pfs

New syntax

In non-FIPS mode:

pfs { **dh-group1 | dh-group2 | dh-group5 | dh-group14 | dh-group19 | dh-group20 | dh-group24** }

undo pfs

In FIPS mode:

pfs { **dh-group14 | dh-group19 | dh-group20 | dh-group24** }

undo pfs

Views

IPsec transform set view

Change description

The following keywords were added:

- **dh-group19**: Uses 256-bit ECP Diffie-Hellman group. This keyword is available only for IKEv2.
- **dh-group20**: Uses 384-bit ECP Diffie-Hellman group. This keyword is available only for IKEv2.

New feature: SSH support for Suite B

Configuring SSH based on Suite B algorithms

Suite B contains a set of encryption and authentication algorithms that meet high security requirements. Table 1 lists all algorithms in Suite B.

The SSH server and client support using the X.509v3 certificate for identity authentication in compliance with the algorithm, negotiation, and authentication specifications defined in RFC 6239.

Table 1 Suite B algorithms

Security level	Key exchange algorithm	Encryption algorithm and HMAC algorithm	Public key algorithm
128-bit	ecdh-sha2-nistp256	AEAD_AES_128_GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384
192-bit	ecdh-sha2-nistp384	AEAD_AES_256_GCM	x509v3-ecdsa-sha2-nistp384
Both	ecdh-sha2-nistp256 ecdh-sha2-nistp384	AEAD_AES_128_GCM AEAD_AES_256_GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384

Specifying a PKI domain for the SSH server

The PKI domain specified for the SSH server has the following functions:

- The SSH server uses the PKI domain to send its certificate to the client in the key exchange stage.
- The SSH server uses the PKI domain to authenticate the client's certificate if no PKI domain is specified for the client authentication by using the **ssh user** command.

To specify a PKI domain for the SSH server:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Specify a PKI domain for the SSH server.	**ssh server pki-domain** *domain-name*	By default, no PKI domain is specified for the SSH server.

Establishing a connection to an Stelnet server based on Suite B

Task	Command	Remarks
Establish a connection to an Stelnet server based on Suite B.	• Establish a connection to an IPv4 Stelnet server based on Suite B: **ssh2** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**dscp** *dscp-value* | **escape** *character* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] * • Establish a connection to an IPv6 Stelnet server based on Suite B: **ssh2 ipv6** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**-i** *interface-type interface-number*] [**prefer-compress zlib**] [**dscp** *dscp-value* | **escape** *character* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *	Available in user view. The client cannot establish connections to both IPv4 and IPv6 Stelnet servers.

Establishing a connection to an SFTP server based on Suite B

Task	Command	Remarks
Establish a connection to an SFTP server based on Suite B.	• Establish a connection to an IPv4 SFTP server based on Suite B: **sftp** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] * • Establish a connection to an IPv6 SFTP server based on Suite B: **sftp ipv6** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**-i** *interface-type interface-number*] [**prefer-compress zlib**] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *	Available in user view. The client cannot establish connections to both IPv4 and IPv6 SFTP servers.

Establishing a connection to an SCP server based on Suite B

Task	Command	Remarks
Establish a connection to an SCP server based on Suite B.	• Establish a connection to an IPv4 SCP server based on Suite B: **scp** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] { **put** | **get** } *source-file-name* [*destination-file-name*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] * • Establish a connection to an IPv6 SCP server based on Suite B: **scp ipv6** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] { **put** | **get** } *source-file-name* [*destination-file-name*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *	Available in user view. The client cannot establish connections to both IPv4 and IPv6 SCP servers.

Specifying algorithms for SSH2

Perform this task to specify the following types of algorithms that the SSH2 client and server use for algorithm negotiation during the Stelnet, SFTP, or SCP session establishment:

- Key exchange algorithms.
- Public key algorithms.
- Encryption algorithms.
- MAC algorithms.

If you specify algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The client uses the specified algorithms to initiate the negotiation, and the server uses the matching algorithms to negotiate with the client.

If multiple algorithms of the same type are specified, the algorithm specified earlier has a higher priority during negotiation.

Specifying key exchange algorithms for SSH2

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Specify key exchange algorithms for SSH2.	• In non-FIPS mode: **ssh2 algorithm key-exchange** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } * • In FIPS mode: **ssh2 algorithm key-exchange**	By default, SSH2 uses the key exchange algorithms **ecdh-sha2-nistp256**, **ecdh-sha2-nistp384**, **dh-group-exchange-sha1**, **dh-group14-sha1**, and **dh-group1-sha1** in descending order of priority for algorithm negotiation.

Step	Command	Remarks
	{ **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } *	

Specifying public key algorithms for SSH2

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Specify public key algorithms for SSH2.	• In non-FIPS mode: **ssh2 algorithm public-key** { **dsa** | **ecdsa** | **rsa** | **x509v3-ecdsa-sha2-nistp384** | **x509v3-ecdsa-sha2-nistp256** } * • In FIPS mode: **ssh2 algorithm public-key** { **ecdsa** | **rsa** | **x509v3-ecdsa-sha2-nistp384** | **x509v3-ecdsa-sha2-nistp256** } *	By default, SSH2 uses the public key algorithms **x509v3-ecdsa-sha2-nistp256**, **x509v3-ecdsa-sha2-nistp384**, **ecdsa**, **rsa**, and **dsa** in descending order of priority for algorithm negotiation.

Specifying encryption algorithms for SSH2

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Specify encryption algorithms for SSH2.	• In non-FIPS mode: **ssh2 algorithm cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } * • In FIPS mode: **ssh2 algorithm cipher** { **aes128-cbc** | **aes256-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } *	By default, SSH2 uses the encryption algorithms **aes128-ctr**, **aes192-ctr**, **aes256-ctr**, **aes128-gcm**, **aes256-gcm**, **aes128-cbc**, **3des-cbc**, **aes256-cbc**, and **des-cbc** in descending order of priority for algorithm negotiation.

Specifying MAC algorithms for SSH2

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Specify MAC algorithms for SSH2.	• In non-FIPS mode: **ssh2 algorithm mac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } * • In FIPS mode: **ssh2 algorithm mac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } *	By default, SSH2 uses the MAC algorithms **sha2-256**, **sha2-512**, **sha1**, **md5**, **sha1-96**, and **md5-96** in descending order of priority for algorithm negotiation.

Command reference

New command: ssh server pki-domain

Use **ssh server pki-domain** to specify a PKI domain for the SSH server.

Use **undo ssh server pki-domain** to delete the PKI domain of the SSH server.

Syntax

ssh server pki-domain *domain-name*

undo ssh server pki-domain

Default

No PKI domain is specified for an SSH server.

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies the name of a PKI domain, a case-insensitive string of 1 to 31 characters, excluding the characters listed in Table 2.

Table 2 Invalid characters for a PKI domain name

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

Examples

Specify the PKI domain **serverpkidomain** for the SSH server.

```
<Sysname> system-view
[Sysname] ssh server pki-domain serverpkidomain
```

New command: scp ipv6 suite-b

Use **scp ipv6 suite-b** to establish a connection to an IPv6 SCP server based on Suite B algorithms and transfer files with the server.

Syntax

scp ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] { **put** | **get** } *source-file-name* [*destination-file-name*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

-i *interface-type interface-number:* Specifies an output interface by its type and number for SCP packets. Specify this option when the server uses a link-local address to provide the SCP service for the client. The specified output interface on the SCP client must have a link-local address.

get: Downloads the file.

put: Uploads the file.

source-file-name: Specifies the name of the source file.

destination-file-name: Specifies the name of the target file. If you do not specify this argument, the target file uses the same file name as the source file.

suite-b: Specifies the Suite B algorithms. If neither the **128-bit** keyword nor the **192-bit** keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see Table 1.

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters, excluding the characters listed in Table 3.

Table 3 Invalid characters for a PKI domain name

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters, excluding the characters listed in Table 3.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies the compression algorithm **zlib**.

source: Specifies a source IPv6 address or source interface for IPv6 SCP packets. By default, the device automatically selects a source address for IPv6 SCP packets in compliance with RFC 3484. For successful SCP connections, use one of the following methods:

- Specify the loopback interface as the source interface.
- Specify the IPv6 address of the loopback interface as the source IPv6 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IPv6 address of the IPv6 SCP packets.

ipv6 *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

Table 1 Suite B algorithms

Security level	Key exchange algorithm	Encryption algorithm and HMAC algorithm	Public key algorithm
128-bit	ecdh-sha2-nistp256	AEAD_AES_128_GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384
192-bit	ecdh-sha2-nistp384	AEAD_AES_256_GCM	x509v3-ecdsa-sha2-nistp384
Both	ecdh-sha2-nistp256 ecdh-sha2-nistp384	AEAD_AES_128_GCM AEAD_AES_256_GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384

If the client and the server have negotiated to use certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, you must specify the server's PKI domain on the client by using the **server-pki-domain** *domain-name* option. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

Examples

Use the 192-bit Suite B algorithms to establish a connection to the SCP sever **2000::1** and download the file **abc.txt** from the server. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> scp ipv6 2000::1 get abc.txt suite-b 192-bit pki-domain clientpkidomain
server-pki-domain serverpkidomain
```

New command: scp suite-b

Use **scp suite-b** to establish a connection to an SCP server based on Suite B algorithms and transfer files with the server.

Syntax

scp *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] { **put** | **get** } *source-file-name* [*destination-file-name*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

get: Downloads the file.

put: Uploads the file.

source-file-name: Specifies the name of the source file.

destination-file-name: Specifies the name of the target file. If you do not specify this argument, the target file uses the same file name as the source file.

suite-b: Specifies the Suite B algorithms. If neither the **128-bit** keyword nor the **192-bit** keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see Table 1.

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters, excluding the characters listed in Table 4.

Table 4 Invalid characters for a PKI domain name

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters, excluding the characters listed in Table 4.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies the compression algorithm **zlib**.

source: Specifies a source IP address or source interface for SCP packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SCP packets. For successful SCP connections, use one of the following methods:

- Specify the loopback interface as the source interface.
- Specify the IPv4 address of the loopback interface as the source IPv4 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number. The IPv4 address of this interface is the source IPv4 address of the SCP packets.

ip *ip-address*: Specifies a source IPv4 address.

Usage guidelines

If the client and the server have negotiated to use certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, you must specify the server's PKI domain on the client by using the **server-pki-domain** *domain-name* option. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

Examples

Use the 128-bit Suite B algorithms to establish a connection to the SCP sever **200.1.1.1** and download the file **abc.txt** from the server. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> scp 200.1.1.1 get abc.txt suite-b 128-bit pki-domain clientpkidomain
server-pki-domain serverpkidomain
```

New command: sftp ipv6 suite-b

Use **sftp ipv6 suite-b** to establish a connection to an IPv6 SFTP server based on Suite B algorithms and enter SFTP client view.

Syntax

sftp ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**-i** *interface-type interface-number*] [**prefer-compress zlib**] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

-i *interface-type interface-number:* Specifies an output interface by its type and number for IPv6 SFTP packets. Specify this option when the server uses a link-local address to provide the SFTP service for the client. The specified output interface on the SFTP client must have a link-local address.

suite-b: Specifies the Suite B algorithms. If neither the **128-bit** keyword nor the **192-bit** keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see Table 1.

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters, excluding the characters listed in Table 2.

Table 2 Invalid characters for a PKI domain name

<table>
<tr><th>Character name</th><th>Symbol</th><th>Character name</th><th>Symbol</th></tr>
<tr><td>Tilde</td><td>~</td><td>Dot</td><td>.</td></tr>
<tr><td>Asterisk</td><td>*</td><td>Left angle bracket</td><td><</td></tr>
<tr><td>Backslash</td><td>\</td><td>Right angle bracket</td><td>></td></tr>
<tr><td>Vertical bar</td><td>|</td><td>Quotation marks</td><td>"</td></tr>
</table>

Character name	Symbol	Character name	Symbol
Colon	:	Apostrophe	'

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters, excluding the characters listed in Table 2.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies the compression algorithm **zlib**.

dscp *dscp-value*: Specifies the DSCP value in the IPv6 SFTP packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

source: Specifies a source IP address or source interface for IPv6 SFTP packets. By default, the device automatically selects a source address for IPv6 SFTP packets in compliance with RFC 3484. For successful IPv6 SFTP connections, use one of the following methods:

- Specify the loopback interface as the source interface.
- Specify the IPv6 address of the loopback interface as the source IPv6 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IP address of the IPv6 SFTP packets.

ipv6 *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

If the client and the server have negotiated to use certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, you must specify the server's PKI domain on the client by using the **server-pki-domain** *domain-name* option. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

Examples

Use the 192-bit Suite B algorithms to establish a connection to the SFTP sever **2000::1**. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> sftp ipv6 2000::1 suite-b 192-bit pki-domain clientpkidomain server-pki-domain
serverpkidomain
```

New command: sftp suite-b

Use **sftp suite-b** to establish a connection to an IPv4 SFTP server based on Suite B algorithms and enter SFTP client view.

Syntax

sftp *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

suite-b: Specifies the Suite B algorithms. If neither the **128-bit** keyword nor the **192-bit** keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see Table 1.

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters, excluding the characters listed in Table 5.

Table 5 Invalid characters for a PKI domain name

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters, excluding the characters listed in Table 5.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies the compression algorithm **zlib**.

dscp *dscp-value*: Specifies the DSCP value in the IPv4 SFTP packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

source: Specifies a source IP address or source interface for the SFTP packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SFTP packets. For successful SFTP connections, use one of the following methods:

- Specify the loopback interface as the source interface.
- Specify the IPv4 address of the loopback interface as the source IPv4 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number. The primary IPv4 address of this interface is the source IPv4 address of the SFTP packets.

ip *ip-address*: Specifies a source IPv4 address.

Usage guidelines

If the client and the server have negotiated to use certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, you must specify the server's PKI domain on the client by using the **server-pki-domain** *domain-name* option. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

Examples

Use the 128-bit Suite B algorithms to establish a connection to the SFTP sever **10.1.1.2**. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> sftp 10.1.1.2 suite-b 128-bit pki-domain clientpkidomain server-pki-domain
serverpkidomain
```

New command: ssh2 ipv6 suite-b

Use **ssh2 ipv6 suite-b** to establish a connection to an IPv6 Stelnet server based on Suite B algorithms.

Syntax

ssh2 ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**-i** *interface-type interface-number*] [**prefer-compress zlib**] [**dscp** *dscp-value* | **escape** *character* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

-i *interface-type interface-number:* Specifies an output interface by its type and number for IPv6 SSH packets. Specify this option when the server uses a link-local address to provide the Stelnet service for the client. The specified output interface on the Stelnet client must have a link-local address.

suite-b: Specifies the Suite B algorithms. If neither the **128-bit** keyword nor the **192-bit** keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see Table 1.

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters, excluding the characters listed in Table 6.

Table 6 Invalid characters for a PKI domain name

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>

Character name	Symbol	Character name	Symbol
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters, excluding the characters listed in Table 6.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies the compression algorithm **zlib**.

dscp *dscp-value*: Specifies the DSCP value in the IPv6 SSH packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

escape *character*: Specifies a case-sensitive escape character. By default, the escape character is a tilde (~).

source: Specifies a source IP address or source interface for IPv6 SSH packets. By default, the device automatically selects a source address for IPv6 SSH packets in compliance with RFC 3484. For successful IPv6 Stelnet connections, use one of the following methods:

- Specify the loopback interface as the source interface.
- Specify the IPv6 address of the loopback interface as the source IPv6 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IP address of the IPv6 SSH packets.

ipv6 *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

If the client and the server have negotiated to use certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, you must specify the server's PKI domain on the client by using the **server-pki-domain** *domain-name* option. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

The combination of an escape character and a dot (.) works as an escape sequence. This escape sequence is typically used to quickly terminate an SSH connection when the server reboots or malfunctions.

For the escape sequence to take effect, you must enter it at the very beginning of a line. If you have entered other characters or performed operations in a line, enter the escape sequence in the next line. Hewlett Packard Enterprise recommends that you use the default escape character (~). Do not use any character in SSH usernames as the escape character.

Examples

Use the 192-bit Suite B algorithms to establish a connection to the Stelnet sever **2000::1**. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> ssh2 ipv6 2000::1 suite-b 192-bit pki-domain clientpkidomain server-pki-domain
serverpkidomain
```

New command: ssh2 suite-b

Use **ssh2 suite-b** to establish a connection to an IPv4 Stelnet server based on Suite B algorithms.

Syntax

ssh2 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**dscp** *dscp-value* | **escape** *character* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.|

suite-b: Specifies the Suite B algorithms. If neither the **128-bit** keyword nor the **192-bit** keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see Table 1.

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters, excluding the characters listed in Table 7.

Table 7 Invalid characters for a PKI domain name

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters, excluding the characters listed in Table 7.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies the compression algorithm **zlib**.

dscp *dscp-value*: Specifies the DSCP value in the IPv4 SSH packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

escape *character*: Specifies a case-sensitive escape character. By default, the escape character is a tilde (~).

source: Specifies a source IP address or source interface for SSH packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SSH packets. For successful Stelnet connections, use one of the following methods:

- Specify the loopback interface as the source interface.
- Specify the IPv4 address of the loopback interface as the source IPv4 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number. The primary IPv4 address of this interface is the source IPv4 address of the SSH packets.

ip *ip-address*: Specifies a source IPv4 address.

Usage guidelines

If the client and the server have negotiated to use certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, you must specify the server's PKI domain on the client by using the **server-pki-domain** *domain-name* option. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

The combination of an escape character and a dot (.) works as an escape sequence. This escape sequence is typically used to quickly terminate an SSH connection when the server reboots or malfunctions.

For the escape sequence to take effect, you must enter it at the very beginning of a line. If you have entered other characters or performed operations in a line, enter the escape sequence in the next line. Hewlett Packard Enterprise recommends that you use the default escape character (~). Do not use any character in SSH usernames as the escape character.

Examples

Use the 128-bit Suite B algorithms to establish a connection to the SFTP sever **3.3.3.3**. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> ssh2 3.3.3.3 suite-b 128-bit pki-domain clientpkidomain server-pki-domain
serverpkidomain
```

New command: display ssh2 algorithm

Use **display ssh2 algorithm** to display algorithms used by SSH2 in the algorithm negotiation stage.

Syntax

display ssh2 algorithm

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display algorithms used by SSH2 in the algorithm negotiation stage.

```
<Sysname> display ssh2 algorithm
 Key exchange algorithms : ecdh-sha2-nistp256 ecdh-sha2-nistp384 dh-group-exchange-sha1
dh-group14-sha1 dh-group1-sha1
 Public key algorithms : x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384 ecdsa rsa
dsa
```

```
 Encryption algorithms : aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm
aes128-cbc 3des-cbc aes256-cbc des-cbc
 MAC algorithms : sha2-256 sha2-512 sha1 md5 sha1-96 md5-96
```

Table 8 Command output

Field	Description
Key exchange algorithms	Key exchange algorithms in descending order of priority for algorithm negotiation.
Public key algorithms	Public key algorithms in descending order of priority for algorithm negotiation.
Encryption algorithms	Encryption algorithms in descending order of priority for algorithm negotiation.
MAC algorithms	MAC algorithms in descending order of priority for algorithm negotiation.

Related commands

- **ssh2 algorithm cipher**
- **ssh2 algorithm key-exchange**
- **ssh2 algorithm mac**
- **ssh2 algorithm public-key**

New command: ssh2 algorithm cipher

Use **ssh2 algorithm cipher** to specify encryption algorithms for SSH2.

Use **undo ssh2 algorithm cipher** to restore the default.

Syntax

In non-FIPS mode:

ssh2 algorithm cipher { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } *

undo ssh2 algorithm cipher

In FIPS mode:

ssh2 algorithm cipher { **aes128-cbc** | **aes256-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } *

undo ssh2 algorithm cipher

Default

SSH2 uses the encryption algorithms **aes128-ctr**, **aes192-ctr**, **aes256-ctr**, **aes128-gcm**, **aes256-gcm**, **aes128-cbc**, **3des-cbc**, **aes256-cbc**, and **des-cbc** in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

Parameters

3des-cbc: Specifies the encryption algorithm **3des-cbc**. Support for this keyword depends on the device model.

aes128-cbc: Specifies the encryption algorithm **aes128-cbc**.

aes256-cbc: Specifies the encryption algorithm **aes256-cbc**.

des-cbc: Specifies the encryption algorithm **des-cbc**.

aes128-ctr: Specifies the encryption algorithm **aes128-ctr**.

aes192-ctr: Specifies the encryption algorithm **aes192-ctr**.

aes256-ctr: Specifies the encryption algorithm **aes256-ctr**.

aes256-gcm: Specifies the encryption algorithm **aes256-gcm**.

aes128-gcm: Specifies the encryption algorithm **aes128-gcm**.

Usage guidelines

If you specify the encryption algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The algorithm specified earlier has a higher priority during negotiation.

Examples

Specify the algorithm **3des-cbc** as the encryption algorithm for SSH2.

```
<Sysname> system-view
[Sysname] ssh2 algorithm cipher 3des-cbc
```

Related commands

- **display ssh2 algorithm**
- **ssh2 algorithm key-exchange**
- **ssh2 algorithm mac**
- **ssh2 algorithm public-key**

New command: ssh2 algorithm key-exchange

Use **ssh2 algorithm key-exchange** to specify key exchange algorithms for SSH2.

Use **undo ssh2 algorithm key-exchange** to restore the default.

Syntax

In non-FIPS mode:

ssh2 algorithm key-exchange { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } *

undo ssh2 algorithm key-exchange

In FIPS mode:

ssh2 algorithm key-exchange { **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } *

undo ssh2 algorithm key-exchange

Default

SSH2 uses the key exchange algorithms **ecdh-sha2-nistp256**, **ecdh-sha2-nistp384**, **dh-group-exchange-sha1**, **dh-group14-sha1**, and **dh-group1-sha1** in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

Parameters

dh-group-exchange-sha1: Specifies the key exchange algorithm **diffie-hellman-group-exchange-sha1**.

dh-group1-sha1: Specifies the key exchange algorithm **diffie-hellman-group1-sha1**.

dh-group14-sha1: Specifies the key exchange algorithm **diffie-hellman-group14-sha1**.

ecdh-sha2-nistp256: Specifies the key exchange algorithm **ecdh-sha2-nistp256**.

ecdh-sha2-nistp384: Specifies the key exchange algorithm **ecdh-sha2-nistp384**.

Usage guidelines

If you specify the key exchange algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The algorithm specified earlier has a higher priority during negotiation.

Examples

Specify the algorithm **dh-group1-sha1** as the key exchange algorithm for SSH2.

```
<Sysname> system-view
[Sysname] ssh2 algorithm key-exchange dh-group1-sha1
```

Related commands

- **display ssh2 algorithm**
- **ssh2 algorithm cipher**
- **ssh2 algorithm mac**
- **ssh2 algorithm public-key**

New command: ssh2 algorithm mac

Use **ssh2 algorithm mac** to specify MAC algorithms for SSH2.

Use **undo ssh2 algorithm mac** to restore the default.

Syntax

In non-FIPS mode:

ssh2 algorithm mac { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } *

undo ssh2 algorithm mac

In FIPS mode:

ssh2 algorithm mac { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } *

undo ssh2 algorithm mac

Default

SSH2 uses the MAC algorithms **sha2-256**, **sha2-512**, **sha1**, **md5**, **sha1-96**, and **md5-96** in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

Parameters

md5: Specifies the HMAC algorithm **hmac-md5**.

md5-96: Specifies the HMAC algorithm **hmac-md5-96**.

sha1: Specifies the HMAC algorithm **hmac-sha1**.

sha1-96: Specifies the HMAC algorithm **hmac-sha1-96**.

sha2-256: Specifies the HMAC algorithm **hmac-sha2-256**.

sha2-512: Specifies the HMAC algorithm **hmac-sha2-512**.

Usage guidelines

If you specify the MAC algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The algorithm specified earlier has a higher priority during negotiation.

Examples

Specify the algorithm **md5** as the MAC algorithm for SSH2.

```
<Sysname> system-view
[Sysname] ssh2 algorithm mac md5
```

Related commands

- **display ssh2 algorithm**
- **ssh2 algorithm cipher**
- **ssh2 algorithm key-exchange**
- **ssh2 algorithm public-key**

New command: ssh2 algorithm public-key

Use **ssh2 algorithm public-key** to specify public key algorithms for SSH2.

Use **undo ssh2 algorithm public-key** to restore the default.

Syntax

In non-FIPS mode:

ssh2 algorithm public-key { **dsa** | **ecdsa** | **rsa** | **x509v3-ecdsa-sha2-nistp384** | **x509v3-ecdsa-sha2-nistp256** } *

undo ssh2 algorithm public-key

In FIPS mode:

ssh2 algorithm public-key { **ecdsa** | **rsa** | **x509v3-ecdsa-sha2-nistp384** | **x509v3-ecdsa-sha2-nistp256** } *

undo ssh2 algorithm public-key

Default

SSH2 uses the public key algorithms **x509v3-ecdsa-sha2-nistp256**, **x509v3-ecdsa-sha2-nistp384**, **ecdsa**, **rsa**, and **dsa** in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

Parameters

dsa: Specifies the public key algorithm **dsa**.

ecdsa: Specifies the public key algorithm **ecdsa**.

rsa: Specifies the public key algorithm **rsa.**

x509v3-ecdsa-sha2-nistp256: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp256**.

x509v3-ecdsa-sha2-nistp384: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp384**.

Usage guidelines

If you specify the public key algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The algorithm specified earlier has a higher priority during negotiation.

Examples

Specify the algorithm **dsa** as the public key algorithm for SSH2.

```
<Sysname> system-view
[Sysname] ssh2 algorithm public-key dsa
```

Related commands

- **display ssh2 algorithm**
- **ssh2 algorithm cipher**
- **ssh2 algorithm key-exchange**
- **ssh2 algorithm mac**

Modified command: display ssh server

Syntax

display ssh server status

Views

Any view

Change description

In the command output, the **SSH Server PKI domain name** field was added to represent the PKI domain of the SSH server.

Modified command: ssh user

Old syntax

In non-FIPS mode:

ssh user *username* **service-type** { **all** | **netconf** | **scp** | **sftp** | **stelnet** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign** { **pki-domain** *domain-name* | **publickey** *keyname* } }

undo ssh user *username*

In FIPS mode:

ssh user *username* **service-type** { **all** | **netconf** | **scp** | **sftp** | **stelnet** } **authentication-type** { **password** | **password-publickey assign** { **pki-domain** *domain-name* | **publickey** *keyname* } }

undo ssh user *username*

New syntax

In non-FIPS mode:

ssh user *username* **service-type** { **all** | **netconf** | **scp** | **sftp** | **stelnet** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } [**assign** { **pki-domain** *domain-name* | **publickey** *keyname* }] }

undo ssh user *username*

In FIPS mode:

ssh user *username* **service-type** { **all** | **netconf** | **scp** | **sftp** | **stelnet** } **authentication-type** { **password | password-publickey** [**assign** { **pki-domain** *domain-name* **|** **publickey** *keyname* }] }

undo ssh user *username*

Views

System view

Change description

Before modification: The options **assign** { **pki-domain** *domain-name* **|** **publickey** *keyname* } are required for verifying the client.

After modification: The options **assign** { **pki-domain** *domain-name* **|** **publickey** *keyname* } are optional for verifying the client.

Modified command: scp

Old syntax

In non-FIPS mode:

scp *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **dsa** | **ecdsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des** | **aes128** | **aes256** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **aes256** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**public-key** *keyname* **|** **source** { **interface** *interface-type interface-number* **|** **ip** *ip-address* }] *

In FIPS mode:

scp *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **ecdsa** | **rsa** } | **prefer-compress zlib** | **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** }] * [**public-key** *keyname* **|** **source** { **interface** *interface-type interface-number* **|** **ip** *ip-address* }] *

New syntax

In non-FIPS mode:

scp *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **dsa** | **ecdsa** | **rsa** | { **x509v3-ecdsa-sha2-nistp384** | **x509v3-ecdsa-sha2-nistp256** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [{ **public-key** *keyname* | **server-pki-domain** *domain-name* } **|** **source** { **interface** *interface-type interface-number* **|** **ip** *ip-address* }] *

In FIPS mode:

scp *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **ecdsa** | **rsa** | { **x509v3-ecdsa-sha2-nistp384** | **x509v3-ecdsa-sha2-nistp256** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **aes128-cbc** | **aes256-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **aes128-cbc** | **aes256-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [{ **public-key** *keyname* |

server-pki-domain *domain-name* } | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

Views

User view

Change description

The following keywords were added:

- Keywords for specifying PKI domains used in certificate verification:
  - **pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. When the public key algorithm is x509v3 (**x509v3-ecdsa-sha2-nistp256** or **x509v3-ecdsa-sha2-nistp384**), you must specify this option for the client to get the correct local certificate.
  - **server-pki-domain** *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

    The PKI domain name cannot contain characters in the following table:

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

- Keywords for specifying the publickey algorithms used in publickey authentication:
  - **x509v3-ecdsa-sha2-nistp256**: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp256**.
  - **x509v3-ecdsa-sha2-nistp384**: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp384**.
- Keywords for specifying the preferred client-to-server encryption algorithms:
  - **aes128-ctr**: Specifies the encryption algorithm **aes128-ctr**.
  - **aes192-ctr**: Specifies the encryption algorithm **aes192-ctr**.
  - **aes256-ctr**: Specifies the encryption algorithm **aes256-ctr**.
  - **aes256-gcm**: Specifies the encryption algorithm **aes256-gcm**.
  - **aes128-gcm**: Specifies the encryption algorithm **aes128-gcm**.
- Keywords for specifying the preferred client-to-server HMAC algorithms:
  - **sha2-256**: Specifies the HMAC algorithm **sha2-256**.
  - **sha2-512**: Specifies the HMAC algorithm **sha2-512**.
- Keywords for specifying the preferred key exchange algorithms:
  - **ecdh-sha2-nistp256**: Specifies the key exchange algorithm **ecdh-sha2-nistp256**.
  - **ecdh-sha2-nistp384**: Specifies the key exchange algorithm **ecdh-sha2-nistp384**.

The following keywords were modified:

- Keywords for the preferred client-to-server encryption algorithm **prefer-ctos-cipher**:
  - The **3des** keyword was changed to **3des-cbc**.
  - The **aes128** keyword was changed to aes128**-cbc**.

- The **aes256** keyword was changed to aes256**-cbc**.
- The **des** keyword was changed to **des-cbc**.
- Keywords for the preferred key exchange algorithm **prefer-kex**:
  - The **dh-group-exchange** keyword was changed to **dh-group-exchange-sha1**.
  - The **dh-group1** keyword was changed to **dh-group1-sha1**.
  - The **dh-group14** keyword was changed to **dh-group14-sha1**.
- Keywords for the preferred server-to-client encryption algorithm **prefer-stoc-cipher**:
  - The **3des** keyword was changed to **3des-cbc**.
  - The **aes128** keyword was changed to **aes128-cbc**.
  - The **aes256** keyword was changed to **aes256-cbc**.
  - The **des** keyword was changed to **des-cbc**.

The default settings for the following algorithms were changed:

- For the preferred client-to-server encryption algorithm **prefer-ctos-cipher**:
  - Before modification: The default is **aes128.**
  - After modification: The default is **aes128-ctr**.
- For the preferred client-to-server HMAC algorithm **prefer-ctos-hmac**:
  - Before modification: The default is **sha1**.
  - After modification: The default is **sha2-256**.
- For the preferred key exchange algorithm **prefer-kex**:
  - Before modification: The default is **dh-group-exchange** in non-FIPS mode and is **dh-group14** in FIPS mode.
  - After modification: The default is **ecdh-sha2-nistp256** in both non-FIPS mode and FIPS mode.
- For the preferred server-to-client encryption algorithm **prefer-stoc-cipher**:
  - Before modification: The default is **aes128**.
  - After modification: The default is **aes128-ctr**.
- For the preferred server-to-client HMAC algorithm **prefer-stoc-hmac**:
  - Before modification: The default is **sha1**.
  - After modification: The default is **sha2-256**.

Modified command: scp ipv6

Old syntax

In non-FIPS mode:

scp ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] { **put | get** } *source-file-name* [*destination-file-name*] [**identity-key** { **dsa | ecdsa | rsa** } **| prefer-compress zlib | prefer-ctos-cipher** { **3des | aes128 | aes256 | des** } **| prefer-ctos-hmac** { **md5 | md5-96 | sha1 | sha1-96** } **| prefer-kex** { **dh-group-exchange | dh-group1 | dh-group14** } **| prefer-stoc-cipher** { **3des | aes128 | aes256 | des** } **| prefer-stoc-hmac** { **md5 | md5-96 | sha1 | sha1-96** }] * [**public-key** *keyname* **| source** { **interface** *interface-type interface-number* **| ipv6** *ipv6-address* }] *

In FIPS mode:

scp ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] { **put | get** } *source-file-name* [*destination-file-name*] [**identity-key** { **ecdsa | rsa** } **| prefer-compress zlib | 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** }] * [**public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

New syntax

In non-FIPS mode:

scp ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **dsa** | **ecdsa** | **rsa** | { **x509v3-ecdsa-sha2-nistp384** | **x509v3-ecdsa-sha2-nistp256** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [{ **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

In FIPS mode:

scp ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **ecdsa** | **rsa** | { **x509v3-ecdsa-sha2-nistp384** | **x509v3-ecdsa-sha2-nistp256** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **aes128-cbc** | **aes256-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **aes128-cbc** | **aes256-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [{ **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

Views

User view

Change description

The following keywords were added:

- Keywords for specifying PKI domains used in certificate verification:
  - **pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. When the public key algorithm is x509v3 (**x509v3-ecdsa-sha2-nistp256** or **x509v3-ecdsa-sha2-nistp384**), you must specify this option for the client to get the correct local certificate.
  - **server-pki-domain** *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

    The PKI domain name cannot contain characters in the following table:

<table>
<tr><th>Character name</th><th>Symbol</th><th>Character name</th><th>Symbol</th></tr>
<tr><td>Tilde</td><td>~</td><td>Dot</td><td>.</td></tr>
<tr><td>Asterisk</td><td>*</td><td>Left angle bracket</td><td><</td></tr>
<tr><td>Backslash</td><td>\</td><td>Right angle bracket</td><td>></td></tr>
<tr><td>Vertical bar</td><td>|</td><td>Quotation marks</td><td>"</td></tr>
<tr><td>Colon</td><td>:</td><td>Apostrophe</td><td>'</td></tr>
</table>

- Keywords for specifying the publickey algorithms used in publickey authentication:

- **x509v3-ecdsa-sha2-nistp256**: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp256**.
- **x509v3-ecdsa-sha2-nistp384**: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp384**.

- Keywords for specifying the preferred client-to-server encryption algorithms:
  - **aes128-ctr**: Specifies the encryption algorithm **aes128-ctr**.
  - **aes192-ctr**: Specifies the encryption algorithm **aes192-ctr**.
  - **aes256-ctr**: Specifies the encryption algorithm **aes256-ctr**.
  - **aes256-gcm**: Specifies the encryption algorithm **aes256-gcm**.
  - **aes128-gcm**: Specifies the encryption algorithm **aes128-gcm**.
- Keywords for specifying the preferred client-to-server HMAC algorithms:
  - **sha2-256**: Specifies the HMAC algorithm **sha2-256**.
  - **sha2-512**: Specifies the HMAC algorithm **sha2-512**.
- Keywords for specifying the preferred key exchange algorithms:
  - **ecdh-sha2-nistp256**: Specifies the key exchange algorithm **ecdh-sha2-nistp256**.
  - **ecdh-sha2-nistp384**: Specifies the key exchange algorithm **ecdh-sha2-nistp384**.

The following keywords were modified:

- Keywords for the preferred client-to-server encryption algorithm **prefer-ctos-cipher**:
  - The **3des** keyword was changed to **3des-cbc**.
  - The **aes128** keyword was changed to **aes128-cbc**.
  - The **aes256** keyword was changed to **aes256-cbc**.
  - The **des** keyword was changed to **des-cbc**.
- Keywords for the preferred key exchange algorithm **prefer-kex**:
  - The **dh-group-exchange** keyword was changed to **dh-group-exchange-sha1**.
  - The **dh-group1** keyword was changed to **dh-group1-sha1**.
  - The **dh-group14** keyword was changed to **dh-group14-sha1**.
- Keywords for the preferred server-to-client encryption algorithm **prefer-stoc-cipher**:
  - The **3des** keyword was changed to **3des-cbc**.
  - The **aes128** keyword was changed to **aes128-cbc**.
  - The **aes256** keyword was changed to **aes256-cbc**.
  - The **des** keyword was changed to **des-cbc**.

The default settings for the following algorithms were changed:

- For the preferred client-to-server encryption algorithm **prefer-ctos-cipher**:
  - Before modification: The default is **aes128**.
  - After modification: The default is **aes128-ctr**.
- For the preferred client-to-server HMAC algorithm **prefer-ctos-hmac**:
  - Before modification: The default is **sha1**.
  - After modification: The default is **sha2-256**.
- For the preferred key exchange algorithm **prefer-kex**:
  - Before modification: The default is **dh-group-exchange** in non-FIPS mode and is **dh-group14** in FIPS mode.
  - After modification: The default is **ecdh-sha2-nistp256** in both non-FIPS mode and FIPS mode.
- For the preferred server-to-client encryption algorithm **prefer-stoc-cipher**:

- Before modification: The default is **aes128**.
- After modification: The default is **aes128-ctr**.

- For the preferred server-to-client HMAC algorithm **prefer-stoc-hmac**:
  - Before modification: The default is **sha1**.
  - After modification: The default is **sha2-256**.

Modified command: sftp

Old syntax

In non-FIPS mode:

sftp *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa** | **ecdsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des** | **aes128** | **aes256** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **aes256** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

In FIPS mode:

sftp *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **ecdsa** | **rsa** } | **prefer-compress zlib** | **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** }] * [**public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

New syntax

In non-FIPS mode:

sftp *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa** | **ecdsa** | **rsa** | { **x509v3-ecdsa-sha2-nistp384** | **x509v3-ecdsa-sha2-nistp256** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [**dscp** *dscp-value* | { **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

In FIPS mode:

sftp *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **ecdsa** | **rsa** | { **x509v3-ecdsa-sha2-nistp384** | **x509v3-ecdsa-sha2-nistp256** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **aes128-cbc** | **aes256-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **aes128-cbc** | **aes256-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [{ **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

Views

User view

Change description

The following keywords were added:

- Keywords for specifying PKI domains used in certificate verification:

- **pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. When the public key algorithm is x509v3 (**x509v3-ecdsa-sha2-nistp256** or **x509v3-ecdsa-sha2-nistp384**), you must specify this option for the client to get the correct local certificate.
- **server-pki-domain** *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

  The PKI domain name cannot contain characters in the following table:

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

- Keywords for specifying the publickey algorithms used in publickey authentication:
  - **x509v3-ecdsa-sha2-nistp256**: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp256**.
  - **x509v3-ecdsa-sha2-nistp384**: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp384**.
- Keywords for specifying the preferred client-to-server encryption algorithms:
  - **aes128-ctr**: Specifies the encryption algorithm **aes128-ctr**.
  - **aes192-ctr**: Specifies the encryption algorithm **aes192-ctr**.
  - **aes256-ctr**: Specifies the encryption algorithm **aes256-ctr**.
  - **aes256-gcm**: Specifies the encryption algorithm **aes256-gcm**.
  - **aes128-gcm**: Specifies the encryption algorithm **aes128-gcm**.
- Keywords for specifying the preferred client-to-server HMAC algorithms:
  - **sha2-256**: Specifies the HMAC algorithm **sha2-256**.
  - **sha2-512**: Specifies the HMAC algorithm **sha2-512**.
- Keywords for specifying the preferred key exchange algorithms:
  - **ecdh-sha2-nistp256**: Specifies the key exchange algorithm **ecdh-sha2-nistp256**.
  - **ecdh-sha2-nistp384**: Specifies the key exchange algorithm **ecdh-sha2-nistp384**.

The following keywords were modified:

- Keywords for the preferred client-to-server encryption algorithm **prefer-ctos-cipher**:
  - The **3des** keyword was changed to **3des-cbc**.
  - The **aes128** keyword was changed to **aes128-cbc**.
  - The **aes256** keyword was changed to **aes256-cbc**.
  - The **des** keyword was changed to **des-cbc**.
- Keywords for the preferred key exchange algorithm **prefer-kex**:
  - The **dh-group-exchange** keyword was changed to **dh-group-exchange-sha1**.
  - The **dh-group1** keyword was changed to **dh-group1-sha1**.
  - The **dh-group14** keyword was changed to **dh-group14-sha1**.
- Keywords for the preferred server-to-client encryption algorithm **prefer-stoc-cipher**:
  - The **3des** keyword was changed to **3des-cbc**.

- The **aes128** keyword was changed to **aes128-cbc**.
- The **aes256** keyword was changed to **aes256-cbc**.
- The **des** keyword was changed to **des-cbc**.

The default settings for the following algorithms were changed:

- For the preferred client-to-server encryption algorithm **prefer-ctos-cipher**:
  - Before modification: The default is **aes128**.
  - After modification: The default is **aes128-ctr**.
- For the preferred client-to-server HMAC algorithm **prefer-ctos-hmac**:
  - Before modification: The default is **sha1**.
  - After modification: The default is **sha2-256**.
- For the preferred key exchange algorithm **prefer-kex**:
  - Before modification: The default is **dh-group-exchange** in non-FIPS mode and is **dh-group14** in FIPS mode.
  - After modification: The default is **ecdh-sha2-nistp256** in both non-FIPS mode and FIPS mode.
- For the preferred server-to-client encryption algorithm **prefer-stoc-cipher**:
  - Before modification: The default is **aes128**.
  - After modification: The default is **aes128-ctr**.
- For the preferred server-to-client HMAC algorithm **prefer-stoc-hmac**:
  - Before modification: The default is **sha1**.
  - After modification: The default is **sha2-256**.

Modified command: sftp ipv6

Old syntax

In non-FIPS mode:

sftp ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] [**identity-key** { **dsa** | **ecdsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des** | **aes128** | **aes256** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **aes256** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

In FIPS mode:

sftp ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] [**identity-key** { **ecdsa** | **rsa** } | **prefer-compress zlib** | **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** }] * [**public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

New syntax

In non-FIPS mode:

sftp ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] [**identity-key** { **dsa** | **ecdsa** | **rsa** | { **x509v3-ecdsa-sha2-nistp384** | **x509v3-ecdsa-sha2-nistp256** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** |

aes256-gcm } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [**dscp** *dscp-value* | { **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

In FIPS mode:

sftp ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] [**identity-key** { **ecdsa** | **rsa** | { **x509v3-ecdsa-sha2-nistp384** | **x509v3-ecdsa-sha2-nistp256** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **aes128-cbc** | **aes256-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **aes128-cbc** | **aes256-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [{ **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

Views

User view

Change description

The following keywords were added:

- Keywords for specifying PKI domains used in certificate verification:
  - **pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. When the public key algorithm is x509v3 (**x509v3-ecdsa-sha2-nistp256** or **x509v3-ecdsa-sha2-nistp384**), you must specify this option for the client to get the correct local certificate.
  - **server-pki-domain** *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

    The PKI domain name cannot contain characters in the following table:

<table>
<tr><th>Character name</th><th>Symbol</th><th>Character name</th><th>Symbol</th></tr>
<tr><td>Tilde</td><td>~</td><td>Dot</td><td>.</td></tr>
<tr><td>Asterisk</td><td>*</td><td>Left angle bracket</td><td><</td></tr>
<tr><td>Backslash</td><td>\</td><td>Right angle bracket</td><td>></td></tr>
<tr><td>Vertical bar</td><td>|</td><td>Quotation marks</td><td>"</td></tr>
<tr><td>Colon</td><td>:</td><td>Apostrophe</td><td>'</td></tr>
</table>

- Keywords for specifying the publickey algorithms used in publickey authentication:
  - **x509v3-ecdsa-sha2-nistp256**: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp256**.
  - **x509v3-ecdsa-sha2-nistp384**: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp384**.
- Keywords for specifying the preferred client-to-server encryption algorithms:
  - **aes128-ctr**: Specifies the encryption algorithm **aes128-ctr**.
  - **aes192-ctr**: Specifies the encryption algorithm **aes192-ctr**.
  - **aes256-ctr**: Specifies the encryption algorithm **aes256-ctr**.
  - **aes256-gcm**: Specifies the encryption algorithm **aes256-gcm**.
  - **aes128-gcm**: Specifies the encryption algorithm **aes128-gcm**.
- Keywords for specifying the preferred client-to-server HMAC algorithms:

- **sha2-256**: Specifies the HMAC algorithm **sha2-256**.
- **sha2-512**: Specifies the HMAC algorithm **sha2-512**.

- Keywords for specifying the preferred key exchange algorithms:
  - **ecdh-sha2-nistp256**: Specifies the key exchange algorithm **ecdh-sha2-nistp256.**
  - **ecdh-sha2-nistp384**: Specifies the key exchange algorithm **ecdh-sha2-nistp384.**

The following keywords were modified:

- Keywords for the preferred client-to-server encryption algorithm **prefer-ctos-cipher**:
  - The **3des** keyword was changed to **3des-cbc**.
  - The **aes128** keyword was changed to **aes128-cbc**.
  - The **aes256** keyword was changed to **aes256-cbc**.
  - The **des** keyword was changed to **des-cbc**.
- Keywords for the preferred key exchange algorithm **prefer-kex**:
  - The **dh-group-exchange** keyword was changed to **dh-group-exchange-sha1**.
  - The **dh-group1** keyword was changed to **dh-group1-sha1.**
  - The **dh-group14** keyword was changed to **dh-group14-sha1**.
- Keywords for the preferred server-to-client encryption algorithm **prefer-stoc-cipher**:
  - The **3des** keyword was changed to **3des-cbc**.
  - The **aes128** keyword was changed to **aes128-cbc**.
  - The **aes256** keyword was changed to **aes256-cbc**.
  - The **des** keyword was changed to **des-cbc**.

The default settings for the following algorithms were changed:

- For the preferred client-to-server encryption algorithm **prefer-ctos-cipher**:
  - Before modification: The default is **aes128.**
  - After modification: The default is **aes128-ctr.**
- For the preferred client-to-server HMAC algorithm **prefer-ctos-hmac**:
  - Before modification: The default is **sha1.**
  - After modification: The default is **sha2-256.**
- For the preferred key exchange algorithm **prefer-kex**:
  - Before modification: The default is **dh-group-exchange** in non-FIPS mode and is **dh-group14** in FIPS mode.
  - After modification: The default is **ecdh-sha2-nistp256** in both non-FIPS mode and FIPS mode.
- For the preferred server-to-client encryption algorithm **prefer-stoc-cipher**:
  - Before modification: The default is **aes128.**
  - After modification: The default is **aes128-ctr**.
- For the preferred server-to-client HMAC algorithm **prefer-stoc-hmac**:
  - Before modification: The default is **sha1.**
  - After modification: The default is **sha2-256.**

Modified command: ssh2

Old syntax

In non-FIPS mode:

ssh2 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa | ecdsa | rsa** } **| prefer-compress zlib | prefer-ctos-cipher** { **3des | aes128 | aes256 | des** } **| prefer-ctos-hmac** { **md5 | md5-96 | sha1 | sha1-96** } **| prefer-kex** { **dh-group-exchange | dh-group1 | dh-group14** } **| prefer-stoc-cipher** { **3des | aes128 | aes256 | des** } **| prefer-stoc-hmac** { **md5 | md5-96 | sha1 | sha1-96** }] * [**dscp** *dscp-value* **| escape** *character* **| public-key** *keyname* **| source** { **interface** *interface-type interface-number* **| ip** *ip-address* }] *

In FIPS mode:

ssh2 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **ecdsa | rsa** } **| prefer-compress zlib | 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** }] * [**escape** *character* **| public-key** *keyname* **| source** { **interface** *interface-type interface-number* **| ip** *ip-address* }] *

New syntax

In non-FIPS mode:

ssh2 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa | ecdsa | rsa |** { **x509v3-ecdsa-sha2-nistp384 | x509v3-ecdsa-sha2-nistp256** } **pki-domain** *domain-name* } **| prefer-compress zlib | prefer-ctos-cipher** { **3des-cbc | aes128-cbc | aes256-cbc | des-cbc | aes128-ctr | aes192-ctr | aes256-ctr | aes128-gcm | aes256-gcm** } **| prefer-ctos-hmac** { **md5 | md5-96 | sha1 | sha1-96 | sha2-256 | sha2-512** } **| prefer-kex** { **dh-group-exchange-sha1 | dh-group1-sha1 | dh-group14-sha1 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384** } **| prefer-stoc-cipher** { **3des-cbc | aes128-cbc | aes256-cbc | des-cbc | aes128-ctr | aes192-ctr | aes256-ctr | aes128-gcm | aes256-gcm** } **| prefer-stoc-hmac** { **md5 | md5-96 | sha1 | sha1-96 | sha2-256 | sha2-512** }] * [**dscp** *dscp-value* **| escape** *character* **|** { **public-key** *keyname* **| server-pki-domain** *domain-name* } **| source** { **interface** *interface-type interface-number* **| ip** *ip-address* }] *

In FIPS mode:

ssh2 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **ecdsa | rsa |** { **x509v3-ecdsa-sha2-nistp384 | x509v3-ecdsa-sha2-nistp256** } **pki-domain** *domain-name* } **| prefer-compress zlib | prefer-ctos-cipher** { **aes128-cbc | aes256-cbc | aes128-ctr | aes192-ctr | aes256-ctr | aes128-gcm | aes256-gcm** } **| prefer-ctos-hmac** { **sha1 | sha1-96 | sha2-256 | sha2-512** } **| prefer-kex** { **dh-group14-sha1 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384** } **| prefer-stoc-cipher** { **aes128-cbc | aes256-cbc | aes128-ctr | aes192-ctr | aes256-ctr | aes128-gcm | aes256-gcm** } **| prefer-stoc-hmac** { **sha1 | sha1-96 | sha2-256 | sha2-512** }] * [**escape** *character* **|** { **public-key** *keyname* **| server-pki-domain** *domain-name* } **| source** { **interface** *interface-type interface-number* **| ip** *ip-address* }] *

Views

User view

Change description

The following keywords were added:

- Keywords for specifying PKI domains used in certificate verification:
  - **pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. When the public key algorithm is x509v3 (**x509v3-ecdsa-sha2-nistp256** or **x509v3-ecdsa-sha2-nistp384**), you must specify this option for the client to get the correct local certificate.
  - **server-pki-domain** *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

    The PKI domain name cannot contain characters in the following table:

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

- Keywords for specifying the publickey algorithms used in publickey authentication:
  - **x509v3-ecdsa-sha2-nistp256**: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp256**.
  - **x509v3-ecdsa-sha2-nistp384**: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp384**.
- Keywords for specifying the preferred client-to-server encryption algorithms:
  - **aes128-ctr**: Specifies the encryption algorithm **aes128-ctr**.
  - **aes192-ctr**: Specifies the encryption algorithm **aes192-ctr**.
  - **aes256-ctr**: Specifies the encryption algorithm **aes256-ctr**.
  - **aes256-gcm**: Specifies the encryption algorithm **aes256-gcm**.
  - **aes128-gcm**: Specifies the encryption algorithm **aes128-gcm**.
- Keywords for specifying the preferred client-to-server HMAC algorithms:
  - **sha2-256**: Specifies the HMAC algorithm **sha2-256**.
  - **sha2-512**: Specifies the HMAC algorithm **sha2-512**.
- Keywords for specifying the preferred key exchange algorithms:
  - **ecdh-sha2-nistp256**: Specifies the key exchange algorithm **ecdh-sha2-nistp256**.
  - **ecdh-sha2-nistp384**: Specifies the key exchange algorithm **ecdh-sha2-nistp384**.

The following keywords were modified:

- Keywords for the preferred client-to-server encryption algorithm **prefer-ctos-cipher**:
  - The **3des** keyword was changed to **3des-cbc**.
  - The **aes128** keyword was changed to **aes128-cbc**.
  - The **aes256** keyword was changed to **aes256-cbc**.
  - The **des** keyword was changed to **des-cbc**.
- Keywords for the preferred key exchange algorithm **prefer-kex**:
  - The **dh-group-exchange** keyword was changed to **dh-group-exchange-sha1**.
  - The **dh-group1** keyword was changed to **dh-group1-sha1**.
  - The **dh-group14** keyword was changed to **dh-group14-sha1**.
- Keywords for the preferred server-to-client encryption algorithm **prefer-stoc-cipher**:
  - The **3des** keyword was changed to **3des-cbc**.
  - The **aes128** keyword was changed to **aes128-cbc**.
  - The **aes256** keyword was changed to **aes256-cbc**.
  - The **des** keyword was changed to **des-cbc**.

The default settings for the following algorithms were changed:

- For the preferred client-to-server encryption algorithm **prefer-ctos-cipher**:
  - Before modification: The default is **aes128**.
  - After modification: The default is **aes128-ctr**.

* For the preferred client-to-server HMAC algorithm **prefer-ctos-hmac**:
    * Before modification: The default is **sha1**.
    * After modification: The default is **sha2-256**.
* For the preferred key exchange algorithm **prefer-kex**:
    * Before modification: The default is **dh-group-exchange** in non-FIPS mode and is **dh-group14** in FIPS mode.
    * After modification: The default is **ecdh-sha2-nistp256** in both non-FIPS mode and FIPS mode.
* For the preferred server-to-client encryption algorithm **prefer-stoc-cipher**:
    * Before modification: The default is **aes128**.
    * After modification: The default is **aes128-ctr**.
* For the preferred server-to-client HMAC algorithm **prefer-stoc-hmac**:
    * Before modification: The default is **sha1**.
    * After modification: The default is **sha2-256**.

Modified command: ssh2 ipv6

Old syntax

In non-FIPS mode:

ssh2 ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] [**identity-key** { **dsa** | **ecdsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des** | **aes128** | **aes256** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **aes256** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **escape** *character* | **public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

In FIPS mode:

ssh2 ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] [**identity-key** { **ecdsa** | **rsa** } | **prefer-compress zlib** | **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** }] * [**escape** *character* | **public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

New syntax

In non-FIPS mode:

ssh2 ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] [**identity-key** { **dsa** | **ecdsa** | **rsa** | { **x509v3-ecdsa-sha2-nistp384** | **x509v3-ecdsa-sha2-nistp256** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [**dscp** *dscp-value* | **escape** *character* | { **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

In FIPS mode:

ssh2 ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] [**identity-key** { **ecdsa** | **rsa** | { **x509v3-ecdsa-sha2-nistp384** |

x509v3-ecdsa-sha2-nistp256 } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **aes128-cbc** | **aes256-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **aes128-cbc** | **aes256-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [**escape** *character* | { **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

Views

User view

Change description

The following keywords were added:

- Keywords for specifying PKI domains used in certificate verification:
  - **pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. When the public key algorithm is x509v3 (**x509v3-ecdsa-sha2-nistp256** or **x509v3-ecdsa-sha2-nistp384**), you must specify this option for the client to get the correct local certificate.
  - **server-pki-domain** *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

    The PKI domain name cannot contain characters in the following table:

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

- Keywords for specifying the publickey algorithms used in publickey authentication:
  - **x509v3-ecdsa-sha2-nistp256**: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp256**.
  - **x509v3-ecdsa-sha2-nistp384**: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp384**.
- Keywords for specifying the preferred client-to-server encryption algorithms:
  - **aes128-ctr**: Specifies the encryption algorithm **aes128-ctr**.
  - **aes192-ctr**: Specifies the encryption algorithm **aes192-ctr**.
  - **aes256-ctr**: Specifies the encryption algorithm **aes256-ctr**.
  - **aes256-gcm**: Specifies the encryption algorithm **aes256-gcm**.
  - **aes128-gcm**: Specifies the encryption algorithm **aes128-gcm**.
- Keywords for specifying the preferred client-to-server HMAC algorithms:
  - **sha2-256**: Specifies the HMAC algorithm **sha2-256**.
  - **sha2-512**: Specifies the HMAC algorithm **sha2-512**.
- Keywords for specifying the preferred key exchange algorithms:
  - **ecdh-sha2-nistp256**: Specifies the key exchange algorithm **ecdh-sha2-nistp256**.
  - **ecdh-sha2-nistp384**: Specifies the key exchange algorithm **ecdh-sha2-nistp384**.

The following keywords were modified:

- Keywords for the preferred client-to-server encryption algorithm **prefer-ctos-cipher**:
  - The **3des** keyword was changed to **3des-cbc**.
  - The **aes128** keyword was changed to **aes128-cbc**.
  - The **aes256** keyword was changed to **aes256-cbc**.
  - The **des** keyword was changed to **des-cbc**.
- Keywords for the preferred key exchange algorithm **prefer-kex**:
  - The **dh-group-exchange** keyword was changed to **dh-group-exchange-sha1**.
  - The **dh-group1** keyword was changed to **dh-group1-sha1**.
  - The **dh-group14** keyword was changed to **dh-group14-sha1**.
- Keywords for the preferred server-to-client encryption algorithm **prefer-stoc-cipher**:
  - The **3des** keyword was changed to **3des-cbc**.
  - The **aes128** keyword was changed to **aes128-cbc**.
  - The **aes256** keyword was changed to **aes256-cbc**.
  - The **des** keyword was changed to **des-cbc**.

The default settings for the following algorithms were changed:

- For the preferred client-to-server encryption algorithm **prefer-ctos-cipher**:
  - Before modification: The default is **aes128**.
  - After modification: The default is **aes128-ctr**.
- For the preferred client-to-server HMAC algorithm **prefer-ctos-hmac**:
  - Before modification: The default is **sha1**.
  - After modification: The default is **sha2-256**.
- For the preferred key exchange algorithm **prefer-kex**:
  - Before modification: The default is **dh-group-exchange** in non-FIPS mode and is **dh-group14** in FIPS mode.
  - After modification: The default is **ecdh-sha2-nistp256** in both non-FIPS mode and FIPS mode.
- For the preferred server-to-client encryption algorithm **prefer-stoc-cipher**:
  - Before modification: The default is **aes128**.
  - After modification: The default is **aes128-ctr**.
- For the preferred server-to-client HMAC algorithm **prefer-stoc-hmac**:
  - Before modification: The default is **sha1**.
  - After modification: The default is **sha2-256**.

New feature: Public key management support for Suite B

Configuring public key management to support Suite B

Suite B contains a set of encryption and authentication algorithms that meet high security requirements. Two local ECDSA key pair generation algorithms were added to the public key management module to support Suite B.

Command reference

Modified command: public-key local create

Old syntax

In non-FIPS mode:

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

In FIPS mode:

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

New syntax

In non-FIPS mode:

public-key local create { **dsa | ecdsa** { **secp192r1 | secp256r1 | secp384r1 | secp521r1** } **| rsa** } [**name** *key-name*]

In FIPS mode:

public-key local create { **dsa | ecdsa** { **secp256r1 | secp384r1 | secp521r1** } **| rsa** } [**name** *key-name*]

Views

System view

Change description

The following keywords were added:

- **secp256r1**: Uses the secp256r1 curve to create an ECDSA key pair with a key modulus length of 256 bits.
- **secp384r1**: Uses the secp384r1 curve to create an ECDSA key pair with a key modulus length of 384 bits.

New feature: PKI support for Suite B

Configuring PKI to support Suite B

Suite B contains a set of encryption and authentication algorithms that meet high security requirements. New commands were added to PKI to support Suite B.

To configure a PKI domain:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a PKI domain and enter its view.	**pki domain** *domain-name*	By default, no PKI domains exist.
3. Specify the ECDSA key pair for certificate request.	**public-key ecdsa name** *key-name* [**secp192r1** | **secp256r1** | **secp384r1** | **secp521r1**]	By default, no key pair is specified.

Command reference

public-key ecdsa

Use **public-key ecdsa** to specify an ECDSA key pair for certificate request.

Use **undo public-key** to restore the default.

Syntax

public-key ecdsa name *key-name* [**secp192r1** | **secp256r1** | **secp384r1** | **secp521r1**]

undo public-key

Default

No key pair is specified for certificate request.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

name *key-name*: Specifies a key pair by its name, a case-insensitive string of 1 to 64 characters. The key pair name can contain only letters, digits, and hyphens (-).

secp192r1: Uses the secp192r1 curve to generate the key pair.

secp256r1: Uses the secp256r1 curve to generate the key pair.

secp384r1: Uses the secp384r1 curve to generate the key pair.

secp521r1: Uses the secp521r1 curve to generate the key pair.

Usage guidelines

You can specify a nonexistent key pair for a PKI domain.

A key pair can be obtained in any of the following ways:

- Use the **public-key local create** command to generate a key pair.
- An application, like IKE using digital signature authentication, triggers the device to generate a key pair.
- Use the **pki import** command to import a certificate containing a key pair.

A PKI domain can have key pairs using only one type of cryptographic algorithm (DSA, ECDSA, or RSA).

If you configure an ECDSA key pair for a PKI domain multiple times, the most recent configuration takes effect.

The specified elliptic curve takes effect only if you specify a nonexistent key pair. The device will automatically create the key pair by using the specified name and curve before submitting a certificate request. The curve parameter is ignored if the specified key pair already exists or is already contained in an imported certificate.

Examples

Specify the ECDSA key pair **abc** for certificate request.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] public-key ecdsa name abc
```

Related commands

- **pki import**
- **public-key local create** (see public key management in *Security Command Reference*)

New feature: SSL support for Suite B

Configuring Suite B in SSL

Suite B contains a set of encryption and authentication algorithms that meet high security requirements.

In this release, Suite B is available in SSL. In addition, a new command was added to display cryptographic library version information on the device.

Command reference

New command: display crypto version

Use **display crypto version** to display cryptographic library version information.

Syntax

display crypto version

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

A cryptographic library version represents a set of cryptographic algorithms.

Examples

Display cryptographic library version information.

```
<Sysname> display crypto version
7.1.3290
```

Table 16 Command output

Field	Description
7.1.3290	Cryptographic library version information, in the format 7.1.*X*: • The value 7.1 represents Comware V700R001. • The value *X* represents the cryptographic library version.

Modified command: ciphersuite

Old syntax

In non-FIPS mode:

ciphersuite { **dhe_rsa_aes_128_cbc_sha** | **dhe_rsa_aes_256_cbc_sha** | **exp_rsa_des_cbc_sha** | **exp_rsa_rc2_md5** | **exp_rsa_rc4_md5** | **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 { **rsa_aes_128_cbc_sha** | **rsa_aes_256_cbc_sha** } *

New syntax

In non-FIPS mode:

ciphersuite { **dhe_rsa_aes_128_cbc_sha** | **dhe_rsa_aes_256_cbc_sha** | **exp_rsa_des_cbc_sha** | **exp_rsa_rc2_md5** | **exp_rsa_rc4_md5** | **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** | **rsa_aes_128_cbc_sha256** | **rsa_aes_256_cbc_sha256** | **dhe_rsa_aes_128_cbc_sha256** | **dhe_rsa_aes_256_cbc_sha256** | **ecdhe_rsa_aes_128_cbc_sha256** | **ecdhe_rsa_aes_256_cbc_sha384** | **ecdhe_rsa_aes_128_gcm_sha256** | **ecdhe_rsa_aes_256_gcm_sha384** | **ecdhe_ecdsa_aes_128_cbc_sha256** | **ecdhe_ecdsa_aes_256_cbc_sha384** | **ecdhe_ecdsa_aes_128_gcm_sha256** | **ecdhe_ecdsa_aes_256_gcm_sha384** } *

In FIPS mode:

cipher { **rsa_aes_128_cbc_sha** | **rsa_aes_256_cbc_sha** | **rsa_aes_128_cbc_sha256** | **rsa_aes_256_cbc_sha256** | **ecdhe_rsa_aes_128_cbc_sha256** | **ecdhe_rsa_aes_256_cbc_sha384** | **ecdhe_rsa_aes_128_gcm_sha256** | **ecdhe_rsa_aes_256_gcm_sha384** | **ecdhe_ecdsa_aes_128_cbc_sha256** | **ecdhe_ecdsa_aes_256_cbc_sha384** | **ecdhe_ecdsa_aes_128_gcm_sha256** | **ecdhe_ecdsa_aes_256_gcm_sha384** } *

Views

SSL server policy view

Change description

The following keywords were added:

- **rsa_aes_128_cbc_sha256**: Specifies the key exchange algorithm RSA, the data encryption algorithm 128-bit AES CBC , and the MAC algorithm SHA256.
- **rsa_aes_256_cbc_sha256**: Specifies the key exchange algorithm RSA, the data encryption algorithm 256-bit AES CBC, and the MAC algorithm SHA256.
- **dhe_rsa_aes_128_cbc_sha256**: Specifies the key exchange algorithm DHE RSA, the data encryption algorithm 128-bit AES CBC, and the MAC algorithm SHA256.
- **dhe_rsa_aes_256_cbc_sha256**: Specifies the key exchange algorithm DHE RSA, the data encryption algorithm 256-bit AES CBC, and the MAC algorithm SHA256.
- **ecdhe_rsa_aes_128_cbc_sha256**: Specifies the key exchange algorithm ECDHE RSA, the data encryption algorithm 128-bit AES CBC, and the MAC algorithm SHA256.
- **ecdhe_rsa_aes_256_cbc_sha384**: Specifies the key exchange algorithm ECDHE RSA, the data encryption algorithm 256-bit AES CBC, and the MAC algorithm SHA384.
- **ecdhe_rsa_aes_128_gcm_sha256**: Specifies the key exchange algorithm ECDHE RSA, the data encryption algorithm 128-bit AES GCM, and the MAC algorithm SHA256.
- **ecdhe_rsa_aes_256_gcm_sha384**: Specifies the key exchange algorithm ECDHE RSA, the data encryption algorithm 256-bit AES GCM, and the MAC algorithm SHA384.
- **ecdhe_ecdsa_aes_128_cbc_sha256**: Specifies the key exchange algorithm ECDHE ECDSA, the data encryption algorithm 128-bit AES CBC, and the MAC algorithm SHA256.
- **ecdhe_ecdsa_aes_256_cbc_sha384**: Specifies the key exchange algorithm ECDHE ECDSA, the data encryption algorithm 256-bit AES CBC, and the MAC algorithm SHA384.
- **ecdhe_ecdsa_aes_128_gcm_sha256**: Specifies the key exchange algorithm ECDHE ECDSA, the data encryption algorithm 128-bit AES GCM, and the MAC algorithm SHA256.
- **ecdhe_ecdsa_aes_256_gcm_sha384**: Specifies the key exchange algorithm ECDHE ECDSA, the data encryption algorithm 256-bit AES GCM, and the MAC algorithm SHA384.

Modified command: prefer-cipher

Old syntax

In non-FIPS mode:

prefer-cipher { **dhe_rsa_aes_128_cbc_sha** | **dhe_rsa_aes_256_cbc_sha** | **exp_rsa_des_cbc_sha** | **exp_rsa_rc2_md5** | **exp_rsa_rc4_md5** | **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:

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

New syntax

In non-FIPS mode:

prefer-cipher { **dhe_rsa_aes_128_cbc_sha** | **dhe_rsa_aes_256_cbc_sha** | **exp_rsa_des_cbc_sha** | **exp_rsa_rc2_md5** | **exp_rsa_rc4_md5** | **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** | **rsa_aes_128_cbc_sha256** | **rsa_aes_256_cbc_sha256** | **dhe_rsa_aes_128_cbc_sha256** | **dhe_rsa_aes_256_cbc_sha256** | **ecdhe_rsa_aes_128_cbc_sha256** | **ecdhe_rsa_aes_256_cbc_sha384** | **ecdhe_rsa_aes_128_gcm_sha256** | **ecdhe_rsa_aes_256_gcm_sha384** | **ecdhe_ecdsa_aes_128_cbc_sha256** | **ecdhe_ecdsa_aes_256_cbc_sha384** | **ecdhe_ecdsa_aes_128_gcm_sha256** | **ecdhe_ecdsa_aes_256_gcm_sha384** }

In FIPS mode:

prefer-cipher { **rsa_aes_128_cbc_sha** | **rsa_aes_256_cbc_sha** | **rsa_aes_128_cbc_sha256** | **rsa_aes_256_cbc_sha256**| **ecdhe_rsa_aes_128_cbc_sha256** |

ecdhe_rsa_aes_256_cbc_sha384 | **ecdhe_rsa_aes_128_gcm_sha256** | **ecdhe_rsa_aes_256_gcm_sha384** | **ecdhe_ecdsa_aes_128_cbc_sha256** | **ecdhe_ecdsa_aes_256_cbc_sha384** | **ecdhe_ecdsa_aes_128_gcm_sha256** | **ecdhe_ecdsa_aes_256_gcm_sha384** }

Views

SSL client policy view

Change description

The following keywords were added:

- **rsa_aes_128_cbc_sha256**: Specifies the key exchange algorithm RSA, the data encryption algorithm 128-bit AES CBC , and the MAC algorithm SHA256.
- **rsa_aes_256_cbc_sha256**: Specifies the key exchange algorithm RSA, the data encryption algorithm 256-bit AES CBC, and the MAC algorithm SHA256.
- **dhe_rsa_aes_128_cbc_sha256**: Specifies the key exchange algorithm DHE RSA, the data encryption algorithm 128-bit AES CBC, and the MAC algorithm SHA256.
- **dhe_rsa_aes_256_cbc_sha256**: Specifies the key exchange algorithm DHE RSA, the data encryption algorithm 256-bit AES CBC, and the MAC algorithm SHA256.
- **ecdhe_rsa_aes_128_cbc_sha256**: Specifies the key exchange algorithm ECDHE RSA, the data encryption algorithm 128-bit AES CBC, and the MAC algorithm SHA256.
- **ecdhe_rsa_aes_256_cbc_sha384**: Specifies the key exchange algorithm ECDHE RSA, the data encryption algorithm 256-bit AES CBC, and the MAC algorithm SHA384.
- **ecdhe_rsa_aes_128_gcm_sha256**: Specifies the key exchange algorithm ECDHE RSA, the data encryption algorithm 128-bit AES GCM, and the MAC algorithm SHA256.
- **ecdhe_rsa_aes_256_gcm_sha384**: Specifies the key exchange algorithm ECDHE RSA, the data encryption algorithm 256-bit AES GCM, and the MAC algorithm SHA384.
- **ecdhe_ecdsa_aes_128_cbc_sha256**: Specifies the key exchange algorithm ECDHE ECDSA, the data encryption algorithm 128-bit AES CBC, and the MAC algorithm SHA256.
- **ecdhe_ecdsa_aes_256_cbc_sha384**: Specifies the key exchange algorithm ECDHE ECDSA, the data encryption algorithm 256-bit AES CBC, and the MAC algorithm SHA384.
- **ecdhe_ecdsa_aes_128_gcm_sha256**: Specifies the key exchange algorithm ECDHE ECDSA, the data encryption algorithm 128-bit AES GCM, and the MAC algorithm SHA256.
- **ecdhe_ecdsa_aes_256_gcm_sha384**: Specifies the key exchange algorithm ECDHE ECDSA, the data encryption algorithm 256-bit AES GCM, and the MAC algorithm SHA384.

Modified command: ssl version disable

Old syntax

ssl version ssl3.0 disable

undo ssl version ssl3.0 disable

New syntax

In non-FIPS mode:

ssl version { **ssl3.0** | **tls1.0** | **tls1.1** } * **disable**

undo ssl version { **ssl3.0** | **tls1.0** | **tls1.1** } * **disable**

In FIPS mode:

ssl version { **tls1.0** | **tls1.1** } * **disable**

undo ssl version { **tls1.0** | **tls1.1** } * **disable**

Views

System view

Change description

The following keywords were added:

- **tls1.0**: Disables TLS 1.0 on the device.
- **tls1.1**: Disables TLS 1.1 on the device.

By default, the device supports TLS 1.0, TLS 1.1, and TLS 1.2 in FIPS mode.

Modified command: version

Old syntax

In non-FIPS mode:

version { **ssl3.0** | **tls1.0** }

In FIPS mode:

version tls1.0

New syntax

In non-FIPS mode:

version { **ssl3.0** | **tls1.0** | **tls1.1** | **tls1.2** }

In FIPS mode:

version { **tls1.0** | **tls1.1** | **tls1.2** }

Views

SSL client policy view

Change description

The following keywords were added:

- **tls1.1**: Specifies TLS 1.0 for the SSL client policy.
- **tls1.2**: Specifies TLS 1.2 for the SSL client policy.

New feature: Disable SSL session renegotiation for the SSL server

Disable SSL session renegotiation for the SSL server

The SSL session renegotiation feature enables the SSL client and server to reuse a previously negotiated SSL session for an abbreviated handshake.

Disabling session renegotiation causes more computational overhead to the system but it can avoid potential risks. Disable SSL session renegotiation only when explicitly required.

To enable the login delay:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Disable SSL session renegotiation for the SSL server.	**ssl renegotiation disable**	By default, SSL session renegotiation is enabled.

Command reference

ssl renegotiation disable

Use **ssl renegotiation disable** to disable SSL session renegotiation.

Use **undo ssl renegotiation disable** to restore the default.

Syntax

ssl renegotiation disable

undo ssl renegotiation disable

Default

SSL session renegotiation is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The SSL session renegotiation feature enables the SSL client and server to reuse a previously negotiated SSL session for an abbreviated handshake.

Disabling session renegotiation causes more computational overhead to the system but it can avoid potential risks. Disable SSL session renegotiation only when explicitly required.

Examples

#Disable SSL session renegotiation.

```
<Sysname> system-view
[Sysname] ssl renegotiation disable
```

New feature: Configuring log suppression for a module

Configuring log suppression for a module

This feature suppresses output of logs. You can use this feature to filter out the logs that you are not concerned with.

Perform this task to configure a log suppression rule to suppress output of all logs or logs with a specific mnemonic value for a module.

The device supports a maximum of 50 log suppression rules.

To configure a log suppression rule for a module:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Configure a log suppression rule for a module.	**info-center logging suppress module** *module-name* **mnemonic** { **all** | *mnemonic-content* }	By default, the device does not suppress output of any logs from any modules.

Command reference

info-center logging suppress module

Use **info-center logging suppress module** to configure a log suppression rule for a module.

Use **undo info-center logging suppress module** to delete a log suppression rule.

Syntax

info-center logging suppress module *module-name* **mnemonic** { **all** | *mnemonic-value* }

undo info-center logging suppress module *module-name* **mnemonic** { **all** | *mnemonic-value* }

Default

The device does not suppress output of any logs from any modules.

Views

System view

Predefined user roles

network-admin

Parameters

module-name: Specifies a log source module by its name, a case-insensitive string of 1 to 8 characters. To view the list of available log source modules, use the **info-center logging suppress module ?** command.

mnemonic: Configures a mnemonic filter for log suppression.

- **all**: Suppresses output of all logs of the module.
- *mnemonic-value*: Suppresses output of logs with the specified mnemonic value. The *mnemonic-value* argument is a case-insensitive string of 1 to 32 characters, which must be the complete value contained in the mnemonic field of the log message. Log suppression will fail if a partial mnemonic value is specified.

Usage guidelines

You can configure log suppression rules to filter out the logs that you are not concerned with. A log suppression rule suppresses output of all logs or only logs with a specific mnemonic value for a module.

The device supports a maximum of 50 log suppression rules.

Examples

Configure a log suppression rule to suppress output of logs with the shell_login mnemonic value for the shell module.

```
<Sysname> system-view
[Sysname] info-center logging suppress module shell mnemonic shell_login
```

Modified feature: Displaying interface information

Feature change description

In this release, you can view the amount of time that has elapsed since the most recent physical state change of an interface.

Command changes

Modified command: display interface

Syntax

display interface [*interface-type*] [**brief** [**down** | **description**]]

display interface [*interface-type* [*interface-number*]] [**brief** [**description**]]

Views

Any view

Change description

The **Last link flapping** field was added to the output from the **display interface** command. This field indicates the amount of time that has elapsed since the most recent physical state change, and displays **Never** if the interface has been physically down since device startup.

Modified feature: Configuring the types of advertisable LLDP TLVs on a port

Feature change description

In this release and later versions, a port can advertise management address TLVs in IPv6 format.

Command changes

Modified command: lldp tlv-enable

Old syntax

In Layer 2 Ethernet interface view or Layer 3 Ethernet interface view:

lldp [**agent** { **nearest-nontpmr** | **nearest-customer** }] **tlv-enable basic-tlv management-address-tlv** [*ip-address*]

In Layer 2 aggregate interface view or Layer 3 aggregate interface view:

lldp agent { **nearest-nontpmr** | **nearest-customer** } **tlv-enable basic-tlv management-address-tlv** [*ip-address*]

New syntax

In Layer 2 Ethernet interface view or Layer 3 Ethernet interface view:

lldp [**agent** { **nearest-nontpmr** | **nearest-customer** }] **tlv-enable basic-tlv management-address-tlv** [**ipv6**] [*ip-address*]

In Layer 2 aggregate interface view or Layer 3 aggregate interface view:

lldp agent { **nearest-nontpmr** | **nearest-customer** } **tlv-enable basic-tlv management-address-tlv** [**ipv6**] [*ip-address*]

Views

Layer 2 Ethernet interface view, Layer 3 Ethernet interface view, Layer 2 aggregate interface view, Layer 3 aggregate interface view

Change description

Before modification: A port cannot advertise management address TLVs in IPv6 format.

After modification: A port can advertise management address TLVs in IPv6 format.

Modified feature: Configuring the device to not change the next hop of routes advertised to EBGP peers

Feature change description

This release added support for the **peer next-hop-invariable** command in BGP VPNv6 address family view.

Command changes

Modified command: peer next-hop-invariable

Syntax

peer { *group-name* **|** *ip-address* [*mask-length*] } **next-hop-invariable**

undo peer { *group-name* **|** *ip-address* [*mask-length*] } **next-hop-invariable**

Views

BGP VPNv4 address family view, BGP VPNv6 address family view

Change description

Before modification: The **peer next-hop-invariable** command is not available in BGP VPNv6 address family view.

After modification: The **peer next-hop-invariable** command is available in BGP VPNv6 address family view.

Modified feature: Specifying RADIUS servers

Feature change description

This release has the following changes:

- The **test-profile** *profile-name* option was added to the **primary authentication** and **secondary authentication** commands in RADIUS scheme view. Use this option to specify a test profile for RADIUS server status detection.
- The **weight** *weight-value* option was added to the following commands in RADIUS scheme view:
  - **primary accounting**.
  - **primary authentication**.
  - **secondary accounting**.
  - **secondary authentication.**

  Use this option to specify the weight value of a RADIUS server for the RADIUS server load sharing feature.

Command changes

Modified command: primary accounting

Old syntax

primary accounting { *host-name* **|** *ipv4-address* **|** **ipv6** *ipv6-address* } [*port-number* **|** **key** { **cipher |** **simple** } *string* **|** **vpn-instance** *vpn-instance-name*] *

New syntax

primary accounting { *host-name* **|** *ipv4-address* **|** **ipv6** *ipv6-address* } [*port-number* **|** **key** { **cipher |** **simple** } *string* **|** **vpn-instance** *vpn-instance-name* **|** **weight** *weight-value*] *

Views

RADIUS scheme view

Change description

The **weight** *weight-value* option was added to this command.

Modified command: primary authentication

Old syntax

primary authentication { *host-name* **|** *ipv4-address* **|** **ipv6** *ipv6-address* } [*port-number* **|** **key** { **cipher** **|** **simple** } *string* **|** **vpn-instance** *vpn-instance-name*] *

New syntax

primary authentication { *host-name* **|** *ipv4-address* **|** **ipv6** *ipv6-address* } [*port-number* **|** **key** { **cipher** **|** **simple** } *string* **|** **test-profile** *profile-name* **|** **vpn-instance** *vpn-instance-name* **|** **weight** *weight-value*] *

Views

RADIUS scheme view

Change description

The **test-profile** *profile-name* and **weight** *weight-value* options were added to this command.

Modified command: secondary accounting

Old syntax

secondary accounting { *host-name* **|** *ipv4-address* **| ipv6** *ipv6-address* } [*port-number* **| key** { **cipher | simple** } *string* **| vpn-instance** *vpn-instance-name*] *

New syntax

secondary accounting { *host-name* **|** *ipv4-address* **| ipv6** *ipv6-address* } [*port-number* **| key** { **cipher | simple** } *string* **| vpn-instance** *vpn-instance-name* **| weight** *weight-value*] *

Views

RADIUS scheme view

Change description

The **weight** *weight-value* option was added to this command.

Modified command: secondary authentication

Old syntax

secondary authentication { *host-name* **|** *ipv4-address* **| ipv6** *ipv6-address* } [*port-number* **| key** { **cipher | simple** } *string* **| vpn-instance** *vpn-instance-name*] *

New syntax

secondary authentication { *host-name* **|** *ipv4-address* **| ipv6** *ipv6-address* } [*port-number* **| key** { **cipher | simple** } *string* **| test-profile** *profile-name* **| vpn-instance** *vpn-instance-name* **| weight** *weight-value*] *

Views

RADIUS scheme view

Change description

The **test-profile** *profile-name* and **weight** *weight-value* options were added to this command.

Modified feature: 802.1X command output

Feature change description

The critical voice VLAN status information was added to the output from the **display dot1x** command, as shown in the following example:

```
<Sysname> display dot1x
Global 802.1X parameters:
   802.1X authentication  : Enabled
   CHAP authentication    : Enabled
   Max-tx period          : 30 s
   Handshake period       : 15 s
```

```
   Quiet timer            : Disabled
       Quiet period       : 60 s
   Supp timeout           : 30 s
   Server timeout         : 100 s
   Reauth period          : 3600 s
   Max auth requests      : 2
   EAD assistant function : Disabled
       EAD timeout        : 30 min
   Domain delimiter       : @
 Max 802.1X users         : 2048 per slot
 Online 802.1X users      : 0

Ten-GigabitEthernet1/0/1  is link-up
   802.1X authentication      : Enabled
   Handshake                  : Enabled
   Handshake security         : Disabled
   Unicast trigger            : Disabled
   Periodic reauth            : Disabled
   Port role                  : Authenticator
   Authorization mode         : Auto
   Port access control        : MAC-based
   Multicast trigger          : Enabled
   Mandatory auth domain      : Not configured
   Guest VLAN                 : Not configured
   Auth-Fail VLAN             : Not configured
   Critical VLAN              : Not configured
   Critical voice VLAN        : Disabled
   Re-auth server-unreachable : Logoff
   Max online users           : 2048

   EAPOL packets: Tx 0, Rx 0
   Sent EAP Request/Identity packets : 0
        EAP Request/Challenge packets: 0
        EAP Success packets: 0
        EAP Failure packets: 0
   Received EAPOL Start packets : 0
            EAPOL LogOff packets: 0
            EAP Response/Identity packets : 0
            EAP Response/Challenge packets: 0
            Error packets: 0
   Online 802.1X users: 0
```

Modified feature: MAC authentication command output

Feature change description

The critical voice VLAN status information was added to the output from the **display mac-authentication** command, as shown in the following example:

```
<Sysname> display mac-authentication
 Global MAC authentication parameters:
   MAC authentication     : Enabled
   User name format       : MAC address in lowercase(xxxxxxxxxxxx)
           Username       : mac
           Password       : Not configured
   Offline detect period  : 300 s
   Quiet period           : 60 s
   Server timeout         : 100 s
   Authentication domain  : Not configured, use default domain
 Max MAC-auth users       : 2048 per slot
 Online MAC-auth users    : 0

 Silent MAC users:
          MAC address       VLAN ID  From port               Port index

 Ten-GigabitEthernet1/0/1  is link-up
   MAC authentication         : Enabled
   Authentication domain      : Not configured
   Auth-delay timer           : Disabled
   Re-auth server-unreachable : Logoff
   Guest VLAN                 : Not configured
   Critical VLAN              : Not configured
   Critical voice VLAN        : Disabled
   Max online users           : 2048
   Authentication attempts    : successful 0, failed 0
   Current online users       : 0
```

MAC address Auth state

Modified feature: Configuring SSH access control

Feature change description

SSH uses ACLs to control access of SSH clients. Keywords for specifying the ACL type were modified.

Command changes

Modified command: ssh server acl

Old syntax

ssh server acl *acl-number*

New syntax

ssh server acl [**mac**] *acl-number*

Views

System view

Change description

Before modification: The value range for the *acl-number* argument is 2000 to 4999.

After modification: The keyword **mac** was added to represent the Layer 2 ACL type.

- If you specify this keyword, the value range for the *acl-number* argument is 4000 to 4999.
- If you do not specify this keyword, an IPv4 ACL is used for access control. Value ranges for the *acl-number* argument are as follows:
    - 2000 to 2999 for IPv4 basic ACLs.
    - 3000 to 3999 for IPv4 advanced ACLs.

Modified command: ssh server ipv6 acl

Old syntax

ssh server ipv6 acl [**ipv6**] *acl-number*

New syntax

ssh server ipv6 acl { **ipv6 | mac** } *acl-number*

Views

System view

Change description

Before modification: The keyword **ipv6** is optional. To use a Layer 2 ACL for access control, do not specify this keyword.

After modification: The keyword **mac** was added to represent the Layer 2 ACL type.

Modified feature: FIPS self-tests

Feature change description

FIPS self-tests were added support for the examination of the Suite B cryptographic algorithms. Suite B is a set of general encryption and authentication algorithms and it can meet high-level security requirements.

Command changes

Modified command: fips self-test

Syntax

fips self-test

Views

System view

Change description

A triggered self-test was added support for the examination of the following algorithms:

- 3DES.
- ECDH.
- RNG.
- GCM.
- GMAC.

The self-test output was changed and displayed as follows:

```
Cryptographic algorithms tests are running.

Slot 1:
Starting Known-Answer tests in the user space.
Known-answer test for 3DES passed.
Known-answer test for SHA1 passed.
Known-answer test for SHA224 passed.
Known-answer test for SHA256 passed.
Known-answer test for SHA384 passed.
Known-answer test for SHA512 passed.
Known-answer test for HMAC-SHA1 passed.
Known-answer test for HMAC-SHA224 passed.
Known-answer test for HMAC-SHA256 passed.
Known-answer test for HMAC-SHA384 passed.
Known-answer test for HMAC-SHA512 passed.
Known-answer test for AES passed.
Known-answer test for RSA(signature/verification) passed.
Pairwise conditional test for RSA(signature/verification) passed.
Pairwise conditional test for RSA(encrypt/decrypt) passed.
Pairwise conditional test for DSA(signature/verification) passed.
Pairwise conditional test for ECDSA(signature/verification) passed.
Known-answer test for ECDH passed.
Known-answer test for random number generator(x931) passed.
Known-answer test for DRBG passed.
Known-Answer tests in the user space passed.
Starting Known-Answer tests in the kernel.
Known-answer test for 3DES passed.
Known-answer test for AES passed.
Known-answer test for HMAC-SHA1 passed.
```

```
Known-answer test for HMAC-SHA256 passed.
Known-answer test for HMAC-SHA384 passed.
Known-answer test for HMAC-SHA512 passed.
Known-answer test for SHA1 passed.
Known-answer test for SHA256 passed.
Known-answer test for SHA384 passed.
Known-answer test for SHA512 passed.
Known-answer test for GCM passed.
Known-answer test for GMAC passed.
Known-Answer tests in the kernel passed.

Cryptographic algorithms tests passed.
```

Release 2422P02

This release has the following changes:

- Modified feature: NTP support for ACL

Modified feature: NTP support for ACL

Feature change description

Before modification:

- You must specify an ACL when you remove the access rights of peer devices to the NTP services on the local device.
- You cannot use an ACL to specify the peer device that can use the authentication ID.

After modification:

- You can choose to specify or to not specify an ACL when you remove the access rights of peer devices to the NTP services on the local device.
- You can use an ACL to specify the peer device that can use the authentication ID.

Command changes

Modified command: undo ntp-service acl

Old syntax

undo ntp-service { **peer** | **query** | **server** | **synchronization** } **acl** *ipv4-acl-number*

New syntax

undo ntp-service { **peer** | **query** | **server** | **synchronization** } [**acl** *ipv4-acl-number*]

Views

System view

Change description

Before modification: The **acl** *ipv4-acl-number* option is required.

After modification: The **acl** *ipv4-acl-number* option is optional.

Modified command: undo ntp-service ipv6 acl

Old syntax

undo ntp-service ipv6 { **peer** | **query** | **server** | **synchronization** } **acl** *ipv6-acl-number*

New syntax

undo ntp-service ipv6 { **peer** | **query** | **server** | **synchronization** } [**acl** *ipv6-acl-number*]

Views

System view

Change description

Before modification: The **acl** *ipv6-acl-number* option is required.

After modification: The **acl** *ipv6-acl-number* option is optional.

Modified command: ntp-service authentication-keyid

Old syntax

ntp-service authentication-keyid *keyid* **authentication-mode** { **hmac-sha-1 | hmac-sha-256 | hmac-sha-384 | hmac-sha-512 | md5** } { **cipher | simple** } *string*

New syntax

ntp-service authentication-keyid *keyid* **authentication-mode** { **hmac-sha-1 | hmac-sha-256 | hmac-sha-384 | hmac-sha-512 | md5** } { **cipher | simple** } *string* [**acl** *ipv4-acl-number* **| ipv6 acl** *ipv6-acl-number*] *

Views

System view

Change description

The **acl** *ipv4-acl-number* and **ipv6 acl** *ipv6-acl-number* options were added to the command.

acl *ipv4-acl-number*: Specifies an IPv4 basic ACL by its number in the range of 2000 to 2999. Only the devices permitted by the ACL can use the authentication ID for authentication.

ipv6 acl *ipv6-acl-number*: Specifies an IPv6 basic ACL by its number in the range of 2000 to 2999. Only the devices permitted by the ACL can use the authentication ID for authentication.

Modified command: sntp authentication-keyid

Old syntax

sntp authentication-keyid *keyid* **authentication-mode** { **hmac-sha-1 | hmac-sha-256 | hmac-sha-384 | hmac-sha-512 | md5** } { **cipher | simple** } *string*

New syntax

sntp authentication-keyid *keyid* **authentication-mode** { **hmac-sha-1 | hmac-sha-256 | hmac-sha-384 | hmac-sha-512 | md5** } { **cipher | simple** } *string* [**acl ipv4-acl-number | ipv6 acl** *ipv6-acl-number*] *

Views

System view

Change description

The **acl** *ipv4-acl-number* and **ipv6 acl** *ipv6-acl-number* options were added to the command.

acl *ipv4-acl-number*: Specifies an IPv4 basic ACL by its number in the range of 2000 to 2999. Only the devices permitted by the ACL can use the authentication ID for authentication.

ipv6 acl *ipv6-acl-number*: Specifies an IPv6 basic ACL by its number in the range of 2000 to 2999. Only the devices permitted by the ACL can use the authentication ID for authentication.

Release 2422P01

This release has the following changes:

- New feature: Peer Zone

New feature: Peer Zone

Configuring a peer zone

This feature allows you to convert a common zone to a peer zone and specify the principal member for the peer zone.

To configure a peer zone:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter VSAN view.	**vsan** *vsan-id*	N/A
3. Create a zone and enter zone view.	**zone name** *zone-name*	By default, no zones exist.
4. Convert the zone to a peer zone and specify the principal member for the peer zone.	**zone-type peer-zone principal-member** *wwn*	By default, a zone is a common zone.

Command reference

zone-type peer-zone

Use **zone-type peer-zone** to convert a common zone to a peer zone and specify the principal member for the peer zone.

Use **undo zone-type peer-zone** to restore the default.

Syntax

zone-type peer-zone principal-member *wwn*

undo zone-type peer-zone

Default

A zone is a common zone.

Views

Zone view

Predefined user roles

network-admin

Parameters

wwn: Specifies the principal member by a WWN, in the format of *xx:xx:xx:xx:xx:xx:xx:xx*, where *x* is a hexadecimal number. The specified principal member must be an N_Port and acts as a target member.

Usage guidelines

This command can be configured only after Smart SAN is enabled for FC/FCoE.

All settings of a zone are deleted when the zone type is changed.

Examples

Convert the common zone **z1** to a peer zone and specify the WWN 20:00:10:00:00:ef:94:00 as the principal member for the peer zone.

```
<Sysname> system-view
[Sysname] vsan 2
[Sysname-vsan2] zone name z1
[Sysname-vsan2-zone-z1] zone-type peer-zone principal-member 20:00:10:00:00:ef:94:00
```

Convert the peer zone **z1** to a common zone.

```
<Sysname> system-view
[Sysname] vsan 2
[Sysname-vsan2] zone name z1
[Sysname-vsan2-zone-z1] undo zone-type peer-zone
```

Related commands

- **zone name**
- **member** (zone view)
- **smartsan enable**

Release 2422

This release has the following changes:

- New feature: Enabling SNMP notifications for new-root election and topology change events
- New feature: Keychain authentication for OSPFv3
- New feature: Configuring keychains
- New feature: Checking sender IP addresses of ARP packets
- New feature: Saving the IP forwarding entries to a file
- New feature: VPN instance for the destination address of a tunnel interface
- New feature: System stability and status displaying
- New feature: Disabling reactivation for edge ports shut down by BPDU guard
- New feature: Support for BPDU guard configuration in interface view
- New feature: Data buffer monitoring
- New feature: Configuring Smart SAN
- New feature: SNMP silence
- New feature: DSCP value for NETCONF over SOAP over HTTP/HTTPS packets
- New feature: MAC authentication offline detection
- New feature: Displaying the maximum number of ARP entries that a device supports
- New feature: Displaying the maximum number of ND entries that a device supports
- New feature: ARP detection logging
- New feature: Attack detection and prevention
- New feature: Configuration commit delay
- New feature: IP address assignment to the management Ethernet port of an IRF member device
- New feature: DHCP snooping logging
- New feature: DHCPv6 snooping logging
- New feature: Logging of BGP route flapping
- New feature: RADIUS DAE server
- New feature: Configuring service loopback group-based remote flow mirroring
- New feature: Display the FCoE configuration of a VLAN
- New feature: Flow entry for filtering slow protocol packets
- New feature: Display the status of a VSAN
- New feature: Setting the operating mode for a VSAN
- New feature: Configuring automatic load balancing for FCoE
- Modified feature: Support for Push-Tag and Pop-Tag in Packet-out messages
- Modified feature: Creating RMON statistics entries
- Modified feature: Creating RMON history control entries
- Modified feature: Automatic configuration
- Modified feature: Disabling advertising prefix information in RA messages
- Modified feature: 802.1X timers
- Modified feature: MAC authentication timers

- Modified feature: Specifying a log host
- Modified feature: Remote file copying
- Modified feature: Multicast VLAN
- Modified feature: Enabling link-aggregation traffic redirection
- Modified feature: TCP maximum segment size (MSS) setting
- Modified feature: Configuring a preemption mode for a smart link group
- Modified feature: Creating a VSAN and entering VSAN view
- Modified feature: Configuring an FCoE mode for the switch
- Modified feature: Setting the mode of a VFC interface
- Modified feature: Setting an FC-MAP value
- Modified feature: Setting an FKA advertisement interval
- Modified feature: Setting the system FCF priority
- Modified feature: Creating an OpenFlow table for an OpenFlow instance
- Modified feature: Frame match criteria of Ethernet service instances

New feature: Enabling SNMP notifications for new-root election and topology change events

Enabling SNMP notifications for new-root election and topology change events

This feature enables the device to generate logs and report new-root election events or spanning tree topology changes to SNMP. For the event notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

When you use the **snmp-agent trap enable stp** [**new-root** | **tc**] command, follow these guidelines:

- The **new-root** keyword applies only to STP, MSTP, and RSTP modes.
- The **tc** keyword applies only to PVST mode.
- In STP, MSTP, or RSTP mode, the **snmp-agent trap enable stp** command enables SNMP notifications for new-root election events.
- In PVST mode, the **snmp-agent trap enable stp** enables SNMP notifications for spanning tree topology changes.

To enable SNMP notifications for new-root election and topology change events:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable SNMP notifications for new-root election events.	In STP, MSTP, or RSTP mode, execute either of the following commands: • **snmp-agent trap enable stp new-root** • **snmp-agent trap enable stp**	The default settings are as follows: • SNMP notifications are disabled for new-root election events. • In MSTP mode, SNMP

Step	Command	Remarks
3. Enable SNMP notifications for spanning tree topology changes.	In PVST mode, execute either of the following commands: • **snmp-agent trap enable stp tc** • **snmp-agent trap enable stp**	notifications are enabled in MSTI 0 and disabled in other MSTIs for spanning tree topology changes. • In PVST mode, SNMP notifications are disabled for spanning tree topology changes in all VLANs.
4. Enable the device to generate a log when it detects or receives a TCN BPDU in PVST mode.	**stp log enable tc**	By default, the device does not generate a log when it detects or receives a TCN BPDU in PVST mode.

Command reference

snmp-agent trap enable stp

Use **snmp-agent trap enable stp** to enable SNMP notifications for new-root election events or spanning tree topology changes.

Use **undo snmp-agent trap enable stp** to disable SNMP notifications for new-root election events or spanning tree topology changes.

Syntax

snmp-agent trap enable stp [**new-root** | **tc**]

undo snmp-agent trap enable stp [**new-root** | **tc**]

Default

SNMP notifications are disabled for new-root election events.

In MSTP mode, SNMP notifications are enabled in MSTI 0 and disabled in other MSTIs for spanning tree topology changes.

In PVST mode, SNMP notifications are disabled for spanning tree topology changes in all VLANs.

Views

System view

Predefined user roles

network-admin

Parameters

new-root: Enables the device to send notifications if the device is elected as a new root bridge. This keyword applies only to STP, MSTP, and RSTP modes.

tc: Enables the device to send traps if the device receives TCN BPDUs. This keyword applies only to PVST mode.

Usage guidelines

If no keyword is specified, the **snmp-agent trap enable stp** command applies to SNMP notifications for different events as follows:

- In STP, MSTP, and RSTP modes, the command applies to SNMP notifications for new-root election events.
- In PVST mode, the command applies to SNMP notifications for spanning tree topology changes.

Examples

Enable SNMP notifications for new-root election events.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable stp new-root
```

Related commands

stp log enable tc

stp log enable tc

Use **stp log enable tc** to enable the device to generate a log when it detects or receives a TCN BPDU in PVST mode.

Use **undo stp log enable tc** to restore the default.

Syntax

stp log enable tc

undo stp log enable tc

Default

In PVST mode, the device does not generate a log when it detects or receives a TCN BPDU.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The command takes effect only in PVST mode.

Examples

Enable the device to generate a log when it detects or receives a TCN BPDU in PVST mode.

```
<Sysname> system-view
[Sysname] stp log enable tc
```

Related commands

snmp-agent trap enable stp

New feature: Keychain authentication for OSPFv3

Configuring keychain authentication for OSPFv3

OSPFv3 uses keychain authentication to prevent routing information from being leaked and routers from being attacked.

OSPFv3 adds the Authentication Trailer option into outgoing packets, and uses the authentication information in the option to authenticate incoming packets. Only packets that pass the authentication can be received. If a packet fails the authentication, the OSPFv3 neighbor relationship cannot be established.

To configure OSPFv3 interface authentication:

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 mode for the interface.	**ospfv3 authentication-mode keychain** *keychain-name* [**instance** *instance-id*]	By default, no authentication is performed on an OSPFv3 interface.

Command reference

ospfv3 authentication-mode

Use **ospfv3 authentication-mode** to specify an authentication mode for an OSPFv3 interface.

Use **undo ospfv3 authentication-mode** to remove the configuration.

Syntax

ospfv3 authentication-mode keychain *keychain-name* [**instance** *instance-id*]

undo ospfv3 authentication-mode [**instance** *instance-id*]

Default

No authentication is performed on an OSPFv3 interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

keychain: Specifies keychain authentication.

keychain-name: Specifies a keychain by its name, a case-sensitive string of 1 to 63 characters.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

When keychain authentication is configured for an OSPFv3 interface, OSPFv3 performs the following operations before sending a packet:

1. Obtains a valid send key from the keychain.

   OSPFv3 does not send the packet if it fails to obtain a valid send key.
2. Uses the key ID, authentication algorithm, and key string to authenticate the packet.

   If the key ID is greater than 255, OSPFv3 does not send the packet.

When keychain authentication is configured for an OSPFv3 interface, OSPFv3 performs the following operations after receiving a packet:

Uses the key ID carried in the packet to obtain a valid accept key from the keychain.

   OSPFv3 discards the packet if it fails to obtain a valid accept key.

3. Uses the authentication algorithm and key string for the valid accept key to authenticate the packet.

   If the authentication fails, OSPFv3 discards the packet.

The ID of keys used for authentication can only be in the range of 0 to 65535.

Examples

Specify the keychain **test** for OSPFv3 packet authentication on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 authentication-mode keychain test
```

New feature: Configuring keychains

Overview

A keychain, a sequence of keys, provides dynamic authentication to ensure secure communication by periodically changing the key and authentication algorithm without service interruption.

Each key in a keychain has a key string, authentication algorithm, sending lifetime, and receiving lifetime. When the system time is within the lifetime of a key in a keychain, an application uses the key to authenticate incoming and outgoing packets. The keys in the keychain take effect one by one according to the sequence of the configured lifetimes. In this way, the authentication algorithms and keys are dynamically changed to implement dynamic authentication.

A keychain operates in absolute time mode. In this mode, each time point during a key's lifetime is the UTC time and is not affected by the system's time zone and daylight saving time.

Configuration procedure

Follow these guidelines when you configure a keychain:

- To make sure only one key in a keychain is used at a time to authenticate packets to a peer, set non-overlapping sending lifetimes for the keys in the keychain.
- The keys used by the local device and the peer device must have the same authentication algorithm and key string.

To configure a keychain:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a keychain and enter keychain view.	**keychain** *keychain-name* [**mode absolute**]	By default, no keychains exist.
3. (Optional.) Set a tolerance time for accept keys in the keychain.	**accept-tolerance** { *value* | **infinite** }	By default, no tolerance time is configured for accept keys in a keychain.
4. Create a key and enter key view.	**key** *key-id*	By default, no keys exist.
5. Specify an authentication algorithm for the key.	**authentication-algorithm hmac-sha-256**	By default, no authentication algorithm is specified for a key.
6. Configure a key string for the key.	**key-string** { **cipher** | **plain** } *string*	By default, no key string is configured.
7. Set the sending lifetime in UTC mode for the key.	**send-lifetime utc** *start-time start-date* { **duration** { *duration-value* | **infinite** } | **to** *end-time end-date* }	By default, the sending lifetime is not configured for a key.
8. Set the receiving lifetime in UTC mode for the key.	**accept-lifetime utc** *start-time*	By default, the receiving lifetime

Step	Command	Remarks
	start-date { **duration** { *duration-value* | **infinite** } | **to** *end-time end-date* }	is not configured for a key.
9. (Optional.) Specify the key as the default send key.	**default-send-key**	By default, no key in a keychain is specified as the default send key.

Displaying and maintaining keychain

Execute **display** commands in any view.

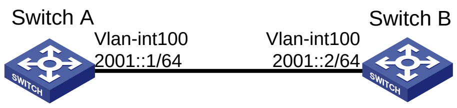
Task	Command
Display keychain information.	**display keychain** [**name** *keychain-name* [**key** *key-id*]]

Keychain configuration example

Network requirements

As shown in Figure 7, establish an OSPFv3 neighbor relationship between Switch A and Switch B, and use a keychain to authenticate packets between the switches. Configure key 1 and key 2 for the keychain and make sure key 2 is used immediately when key 1 expires.

Figure 7 Network diagram



Configuration procedure

Configuring Switch A

Configure IPv6 addresses for interfaces. (Details not shown.)

Configure OSPFv3.

```
<SwitchA> system-view
[SwitchA] ospfv3 1
[SwitchA-ospfv3-1] router-id 1.1.1.1
[SwitchA-ospfv3-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ospfv3 1 area 0
[SwitchA-Vlan-interface100] quit
```

Create a keychain named **abc**, and specify the absolute time mode for it.

```
[SwitchA] keychain abc mode absolute
```

Create key **1** for the keychain **abc**, specify an authentication algorithm, and configure a key string and the sending and receiving lifetimes for the key.

```
[SwitchA-keychain-abc] key 1
[SwitchA-keychain-abc-key-1] authentication-algorithm hmac-sha-256
```

```
[SwitchA-keychain-abc-key-1] key-string plain 123456
[SwitchA-keychain-abc-key-1] send-lifetime utc 10:00:00 2015/02/06 to 11:00:00 2015/02/06
[SwitchA-keychain-abc-key-1] accept-lifetime utc 10:00:00 2015/02/06 to 11:00:00
2015/02/06
[SwitchA-keychain-abc-key-1] quit
```

Create key **2** for the keychain **abc**, specify an authentication algorithm, and configure a key string and the sending and receiving lifetimes for the key.

```
[SwitchA-keychain-abc] key 2
[SwitchA-keychain-abc-key-2] authentication-algorithm hmac-sha-256
[SwitchA-keychain-abc-key-2] key-string plain pwd123
[SwitchA-keychain-abc-key-2] send-lifetime utc 11:00:00 2015/02/06 to 12:00:00 2015/02/06
[SwitchA-keychain-abc-key-2] accept-lifetime utc 11:00:00 2015/02/06 to 12:00:00
2015/02/06
[SwitchA-keychain-abc-key-2] quit
[SwitchA-keychain-abc] quit
```

Configure VLAN-interface 100 to use the keychain **abc** for authentication.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ospfv3 authentication-mode keychain abc
[SwitchA-Vlan-interface100] quit
```

Configuring Switch B

Configure IPv6 addresses for interfaces. (Details not shown.)

Configure OSPFv3.

```
<SwitchB> system-view
[SwitchB] ospfv3 1
[SwitchB-ospfv3-1] router-id 2.2.2.2
[SwitchB-ospfv3-1] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ospfv3 1 area 0
[SwitchB-Vlan-interface100] quit
```

Create a keychain named **abc**, and specify the absolute time mode for it.

```
[SwitchB] keychain abc mode absolute
```

Create key **1** for the keychain **abc**, specify an authentication algorithm, and configure a key string and the sending and receiving lifetimes for the key.

```
[SwitchB-keychain-abc] key 1
[SwitchB-keychain-abc-key-1] authentication-algorithm hmac-sha-256
[SwitchB-keychain-abc-key-1] key-string plain 123456
[SwitchB-keychain-abc-key-1] send-lifetime utc 10:00:00 2015/02/06 to 11:00:00 2015/02/06
[SwitchB-keychain-abc-key-1] accept-lifetime utc 10:00:00 2015/02/06 to 11:00:00
2015/02/06
[SwitchB-keychain-abc-key-1] quit
```

Create key **2** for the keychain **abc**, specify an authentication algorithm, and configure a key string and the sending and receiving lifetimes for the key.

```
[SwitchB-keychain-abc] key 2
[SwitchB-keychain-abc-key-2] authentication-algorithm hmac-sha-256
[SwitchB-keychain-abc-key-2] key-string plain pwd123
[SwitchB-keychain-abc-key-2] send-lifetime utc 11:00:00 2015/02/06 to 12:00:00 2015/02/06
```

```
[SwitchB-keychain-abc-key-2] accept-lifetime utc 11:00:00 2015/02/06 to 12:00:00
2015/02/06
[SwitchB-keychain-abc-key-2] quit
[SwitchB-keychain-abc] quit
```

Configure VLAN-interface 100 to use the keychain **abc** for authentication.

```
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ospfv3 authentication-mode keychain abc
[SwitchB-Vlan-interface100] quit
```

Verifying the configuration

1. When the system time is within the lifetime from 10:00:00 to 11:00:00 on the day 2015/02/06, verify the status of the keys in the keychain **abc**.

   # Display keychain information on Switch A. The output shows that key 1 is the valid key.

```
[SwitchA] display keychain

 Keychain name          : abc
   Mode                 : absolute
   Accept tolerance     : 0
   Default send key ID  : None
   Active send key ID   : 1
   Active accept key IDs: 1

   Key ID               : 1
     Key string         : $c$3$dYTC8QeOKJkwFwP2k/rWL+1p6uMTw3MqNg==
     Algorithm          : hmac-sha-256
     Send lifetime      : 10:00:00 2015/02/06 to 11:00:00 2015/02/06
     Send status        : Active
     Accept lifetime    : 10:00:00 2015/02/06 to 11:00:00 2015/02/06
     Accept status      : Active

   Key ID               : 2
     Key string         : $c$3$7TSPbUxoP1ytOqkdcJ3K3x0BnXEWl4mOEw==
     Algorithm          : hmac-sha-256
     Send lifetime      : 11:00:00 2015/02/06 to 12:00:00 2015/02/06
     Send status        : Inactive
     Accept lifetime    : 11:00:00 2015/02/06 to 12:00:00 2015/02/06
     Accept status      : Inactive
```

   # Display keychain information on Switch B. The output shows that key 1 is the valid key.

```
[SwitchB]display keychain

 Keychain name          : abc
   Mode                 : absolute
   Accept tolerance(min): 0
   Default send key ID  : None
   Active send key ID   : 1
   Active accept key IDs: 1
```

```
  Key ID              : 1
    Key string        : $c$3$/G/Shnh6heXWprlSQy/XDmftHa2JZJBSgg==
    Algorithm         : hmac-sha-256
    Send lifetime     : 10:00:00 2015/02/06 to 11:00:00 2015/02/06
    Send status       : Active
    Accept lifetime   : 10:00:00 2015/02/06 to 11:00:00 2015/02/06
    Accept status     : Active

  Key ID              : 2
    Key string        : $c$3$t4qHAw1hpZYN0JKIEpXPcMFMVT81u0hiOw==
    Algorithm         : hmac-sha-256
    Send lifetime     : 11:00:00 2015/02/06 to 12:00:00 2015/02/06
    Send status       : Inactive
    Accept lifetime   : 11:00:00 2015/02/06 to 12:00:00 2015/02/06
    Accept status     : Inactive
```

2. When the system time is within the lifetime from 11:00:00 to 12:00:00 on the day 2015/02/06, verify the status of the keys in the keychain **abc**.

   # Display keychain information on Switch A. The output shows that key 2 becomes the valid key.

```
[SwitchA]display keychain

 Keychain name          : abc
   Mode                 : absolute
   Accept tolerance     : 0
   Default send key ID  : None
   Active send key ID   : 2
   Active accept key IDs: 2

   Key ID               : 1
     Key string         : $c$3$dYTC8QeOKJkwFwP2k/rWL+1p6uMTw3MqNg==
     Algorithm          : hmac-sha-256
     Send lifetime      : 10:00:00 2015/02/06 to 11:00:00 2015/02/06
     Send status        : Inactive
     Accept lifetime    : 10:00:00 2015/02/06 to 11:00:00 2015/02/06
     Accept status      : Inactive

   Key ID               : 2
     Key string         : $c$3$7TSPbUxoP1ytOqkdcJ3K3x0BnXEWl4mOEw==
     Algorithm          : hmac-sha-256
     Send lifetime      : 11:00:00 2015/02/06 to 12:00:00 2015/02/06
     Send status        : Active
     Accept lifetime    : 11:00:00 2015/02/06 to 12:00:00 2015/02/06
     Accept status      : Active
```

   # Display keychain information on Switch B. The output shows that key 2 becomes the valid key.

```
[SwitchB]display keychain

 Keychain name          : abc
   Mode                 : absolute
```

```
Accept tolerance     : 0
Default send key ID  : None
Active send key ID   : 1
Active accept key IDs: 1

Key ID               : 1
  Key string         : $c$3$/G/Shnh6heXWprlSQy/XDmftHa2JZJBSgg==
  Algorithm          : hmac-sha-256
  Send lifetime      : 10:00:00 2015/02/06 to 11:00:00 2015/02/06
  Send status        : Inactive
  Accept lifetime    : 10:00:00 2015/02/06 to 11:00:00 2015/02/06
  Accept status      : Inactive

Key ID               : 2
  Key string         : $c$3$t4qHAw1hpZYN0JKIEpXPcMFMVT81u0hiOw==
  Algorithm          : hmac-sha-256
  Send lifetime      : 11:00:00 2015/02/06 to 12:00:00 2015/02/06
  Send status        : Active
  Accept lifetime    : 11:00:00 2015/02/06 to 12:00:00 2015/02/06
  Accept status      : Active
```

Command reference

accept-lifetime utc

Use **accept-lifetime utc** to set the receiving lifetime for a key of a keychain in absolute time mode.

Use **undo accept-lifetime** to restore the default.

Syntax

accept-lifetime utc *start-time start-date* { **duration** { *duration-value* **|** **infinite** } **|** **to** *end-time end-date* }

undo accept-lifetime

Default

The receiving lifetime is not configured for a key.

Views

Key view

Predefined user roles

network-admin

Parameters

start-time: Specifies the start time in the HH:MM:SS format. The value range for this argument is 0:0:0 to 23:59:59.

start-date: Specifies the start date in the MM/DD/YYYY or YYYY/MM/DD format. The value range for YYYY is 2000 to 2035.

duration *duration-value*: Specifies the lifetime of the key, in the range of 1 to 2147483646 seconds.

duration infinite: Specifies that the key never expires after it becomes valid.

to: Specifies the end time and date.

end-time: Specifies the end time in the HH:MM:SS format. The value range for this argument is 0:0:0 to 23:59:59.

end-date: Specifies the end date in the MM/DD/YYYY or YYYY/MM/DD format. The value range for YYYY is 2000 to 2035.

Usage guidelines

A key becomes a valid accept key when the following requirements are met:

- A key string has been configured.
- An authentication algorithm has been specified.
- The system time is within the specified receiving lifetime.

If an application receives a packet that carries a key ID, and the key is valid, the application uses the key to authenticate the packet. If the key is not valid, packet authentication fails.

If the received packet does not carry a key ID, the application uses all valid keys in the keychain to authenticate the packet. If the packet does not pass any authentication, packet authentication fails.

An application can use multiple valid keys to authenticate packets received from a peer.

Examples

Set the receiving lifetime for key 1 of the keychain **abc** in absolute time mode.

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] key 1
[Sysname-keychain-abc-key-1] accept-lifetime utc 12:30 2015/1/21 to 18:30 2015/1/21
```

accept-tolerance

Use **accept-tolerance** to set a tolerance time for accept keys in a keychain.

Use **undo accept-tolerance** to restore the default.

Syntax

accept-tolerance { *value* **|** **infinite** }

undo accept-tolerance

Default

No tolerance time is configured for accept keys in a keychain.

Views

Keychain view

Predefined user roles

network-admin

Parameters

value: Specifies a tolerance time in the range of 1 to 8640000 seconds.

infinite: Specifies that the accept keys never expires.

Usage guidelines

After a tolerance time is configured, the start time and the end time configured in the **accept-lifetime utc** command are extended for the period of the tolerance time.

If authentication information is changed, information mismatch occurs on the local and peer devices, and the service might be interrupted. Use this command to ensure continuous packet authentication.

Examples

Set the tolerance time to 100 seconds for accept keys in the keychain **abc**.

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] accept-tolerance 100
```

Configure the accept keys in the keychain **abc** to never expire.

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] accept-tolerance infinite
```

authentication-algorithm

Use **authentication-algorithm** to specify an authentication algorithm for a key.

Use **undo authentication-algorithm** to restore the default.

Syntax

authentication-algorithm hmac-sha-256

undo authentication-algorithm

Default

No authentication algorithm is specified for a key.

Views

Key view

Predefined user roles

network-admin

Parameters

hmac-sha-256: Specifies the HMAC-SHA-256 authentication algorithm.

Usage guidelines

If an application does not support the authentication algorithm specified for a key, the application cannot use the key for packet authentication.

Examples

Specify the HMAC-SHA-256 authentication algorithm for key 1 of the keychain **abc** in absolute time mode.

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] key 1
[Sysname-keychain-abc-key-1] authentication-algorithm hmac-sha-256
```

default-send-key

Use **default-send-key** to specify a key as the default send key.

Use **undo default-send-key** to restore the default.

Syntax

default-send-key

undo default-send-key

Default

No key in a keychain is specified as the default send key.

Views

Key view

Predefined user roles

network-admin

Usage guidelines

When send keys in a keychain are inactive, the default send key can be used for packet authentication.

A keychain can have only one default send key. The default send key must be configured with an authentication algorithm and a key string.

Examples

Specify key **1** in the keychain **abc** as the default send key.

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] key 1
[Sysname-keychain-abc-key-1] default-send-key
```

display keychain

Use **display keychain** to display keychain information.

Syntax

display keychain [**name** *keychain-name* [**key** *key-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *keychain-name*: Specifies a keychain by its name, a case-sensitive string of 1 to 63 characters. If you do not specify a keychain, this command displays information about all keychains.

key *key-id*: Specifies a key by its ID in the range of 0 to 281474976710655. If you do not specify a key, this command displays information about all keys in a keychain.

Examples

Display information about all keychains.

```
<Sysname> display keychain

 Keychain name          : abc
   Mode                 : absolute
   Accept tolerance     : 0
   Default send key ID  : 2 (Inactive)
   Active send key ID   : 1
   Active accept key IDs: 1 2
```

```
Key ID                  : 1
  Key string            : $c$3$vuJpEX3Lah7xcSR2uqmrTK2IZQJZguJh3g==
  Algorithm             : hmac-sha-256
  Send lifetime         : 01:00:00 2015/01/22 to 01:00:00 2015/01/25
  Send status           : Active
  Accept lifetime       : 01:00:00 2015/01/22 to 01:00:00 2015/01/27
  Accept status         : Active

Key ID                  : 2
  Key string            : $c$3$vuJpEX3Lah7xcSR2uqmrTK2IZQJZguJh3g==
  Algorithm             : hmac-sha-256
  Send lifetime         : 01:00:01 2015/01/25 to 01:00:00 2015/01/27
  Send status           : Inactive
  Accept lifetime       : 01:00:00 2015/01/22 to 01:00:00 2015/01/27
  Accept status         : Active
```

Table 17 Command output

Field	Description
Mode	Time mode for the keychain.
Accept tolerance	Tolerance time (in minutes) for accept keys of the keychain.
Default send key ID	ID of the default send key. The status for the key is displayed in parentheses.
Key string	Key string in encrypted form.
Algorithm	Authentication algorithm for the key: **hamc-sha-256**.
Send lifetime	Sending lifetime for the key.
Send status	Status of the send key: **Active** or **Inactive**.
Accept lifetime	Receiving lifetime for the key.
Accept status	Status of the accept key: **Active** or **Inactive**.

key

Use **key** to create a key and enter its view, or enter the view of an existing key.

Use **undo key** to delete a key and all its configurations.

Syntax

key *key-id*

undo key *key-id*

Default

No keys exist.

Views

Keychain view

Predefined user roles

network-admin

Parameters

key-id: Specifies a key ID in the range of 0 to 281474976710655.

Usage guidelines

The keys in a keychain must have different key IDs.

Examples

Create key 1 and enter its view.

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] key 1
[Sysname-keychain-abc-key-1]
```

keychain

Use **keychain** to create a keychain and enter its view, or enter the view of an existing keychain.

Use **undo keychain** to delete a keychain and all its configurations.

Syntax

keychain *keychain-name* [**mode absolute**]

undo keychain *keychain-name*

Default

No keychains exist.

Views

System view

Predefined user roles

network-admin

Parameters

keychain-name: Specifies a keychain name, a case-sensitive string of 1 to 63 characters.

mode: Specifies a time mode.

absolute: Specifies the absolute time mode. In this mode, each time point during a key's lifetime is the UTC time and is not affected by the system's time zone and daylight saving time.

Usage guidelines

You must specify the time mode when you create a keychain. You cannot change the time mode for an existing keychain.

The time mode is not required when you enter the view of an existing keychain.

Examples

Create the keychain **abc**, specify the absolute time mode for it, and enter keychain view.

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc]
```

key-string

Use **key-string** to configure a key string for a key.

Use **undo key-string** to restore the default.

Syntax

key-string { **cipher** | **plain** } *string*

undo key-string

Default

No key string is configured for a key.

Views

Key view

Predefined user roles

network-admin

Parameters

cipher: Specifies a key in encrypted form.

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

string: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 255 characters. Its encrypted form is a case-sensitive string of 33 o 373 characters.

Usage guidelines

If the length of a plaintext key exceeds the length limit supported by an application, the application uses the supported length of the key to authenticate packets.

Examples

Set the key to **123456** in plaintext form for key 1.

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] key 1
[Sysname-keychain-abc-key-1] key-string plain 123456
```

send-lifetime utc

Use **send-lifetime utc** to set the sending lifetime for a key of a keychain in absolute time mode.

Use **undo send-lifetime** to restore the default.

Syntax

send-lifetime utc *start-time start-date* { **duration** { *duration-value* **| infinite** } **| to** *end-time end-date* }

undo send-lifetime

Default

The sending lifetime is not configured for a key.

Views

Key view

Predefined user roles

network-admin

Parameters

start-time: Specifies the start time in the HH:MM:SS format. The value range for this argument is 0:0:0 to 23:59:59.

start-date: Specifies the start date in the MM/DD/YYYY or YYYY/MM/DD format. The value range for YYYY is 2000 to 2035.

duration *duration-value*: Specifies the lifetime of the key, in the range of 1 to 2147483646 seconds.

duration infinite: Specifies that the key never expires after it becomes valid.

to: Specifies the end time and date.

end-time: Specifies the end time in the HH:MM:SS format. The value range for this argument is 0:0:0 to 23:59:59.

end-date: Specifies the end date in the MM/DD/YYYY or YYYY/MM/DD format. The value range for YYYY is 2000 to 2035.

Usage guidelines

A key becomes a valid send key when the following requirements are met:

- A key string has been configured.
- An authentication algorithm has been specified.
- The system time is within the specified sending lifetime.

To make sure only one key in a keychain is used at a time to authenticate packets to a peer, set non-overlapping sending lifetimes for the keys in the keychain.

Examples

Set the sending lifetime for key 1 of the keychain **abc** in absolute time mode.

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] key 1
[Sysname-keychain-abc-key-1] send-lifetime utc 12:30 2015/1/21 to 18:30 2015/1/21
```

New feature: Checking sender IP addresses of ARP packets

Configuring the checking of sender IP addresses for ARP packets

This feature allows a gateway to check the sender IP address of an ARP packet before creating an ARP entry. If the sender IP address is within the allowed IP address range, the gateway creates the ARP entry. If the sender IP address is out of the range, the gateway determines the ARP packet as an attack packet and discards it.

When you specify the sender IP address range for this feature, follow these restrictions and guidelines:

- When a super VLAN is associated with sub-VLANs, to check the ARP packets in the sub-VLANs, you can configure this feature in the sub-VLANs.
- If Layer 3 communication is configured between the specified secondary VLANs associated with a primary VLAN, configure the sender IP address range in the primary VLAN. If Layer 3 communication is not configured between the secondary VLANs associated with a primary VLAN, configure the sender IP address range in the target VLAN.

To configure the checking of sender IP addresses for ARP packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter VLAN view.	**vlan** *vlan-id*	N/A
3. Specify the sender IP address range for checking ARP packets.	**arp sender-ip-range** *start-ip-address end-ip-address*	By default, no sender IP address range is specified for checking ARP packets.

Command reference

arp sender-ip-range

Use **arp sender-ip-range** to specify the sender IP address range for checking ARP packets.

Use **undo arp sender-ip-range** to restore the default.

Syntax

arp sender-ip-range *start-ip-address end-ip-address*

undo arp sender-ip-range

Default

No sender IP address range is specified for checking ARP packets.

Views

VLAN view

Predefined user roles

network-admin

Parameters

start-ip-address: Specifies the start IP address.

end-ip-address: Specifies the end IP address. The end IP address must be higher than or equal to the start IP address.

Usage guidelines

The gateway discards an ARP packet if its sender IP address is not within the allowed IP address range.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the sender IP address range 1.1.1.1 to 1.1.1.20 for checking ARP packets in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname–vlan2] arp sender-ip-range 1.1.1.1 1.1.1.20
```

New feature: Saving the IP forwarding entries to a file

Saving the IP forwarding entries to a file

Step	Command	Remarks
Specify a file to save the IP forwarding entries.	**ip forwarding-table save filename** *filename*	Executing this command triggers one-time saving of the IP forwarding entries. Execute this command in any view.

Command reference

ip forwarding-table save

Use **ip forwarding-table save** to save the IP forwarding entries to a file.

Syntax

ip forwarding-table save filename *filename*

Views

Any view

Predefined user roles

network-admin

Parameters

filename *filename*: Specifies the name of a file, a string of 1 to 255 characters. For information about the *filename* argument, see *Fundamentals Configuration Guide*.

Usage guidelines

The command automatically creates the file if you specify a nonexistent file. If the file already exists, this command overwrites the file content.

To automatically save the IP forwarding entries periodically, configure a schedule for the device to automatically run the **ip forwarding-table save** command. For information about scheduling a task, see *Fundamentals Configuration Guide*.

Examples

Save the IP forwarding entries to the file **fib.txt**.

```
<Sysname> ip forwarding-table save filename fib.txt
```

New feature: VPN instance for the destination address of a tunnel interface

Specifying a VPN instance for the destination address of a tunnel interface

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a tunnel interface, specify the tunnel mode, and enter tunnel interface view.	**interface tunnel** *number* **mode** { **gre** [**ipv6**] | **ipv4-ipv4** | **ipv6** | **ipv6-ipv4** [**6to4** | **isatap**] | **mpls-te** }	By default, no tunnel interfaces exist. When you create a new tunnel interface, you must specify the tunnel mode. When you enter the view of an existing tunnel interface, you do not need to specify the tunnel mode. For packet tunneling to succeed, the two ends of a tunnel must use the same tunnel mode.
3. Specify the VPN instance to which the destination address of the tunnel interface belongs.	**tunnel vpn-instance** *vpn-instance-name*	By default, the tunnel destination belongs to the public network. For a tunnel interface to come up, the tunnel source and destination must belong to the same VPN. To specify a VPN instance for the tunnel source, use the **ip binding vpn-instance** command on the tunnel source interface.

Command reference

tunnel vpn-instance

Use **tunnel vpn-instance** to specify a VPN instance for the destination address of a tunnel interface.

Use **undo tunnel vpn-instance** to restore the default.

Syntax

tunnel vpn-instance *vpn-instance-name*

undo tunnel vpn-instance

Default

The destination address of a tunnel interface belongs to the public network.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

vpn-instance-name: Specifies the name of a VPN instance, a case-sensitive string of 1 to 31 characters.

Usage guidelines

After this command is executed, the device looks up the routing table of the specified VPN instance to forward tunneled packets on the tunnel interface.

For a tunnel interface to come up, the tunnel source and destination must belong to the same VPN. To specify a VPN instance for the tunnel source, use the **ip binding vpn-instance** command on the tunnel source interface.

Examples

Specify the VPN instance **vpn10** for the tunnel destination on interface Tunnel 1.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn10
[Sysname-vpn-instance-vpn10] route-distinguisher 1:1
[Sysname-vpn-instance-vpn10] vpn-target 1:1
[Sysname-vpn-instance-vpn10] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ip binding vpn-instance vpn10
[Sysname-Vlan-interface10] ip address 1.1.1.1 24
[Sysname-Vlan-interface10] quit
[Sysname] interface tunnel 1 mode gre
[Sysname-Tunnel1] source vlan-interface 10
[Sysname-Tunnel1] destination 1.1.1.2
[Sysname-Tunnel1] tunnel vpn-instance vpn10
```

New feature: System stability and status displaying

Displaying system stability and status

Task	Command
Display system stability and status information.	**display system stable state**

Command reference

New command: display system stable state

Use **display system stable state** to display system stability and status information.

Syntax

display system stable state

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Before performing a master/subordinate switchover, use this command to verify that the system is stable. If the **Redundancy Stable** filed does not display **Stable**, you cannot perform a master/subordinate switchover.

At startup, an IRF fabric takes some time to enter **Stable** state. If an IRF fabric cannot enter **Stable** state, use this command to locate the member device that is not in **Stable** state. To locate the instability problem, also use the following commands:

- **display device**—Displays device information to locate member devices that are faulty.
- **display ha service-group**—Displays service group status information to locate the service groups in **Batch Backup** state.
- **display system internal process state**—Displays service operating status information in probe view.

You can use these commands multiple times to observe status changes.

Examples

Display system stability and status information.

```
<Sysname> display system stable state
System state    : Stable
Redundancy state: No redundance
  Slot   CPU   Role      State
  1      0     Active    Stable
```

Table 18 Command output

Field	Description
System state	IRF status: • **Stable**—The IRF fabric is operating stably. • **Not ready**—The IRF fabric is not stable.
Redundancy state	Redundancy status: • **Stable**—The IRF fabric is operating stably. You can perform a master/subordinate switchover. • **No Redundance**—The IRF fabric has only one member device. You cannot perform a master/subordinate switchover. • **Not ready**—The IRF fabric is not stable. You cannot perform a master/subordinate switchover.
Role	Role of the member device in the IRF fabric: • **Active**—Master member. • **Standby**—Subordinate member.
State	Status of the member device: • **Stable**—The member device is operating stably. • **Board Inserted**—The member device has just been installed. • **Kernel Init**—The member device kernel is being initialized. • **Service Starting**—Services are starting on the member device. • **Service Stopping**—Services are stopping on the member device.

Field	Description
	• **HA Batch Backup**—An HA batch backup is in progress on the member device. • **Interface Data Batch Backup**—An interface data batch backup is in progress on the member device.
*	The member device is not operating stably.

New feature: Disabling reactivation for edge ports shut down by BPDU guard

Disabling the device to reactivate edge ports shut down by BPDU guard

A device enabled with BPDU guard shuts down edge ports that have received configuration BPDUs and notifies the NMS of the shutdown event. After a port status detection interval, the device reactivates the shutdown ports. This task disables the device to reactivate the edge ports that are shut down by BPDU guard. For more information about the port status detection interval, see device management configuration in *Fundamentals Configuration Guide*.

This feature takes effect only on edge ports that are shut down by BPDU guard after the feature is configured.

To disable the device to reactivate edge ports shut down by BPDU guard:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Disable the device to reactivate edge ports shut down by BPDU guard.	**stp port shutdown permanent**	By default, a device reactivates the shutdown edge ports after a port status detection interval.

Command reference

stp port shutdown permanent

Use **stp port shutdown permanent** to disable the device to reactivate edge ports shut down by BPDU guard.

Use **undo stp port shutdown permanent** to restore the default.

Syntax

stp port shutdown permanent

undo stp port shutdown permanent

Default

The device reactivates the shutdown edge ports after a port status detection interval.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only on edge ports that are shut down by BPDU guard after the command is executed.

You can use the **shutdown-interval** *time* command to set the port status detection interval after which the device reactivates the shutdown ports. For information about the **shutdown-interval** *time* command, see *Fundamentals Command Reference*.

Examples

Disable a device to reactivate edge ports shut down by BPDU guard.

```
<Sysname> system-view
[Sysname] stp port shutdown permanent
```

New feature: Support for BPDU guard configuration in interface view

Configuring BPDU guard on an interface

Before this release, the device supported only global BPDU guard configuration (**stp bpdu-protection**). Global BPDU guard configuration takes effect on all edge ports. This release allows you to enable or disable BPDU guard on a per-edge port basis.

To configure BPDU guard on an interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.	**interface** *interface-type interface-number*	The specified interface must connect to a user terminal rather than another device or shared LAN segment.
3. Configure BPDU guard on the interface.	**stp port bpdu-protection** { **enable** | **disable** }	By default, BPDU guard is not configured on an interface. BPDU guard is disabled on all edge ports if it is globally disabled. BPDU guard is enabled on all edge ports if it is globally enabled.

Command reference

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 feature is globally enabled. BPDU guard is disabled on the port if the feature is globally disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

enable: Enables BPDU guard.

disable: Disables BPDU guard.

Usage guidelines

When the setting is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

When the setting is configured in Layer 2 aggregate interface view, it takes effect only on that aggregate interface.

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 FortyGigE 1/1/4.

```
<Sysname> system-view
[Sysname] interface fortygige 1/1/4
[Sysname-FortyGigE1/1/4] stp port bpdu-protection enable
```

Related commands

- **stp bpdu-protection** (*Layer 2—LAN Switching Command Reference)*
- **stp edged-port** (*Layer 2—LAN Switching Command Reference)*

New feature: Data buffer monitoring

Configuring data buffer monitoring

The data buffer on a switch is shared by all interfaces for buffering packets during periods of congestion.

This feature allows you to identify the interfaces that use an excessive amount of data buffer space. Then, you can diagnose those interfaces for anomalies.

You can set a per-interface buffer usage threshold. The buffer usage threshold for a queue is the same as the per-interface threshold value. The switch automatically records buffer usage for each interface. When a queue on an interface uses more buffer space than the set threshold, the system counts one threshold violation for the queue.

To configure data buffer monitoring:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set a per-interface buffer usage threshold.	**buffer usage threshold slot** *slot-number* **ratio** *ratio*	By default, no buffer usage threshold is set.
3. Return to user view.	**quit**	N/A
4. Display buffer usage statistics for interfaces.	**display buffer usage interface** [*interface-type* [*interface-number*]]	Available in any view.

Command reference

New command: buffer usage threshold

Use **buffer usage threshold** to set a per-interface buffer usage threshold.

Use **undo buffer usage threshold** to restore the default.

Syntax

buffer usage threshold slot *slot-number* **ratio** *ratio*

undo buffer usage threshold slot *slot-number*

Default

No per-interface buffer usage threshold is set.

Views

System view

Predefined user roles

network-admin

Parameters

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

ratio *ratio*: Specifies the buffer usage threshold in percentage, in the range of 1 to 100.

Usage guidelines

After you configure this command, the switch automatically records buffer usage for each interface. When a queue on an interface uses more buffer space than the set threshold, the system counts one threshold violation for the queue.

To display the buffer usage statistics for interfaces, use the **display buffer usage interface** command.

Examples

Set the per-interface buffer usage threshold to 50% for IRF member device 2.

```
<Sysname> system-view
[Sysname] buffer usage threshold slot 2 ratio 50
```

New command: display buffer usage interface

Use **display buffer usage interface** to display buffer usage statistics for interfaces.

Syntax

display buffer usage interface [*interface-type* [*interface-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type [*interface-number*]: Specifies an interface by its type and number. If you do not specify the *interface-type* argument, this command displays buffer usage statistics for all Ethernet interfaces. If you specify the *interface-type* argument without the *interface-number* argument, this command displays buffer usage statistics for all Ethernet interfaces of the specified type.

Examples

Display buffer usage statistics for Ten-GigabitEthernet 1/0/1.

```
<Sysname> display buffer usage interface ten-gigabitethernet 1/0/1
Interface              QueueID Total       Used        Threshold(%) Violations
--------------------------------------------------------------------------------
XGE1/0/1               0       9418032     0           30           0
                       1       9418032     0           30           0
                       2       9418032     0           30           0
                       3       9418032     0           30           0
                       4       9418032     0           30           0
                       5       9418032     0           30           0
                       6       9418032     0           30           0
                       7       9418032     0           30           0
```

Table 19 Command output

Field	Description
Total	Data buffer size in bytes allowed for a queue.
Used	Data buffer size in bytes that has been used by a queue.
Threshold(%)	Buffer usage threshold for a queue. The threshold value is the same as the per-interface threshold value.
Violations	Number of threshold violations for a queue. The value of this field is reset upon a switch reboot.

Modified command: display packet-drop

Syntax

display packet-drop { **interface** [*interface-type* [*interface-number*]] | **summary** }

Views

Any view

Change description

The following line is added to the command output:

```
Packets dropped by insufficient data buffer. Input dropped: 65535 Output dropped: 32768
```

New feature: Configuring Smart SAN

This feature is available only on FCF and FCF-NPV switches.

Overview

Smart SAN is a SAN configuration and management solution that is designed for intelligence, simplicity, ease of maintenance, ease of diagnosis, and self-healing. Smart SAN simplifies user operations while increasing manageability for SANs. Smart SAN is deployed on all SAN network elements (storage devices, servers, and switches). A switch with Smart SAN enabled performs the following operations:

- Collects information about servers and storage devices for mutual discovery.
- Controls access between servers and storage devices, and automates zoning configuration.

  The zoning configuration includes creating and deleting peer zones, adding members to peer zones, and adding peer zones to a zone set and activating the zone set.
- Collects diagnostic information about servers and storage devices by using Add Diagnostic Parameters (RDP) request packets for network monitoring and diagnosis.
- Controls automatic login of servers and storage devices.

Configuration procedure

Smart SAN can be configured for FC/FCoE.

After Smart SAN is enabled for FC/FCoE, the switch notifies the following modules to act accordingly:

- **FDMI**—This module performs the following operations:
  - **a.** Regularly sends RDP request packets to request diagnostic information about nodes.
  - **b.** Updates information about local ports.
  - **c.** Sends Add Diagnostic Parameters (ADP) packets to other switches to synchronize RDP database information.
- **FC zone**—This module automatically configures each VSAN to operate in enhanced zoning mode.

To configure Smart SAN:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable Smart SAN.	**smartsan enable** [**fcoe**]	By default, Smart SAN is disabled.
3. Set the interval for sending RDP request packets.	**rdp request-polling-interval** *interval*	The default setting is 30 minutes. This command can be configured only after Smart SAN is enabled for FC/FCoE.

Command reference

New command: smartsan enable

Use **smartsan enable** to enable Smart SAN.

Use **undo smartsan enable** to disable Smart SAN.

Syntax

smartsan enable [**fcoe**]

undo smartsan enable [**fcoe**]

Default

Smart SAN is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

fcoe: Specifies Smart SAN for FC/FCoE.

Usage guidelines

The **undo smartsan enable** command deletes local peer zone information, but not peer zone information received from other switches. For more information about peer zones, see *FCoE Configuration Guide*.

Examples

Enable Smart SAN for FC/FCoE.

```
<Sysname> system-view
[Sysname] smartsan enable fcoe
```

Related commands

display smartsan status

New command: rdp request-polling-interval

Use **rdp request-polling-interval** to set the interval for sending RDP request packets.

Use **undo rdp request-polling-interval** to restore the default.

Syntax

rdp request-polling-interval *interval*

undo rdp request-polling-interval

Default

The interval for sending RDP request packets is 30 minutes.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval for sending RDP request packets, in the range of 5 to 1440 minutes.

Usage guidelines

The interval for sending RDP request packets can be set only after Smart SAN is enabled for FC/FCoE.

Examples

Set the interval for sending RDP request packets.

```
<Sysname> system-view
[Sysname] rdp request-polling-interval 5
```

Related commands

display rdp request-polling-interval

New command: display rdp database

Use **display rdp database** to display RDP database information.

Syntax

display rdp database [**port-name** *port-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

port-name *port-name*: Specifies a port by its name, in the format of *xx:xx:xx:xx:xx:xx:xx:xx*, where *x* is a hexadecimal number. The port can be any port in the FC SAN. If you do not specify a port, this command displays RDP database information for all ports in the FC SAN.

Usage guidelines

RDP database information can be displayed only after Smart SAN is enabled for FC/FCoE.

The RDP database includes the RDP database information of the following ports:

- N_Ports directly connected to the switch.
- Ports on the switch.
- N_Ports not directly connected to the switch and ports on other switches in the FC SAN.

Examples

Display the RDP database information of the N_Port 10:00:00:00:c9:88:a4:9e.

```
<Sysname> display rdp database port-name 10:00:00:00:c9:88:a4:9e
Port Name: 10:00:00:00:c9:88:a4:9e
Node Name: 20:00:00:e0:fc:f1:e8:00
Fabric Port Name: 20:00:00:50:c9:a3:c4:56
Fabric Node Name: 20:64:00:e1:cf:25:09:00
Port Speed:
```

```
  Port Speed Capabilities: 10 Gb
  Port Operating Speed: 10 Gb
Link Error Status (FCoE):
  Link Failure Count: 1
  Virtual Link Failure Count: 2
  Missing FIP Keep Alive or Discovery Advertisement Count: 3
  Symbol Error During Carrier Count: 4
  Error Block Count: 5
  Frame Check Sequence Error Count: 6
SFP Diagnostics:
  Temperature: 40C
  Voltage: 5V
  Bias Current: 100Ma
  Tx Power: 6mW
  Rx Power: 6mW
  Tx Type: Short Wave Laser
  Optical Port: Yes
  Connector Type: SFP+
```

Table 20 Command output

Field	Description
Port Name	WWN of the N_Port.
Node Name	WWN of the node where the N_Port resides.
Fabric Port Name	WWN of the F_Port or NP_Port directly connected to the Nx_Port.
Fabric Node Name	WWN of the switch where the F_Port or NP_Port directly connected to the Nx_Port resides.
Port Speed Capabilities	The supported speed can be one or more of the following options: • 1 Gbps. • 2 Gbps. • 4 Gbps. • 8 Gbps. • 10 Gbps. • 16 Gbps. • 32 Gbps.
Port Operating Speed	The current speed can only be one of the following options: • 1 Gbps. • 2 Gbps. • 4 Gbps. • 8 Gbps. • 10 Gbps. • 16 Gbps. • 32 Gbps.
Link Error Status	Link error state: • **Link Error Status (FCoE)**—Link error state for the VFC interface directly connected to the Nx_Port. • **Link Error Status (FC)** —Link error state for the FC interface directly connected to the Nx_Port.
Link Failure Count	Number of link failures detected through physical link transition detection.

Field	Description
Virtual Link Failure Count	Number of link failures detected by the virtual link maintenance protocol.
Missing FIP Keep Alive or Discovery Advertisement Count	Number of missing virtual link maintenance protocol frames.
Symbol Error During Carrier Count	Number of reception errors at the PHY layer that occur during frame reception.
Error Block Count	Cumulative count of the events counted by the 8-bit errored blocks counter.
Frame Check Sequence Error Count	Number of Ethernet frames received that are an integral number of octets in length and do not pass the FCS check.
Temperature	Internally measured transceiver temperature.
Voltage	Internally measured supply voltage.
Bias Current	Measured transmitter laser bias current.
Tx Power	Measured coupled TX output power.
Rx Power	Measured received optical power.
Tx Type	Transmitter type of the Nx_Port: • Short Wave Laser. • Long Wave Laser LC 1310nm. • Long Wave Laser LL 1550nm.
Optical Port	Indicates whether the Nx_Port is an optical port: Yes or No.

Display the RDP database information of a switch port (an F_Port in this example).

```
<Sysname> display rdp database port-name 28:05:00:e0:fc:f1:58:2a
Port Name: 28:05:00:e0:fc:f1:58:2a
 Node Name: -
 Port Speed:
  Port Speed Capabilities: 10 Gbps
  Port Operating Speed: 10 Gbps
 SFP Diagnostics:
  Temperature: 35C
  Voltage: 2.5184V
  Bias Current: 12.000mA
  Tx Power: 0.0000mW
  Rx Power: 0.0000mW
  Tx Type: Short Wave Laser
  Optical Port: Yes
  Connector Type: SFP+
```

Table 21 Command output

Field	Description
Port Name	WWN of the F_Port.
Node Name	This fields displays a hyphen (-) for an F_Port or E_Port and displays the WWN of the NPV switch for an NP_Port.
Port Speed Capabilities	The supported speed can be one or more of the following options: • 1 Gbps. • 2 Gbps.

Field	Description
	• 4 Gbps. • 8 Gbps. • 10 Gbps. • 16 Gbps. • 32 Gbps.
Port Operating Speed	The current speed can only be one of the following options: • 1 Gbps. • 2 Gbps. • 4 Gbps. • 8 Gbps. • 10 Gbps. • 16 Gbps. • 32 Gbps.
Temperature	Internally measured transceiver temperature.
Voltage	Internally measured supply voltage.
Bias Current	Measured transmitter laser bias current.
Tx Power	Measured coupled TX output power.
Rx Power	Measured received optical power.
Tx Type	Transmitter type of the port: • Short Wave Laser. • Long Wave Laser LC 1310nm. • Long Wave Laser LL 1550nm.
Optical Port	Indicates whether the port is an optical port: Yes or No.

New command: display rdp request-polling-interval

Use **display rdp request-polling-interval** to display the interval for sending RDP request packets.

Syntax

display rdp request-polling-interval

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

The interval for sending RDP request packets can be displayed only after Smart SAN is enabled for FC/FCoE.

Examples

Display the interval for sending RDP request packets.

```
<Sysname> display rdp request-polling-interval
RDP request-polling-interval: 30 minutes
```

New command: display smartsan status

Use **display smartsan status** to display the Smart SAN status.

Syntax

display smartsan status

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the Smart SAN status.

```
<Sysname> display smartsan status
Smart SAN Status:
  FC/FCoE: Enabled
  iSCSI: Disabled
```

New feature: SNMP silence

SNMP silence enables the device to automatically detect and defend against SNMP attacks.

After you enable SNMP, the device automatically starts an SNMP silence timer and counts the number of packets that fail SNMP authentication within 1 minute.

- If the number of the packets is smaller than 100, the device restarts the timer and counting.
- If the number of the packets is equal to or greater than 100, the SNMP module enters a 5-minute silence period, during which the device does not respond to any SNMP packets. After the 5 minutes expire, the device restarts the timer and counting.

New feature: DSCP value for NETCONF over SOAP over HTTP/HTTPS packets

Setting the DSCP value for NETCONF over SOAP over HTTP/HTTPS packets

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the DSCP value for NETCONF over SOAP over HTTP packets.	**netconf soap http dscp** *dscp-value*	By default, the DSCP value is 0 for NETCONF over SOAP over HTTP packets.
3. Set the DSCP value for NETCONF over SOAP over HTTPS packets.	**netconf soap https dscp** *dscp-value*	By default, the DSCP value is 0 for NETCONF over SOAP over HTTPS packets.

Command reference

netconf soap http dscp

Use **netconf soap http dscp** to set the DSCP value for outgoing NETCONF over SOAP over HTTP packets.

Use **undo netconf soap http dscp** to restore the default.

Syntax

netconf soap http dscp *dscp-value*

undo netconf soap http dscp

Default

The DSCP value is 0 for outgoing NETCONF over SOAP over HTTP packets.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63. A larger DSCP value represents a higher priority.

Usage guidelines

The DSCP value of an IP packet specifies the priority level of the packet and affects the transmission priority of the packet.

Examples

Set the DSCP value to 30 for outgoing NETCONF over SOAP over HTTP packets.

```
<Sysname> system-view
[Sysname] netconf soap http dscp 30
```

netconf soap https dscp

Use **netconf soap https dscp** to set the DSCP value for outgoing NETCONF over SOAP over HTTPS packets.

Use **undo netconf soap https dscp** to restore the default.

Syntax

netconf soap https dscp *dscp-value*

undo netconf soap https dscp

Default

The DSCP value is 0 for outgoing NETCONF over SOAP over HTTPS packets.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63. A larger DSCP value represents a higher priority.

Usage guidelines

The DSCP value of an IP packet specifies the priority level of the packet and affects the transmission priority of the packet.

Examples

Set the DSCP value to 30 for outgoing NETCONF over SOAP over HTTPS packets.

```
<Sysname> system-view
[Sysname] netconf soap https dscp 30
```

New feature: MAC authentication offline detection

Enabling MAC authentication offline detection

This feature logs a user out of the device if the device does not receive any packets from the user within the offline detect timer. The device also requests to stop accounting for the user at the same time. To set the offline detect timer, use the **mac-authentication timer** command.

Disabling this feature disables the device from inspecting the online user status.

To enable MAC authentication offline detection:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Enable MAC authentication offline detection.	**mac-authentication offline-detect enable**	By default, MAC authentication offline detection is enabled.

Command reference

mac-authentication offline-detect enable

Use **mac-authentication offline-detect enable** to enable MAC authentication offline detection on a port.

Use **undo mac-authentication offline-detect enable** to disable MAC authentication offline detection.

Syntax

mac-authentication offline-detect enable

undo mac-authentication offline-detect enable

Default

MAC authentication offline detection is enabled on a port.

Views

Ethernet interface view

Predefined user roles

network-admin

Examples

Disable MAC authentication offline detection on the port FortyGigE 1/1/4.

```
<Sysname> system-view
[Sysname] interface fortygige 1/1/4
[Sysname-FortyGigE1/1/4] undo mac-authentication offline-detect enable
```

Related commands

mac-authentication timer

New feature: Displaying the maximum number of ARP entries that a device supports

Displaying the maximum number of ARP entries that a device supports

In this release, you can display the maximum number of ARP entries that a device supports by using the **display arp entry-limit** command.

Command reference

New command: display arp entry-limit

Use **display arp entry-limit** to display the maximum number of ARP entries that a device supports.

Syntax

display arp entry-limit

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the maximum number of ARP entries that the device supports.

```
<Sysname> display arp entry-limit
ARP entries: 16384
```

New feature: Displaying the maximum number of ND entries that a device supports

Displaying the maximum number of ND entries that a device supports

In this release, you can display the maximum number of ND entries that a device supports by using the **display ipv6 neighbors entry-limit** command.

Command reference

New command: display ipv6 neighbors entry-limit

Use **display ipv6 neighbors entry-limit** to display the maximum number of ND entries that a device supports.

Syntax

display ipv6 neighbors entry-limit

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the maximum number of ND entries that the device supports.

```
<Sysname> display ipv6 neighbors entry-limit
ND entries: 16384
```

New feature: ARP detection logging

Enabling ARP detection logging

The ARP detection logging feature enables a device to generate ARP detection log messages when illegal ARP packets are detected. An ARP detection log message contains the following information:

- Receiving interface of the ARP packets.
- Sender IP address.
- Total number of dropped ARP packets.

The following is an example of an ARP detection log message:

```
Detected an inspection occurred on interface FortyGigE1/0/1 with IP address 172.18.48.55
(Total 10 packets dropped).
```

To enable ARP detection logging:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable ARP detection logging.	**arp detection log enable**	By default, ARP detection logging is disabled.

Command reference

arp detection log enable

Use **arp detection log enable** to enable ARP detection logging.

Use **undo arp detection log enable** to disable ARP detection logging.

Syntax

arp detection log enable

undo arp detection log enable

Default

ARP detection logging is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable ARP detection logging.

```
<Sysname> system-view
[Sysname] arp detection log enable
```

Disable ARP detection logging.

```
<Sysname> system-view
[Sysname] undo arp detection log enable
```

New feature: Attack detection and prevention

Overview

Attack detection and prevention enables a device to detect attacks by inspecting arriving packets, and to take prevention actions to protect a private network. Prevention actions include logging and packet dropping.

Attacks that the device can prevent

This section describes the attacks that the device can detect and prevent.

Single-packet attacks

Single-packet attacks are also known as malformed packet attacks. An attacker typically launches single-packet attacks by using the following methods:

- An attacker sends defective packets to a device, which causes the device to malfunction or crash.
- An attacker sends normal packets to a device, which interrupts connections or probes network topologies.
- An attacker sends a large number of forged packets to a target device, which consumes network bandwidth and causes denial of service (DoS).

Table 22 lists the single-packet attack types that the device can detect and prevent.

Table 22 Types of single-packet attacks

Single-packet attack	Description
ICMP redirect	An attacker sends ICMP redirect messages to modify the victim's routing table. The victim cannot forward packets correctly.
ICMP destination unreachable	An attacker sends ICMP destination unreachable messages to cut off the connections between the victim and its destinations.
ICMP type	A receiver responds to an ICMP packet according to its type. An attacker sends forged ICMP packets of a specific type to affect the packet processing of the victim.
ICMPv6 type	A receiver responds to an ICMPv6 packet according to its type. An attacker sends forged ICMPv6 packets of specific types to affect the packet processing of the victim.
Land	An attacker sends the victim a large number of TCP SYN packets, which contain the victim's IP address as the source and destination IP addresses. This attack exhausts the half-open connection resources on the victim, and locks the victim's system.
Large ICMP packet	An attacker sends large ICMP packets to crash the victim. Large ICMP packets can cause memory allocation error and crash the protocol stack.
Large ICMPv6 packet	An attacker sends large ICMPv6 packets to crash the victim. Large ICMPv6 packets can cause memory allocation error and crash the protocol stack.
IP options	An attacker sends IP datagrams in which the IP options are abnormal. This attack intends to probe the network topology. The target system will break down if it is incapable of processing error packets.
IP fragment	An attacker sends the victim an IP datagram with an offset smaller than 5, which causes the victim to malfunction or crash.
IP impossible packet	An attacker sends IP packets whose source IP address is the same as the destination IP address, which causes the victim to malfunction.
Tiny fragment	An attacker makes the fragment size small enough to force Layer 4 header fields into the second fragment. These fragments can pass the packet filtering because they do not hit any match.
Smurf	An attacker broadcasts an ICMP echo request to target networks. These requests contain the victim's IP address as the source IP address. Every receiver on the target networks will send an ICMP echo reply to the victim. The victim will be flooded with replies, and will be unable to provide services. Network congestion might occur.
TCP flag	An attacker sends packets with defective TCP flags to probe the operating system of the target host. Different operating systems process

Single-packet attack	Description
	unconventional TCP flags differently. The target system will break down if it processes this type of packets incorrectly.
Traceroute	An attacker uses traceroute tools to probe the topology of the victim network.
WinNuke	An attacker sends Out-Of-Band (OOB) data to the TCP port 139 (NetBIOS) on the victim that runs Windows system. The malicious packets contain an illegal Urgent Pointer, which causes the victim's operating system to crash.
UDP bomb	An attacker sends a malformed UDP packet. The length value in the IP header is larger than the IP header length plus the length value in the UDP header. When the target system processes the packet, a buffer overflow can occur, which causes a system crash.
UDP Snork	An attacker sends a UDP packet with destination port 135 (the Microsoft location service) and source port 135, 7, or 19. This attack causes an NT system to exhaust its CPU.
UDP Fraggle	An attacker sends a large number of chargen packets with source UDP port 7 and destination UDP port 19 to a network. These packets use the victim's IP address as the source IP address. Replies will flood the victim, resulting in DoS.
Teardrop	An attacker sends a stream of overlapping fragments. The victim will crash when it tries to reassemble the overlapping fragments.
Ping of death	An attacker sends the victim an ICMP echo request larger than 65535 bytes that violates the IP protocol. When the victim reassembles the packet, a buffer overflow can occur, which causes a system crash.

Scanning attacks

Scanning is a preintrusion activity used to prepare for intrusion into a network. The scanning allows the attacker to find a way into the target network and to disguise the attacker's identity.

Attackers will use scanning tools to probe a network, find vulnerable hosts, and discover services that are running on the hosts. Attackers can use the information to launch attacks.

The device can detect and prevent the IP sweep and port scan attacks. If an attacker performs port scanning from multiple hosts to the target host, distributed port scan attacks occur.

Flood attacks

An attacker launches a flood attack by sending a large number of forged requests to the victim in a short period of time. The victim is too busy responding to these forged requests to provide services for legal users, and a DoS attack occurs.

The device can detect and prevent the following types of flood attacks:

- SYN flood attack.

  A SYN flood attacker exploits the TCP three-way handshake characteristics and makes the victim unresponsive to legal users. An attacker sends a large number of SYN packets with forged source addresses to a server. This causes the server to open a large number of half-open connections and respond to the requests. However, the server will never receive the expected ACK packets. The server is unable to accept new incoming connection requests because all of its resources are bound to half-open connections.
- ACK flood attack.

An ACK packet is a TCP packet only with the ACK flag set. Upon receiving an ACK packet from a client, the server must search half-open connections for a match.

An ACK flood attacker sends a large number of ACK packets to the server. This causes the server to be busy searching for half-open connections, and the server is unable to process packets for normal services.

- SYN-ACK flood attack.

  Upon receiving a SYN-ACK packet, the server must search for the matching SYN packet it has sent. A SYN-ACK flood attacker sends a large number of SYN-ACK packets to the server. This causes the server to be busy searching for SYN packets, and the server is unable to process packets for normal services.

- FIN flood attack.

  FIN packets are used to shut down TCP connections.

  A FIN flood attacker sends a large number of forged FIN packets to a server. The victim might shut down correct connections, or be unable to provide services because it is busy searching for matching connections.

- RST flood attack.

  RST packets are used to abort TCP connections when TCP connection errors occur.

  An RST flood attacker sends a large number of forged RST packets to a server. The victim might shut down correct connections, or be unable to provide services because it is busy searching for matching connections.

- DNS flood attack.

  The DNS server processes and replies all DNS queries that it receives.

  A DNS flood attacker sends a large number of forged DNS queries. This attack consumes the bandwidth and resources of the DNS server, which prevents the server from processing and replying legal DNS queries.

- HTTP flood attack.

  Upon receiving an HTTP GET request, the HTTP server performs complex operations, including character string searching, database traversal, data reassembly, and format switching. These operations consume a large amount of system resources.

  An HTTP flood attacker sends a large number of HTTP GET requests that exceed the processing capacity of the HTTP server, which causes the server to crash.

- ICMP flood attack.

  An ICMP flood attacker sends ICMP request packets, such as ping packets, to a host at a fast rate. Because the target host is busy replying to these requests, it is unable to provide services.

- ICMPv6 flood attack.

  An ICMPv6 flood attacker sends ICMPv6 request packets, such as ping packets, to a host at a fast rate. Because the target host is busy replying to these requests, it is unable to provide services.

- UDP flood attack.

  A UDP flood attacker sends UDP packets to a host at a fast rate. These packets consume a large amount of the target host's bandwidth, so the host cannot provide other services.

Configuring an attack defense policy

Creating an attack defense policy

An attack defense policy can contain a set of attack detection and prevention configuration against multiple attacks.

To create an attack defense policy:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Create an attack defense policy and enter its view.	**attack-defense policy** *policy-name*	By default, no attack defense policy exists.

Configuring a single-packet attack defense policy

Single-packet attack detection inspects packets destined for the device based on the packet signature. If an attack packet is detected, the device can take the following actions:

- Output logs (the default action).
- Drop attack packets.

You can also configure the device to not take any actions.

To configure a single-packet attack defense policy:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter attack defense policy view.	**attack-defense policy** *policy-name*	N/A
3.	Configure signature detection for single-packet attacks.	• **signature detect** { **fraggle** | **fragment** | **impossible** | **ip-option-abnormal** | **land** | **large-icmp** | **large-icmpv6** | **ping-of-death** | **smurf** | **snork** | **tcp-all-flags** | **tcp-fin-only** | **tcp-invalid-flags** | **tcp-null-flag** | **tcp-syn-fin** | **teardrop** | **tiny-fragment** | **traceroute** | **udp-bomb** | **winnuke** } [**action** { { **drop** | **logging** } * | **none** }] • **signature detect icmp-type** { *icmp-type-value* | **address-mask-reply** | **address-mask-request** | **destination-unreachable** | **echo-reply** | **echo-request** | **information-reply** | **information-request** | **parameter-problem** | **redirect** | **source-quench** | **time-exceeded** | **timestamp-reply** | **timestamp-request** } [**action** { { **drop** | **logging** } * | **none** }] • **signature detect icmpv6-type** { *icmpv6-type-value* | **destination-unreachable** | **echo-reply** | **echo-request** | **group-query** | **group-reduction** | **group-report** | **packet-too-big** | **parameter-problem** | **time-exceeded** } [**action** { { **drop** | **logging** } * | **none** }] • **signature detect ip-option** { *option-code* | **internet-timestamp** | **loose-source-routing** | **record-route** | **route-alert** | **security** | **stream-id** | **strict-source-routing** } [**action** { { **drop** | **logging** } * | **none** }] • **signature detect ipv6-ext-header** *ext-header-value* [**action** { { **drop** | **logging** } * | **none** }]	By default, signature detection is not configured for single-packet attacks. You can configure signature detection for multiple single-packet attacks.
4.	(Optional.) Set the maximum length of safe ICMP or	**signature** { **large-icmp** | **large-icmpv6** } **max-length** *length*	By default, the maximum length of safe ICMP or ICMPv6

Step	Command	Remarks
ICMPv6 packets.		packets is 4000 bytes. A large ICMP or ICMPv6 attack occurs if an ICMP or ICMPv6 packet larger than the specified length is detected.
5. (Optional.) Specify the actions against single-packet attacks of a specific level.	**signature level** { **high** | **info** | **low** | **medium** } **action** { { **drop** | **logging** } * | **none** }	The default action is **logging** for single-packet attacks of the informational and low levels. The default actions are **logging** and **drop** for single-packet attacks of the medium and high levels.
6. (Optional.) Enable signature detection for single-packet attacks of a specific level.	**signature level** { **high** | **info** | **low** | **medium** } **detect**	By default, signature detection is disabled for all levels of single-packet attacks.

Configuring a scanning attack defense policy

Scanning attack detection monitors the rate at which connections are initiated to the device. If a source initiates connections at a rate equal to or exceeding the pre-defined threshold, the device can take the following actions:

- Output logs.
- Drop subsequent packets from the IP address of the attacker.

To configure a scanning attack defense policy:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter attack defense policy view.	**attack-defense policy** *policy-name*	N/A
3. Configure scanning attack detection.	**scan detect level** { **high** | **low** | **medium** } **action** { **drop** | **logging** } *	By default, scanning attack detection is not configured.

Configuring a flood attack defense policy

Attack detection and prevention takes effect only on packets destined for the device in the current release. The IP address specified for IP address-specific flood attack detection must be an IP address of a Layer 3 interface on the device.

Flood attack detection monitors the rate at which connections are initiated to the device.

With flood attack detection configured, the device is in attack detection state. When the packet sending rate to an IP address reaches or exceeds the threshold, the device enters prevention state and takes the specified actions. When the rate is below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

You can configure flood attack detection and prevention for a specific IP address. For non-specific IP addresses, the device uses the global attack prevention settings.

Configuring a SYN flood attack defense policy

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter attack defense policy view.	**attack-defense policy** *policy-name*	N/A
3. Enable global SYN flood attack detection.	**syn-flood detect non-specific**	By default, global SYN flood attack detection is disabled.
4. Set the global trigger threshold for SYN flood attack prevention.	**syn-flood threshold** *threshold-value*	The default setting is 1000.
5. Specify global actions against SYN flood attacks.	**syn-flood action** { **drop** | **logging** } *	By default, no global action is specified for SYN flood attacks.
6. Configure IP address-specific SYN flood attack detection.	**syn-flood detect** { **ip** *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { **drop** | **logging** } *]	By default, IP address-specific SYN flood attack detection is not configured.

Configuring an ACK flood attack defense policy

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter attack defense policy view.	**attack-defense policy** *policy-name*	N/A
3. Enable global ACK flood attack detection.	**ack-flood detect non-specific**	By default, global ACK flood attack detection is disabled.
4. Set the global trigger threshold for ACK flood attack prevention.	**ack-flood threshold** *threshold-value*	The default setting is 1000.
5. Specify global actions against ACK flood attacks.	**ack-flood action** { **drop** | **logging** } *	By default, no global action is specified for ACK flood attacks.
6. Configure IP address-specific ACK flood attack detection.	**ack-flood detect** { **ip** *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { **drop** | **logging** } *]	By default, IP address-specific ACK flood attack detection is not configured.

Configuring a SYN-ACK flood attack defense policy

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter attack defense policy view.	**attack-defense policy** *policy-name*	N/A
3. Enable global SYN-ACK flood attack detection.	**syn-ack-flood detect non-specific**	By default, global SYN-ACK flood attack detection is disabled.

Step	Command	Remarks
4. Set the global trigger threshold for SYN-ACK flood attack prevention.	**syn-ack-flood threshold** *threshold-value*	The default setting is 1000.
5. Specify global actions against SYN-ACK flood attacks.	**syn-ack-flood action** { **drop** | **logging** } *	By default, no global action is specified for SYN-ACK flood attacks.
6. Configure IP address-specific SYN-ACK flood attack detection.	**syn-ack-flood detect** { **ip** *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { **drop** | **logging** } *]	By default, IP address-specific SYN-ACK flood attack detection is not configured.

Configuring a FIN flood attack defense policy

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter attack defense policy view.	**attack-defense policy** *policy-name*	N/A
3. Enable global FIN flood attack detection.	**fin-flood detect non-specific**	By default, global FIN flood attack detection is disabled.
4. Set the global trigger threshold for FIN flood attack prevention.	**fin-flood threshold** *threshold-value*	The default setting is 1000.
5. Specify global actions against FIN flood attacks.	**fin-flood action** { **drop** | **logging** } *	By default, no global action is specified for FIN flood attacks.
6. Configure IP address-specific FIN flood attack detection.	**fin-flood detect** { **ip** *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { **drop** | **logging** } *]	By default, IP address-specific FIN flood attack detection is not configured.

Configuring an RST flood attack defense policy

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter attack defense policy view.	**attack-defense policy** *policy-name*	N/A
3. Enable global RST flood attack detection.	**rst-flood detect non-specific**	By default, global RST flood attack detection is disabled.
4. Set the global trigger threshold for RST flood attack prevention.	**rst-flood threshold** *threshold-value*	The default setting is 1000.
5. Specify global actions against RST flood attacks.	**rst-flood action** { **drop** | **logging** } *	By default, no global action is specified for RST flood attacks.
6. Configure IP address-specific RST flood attack detection.	**rst-flood detect** { **ip** *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { **drop** |	By default, IP address-specific RST flood attack detection is not configured.

Step	Command	Remarks
	logging } *]	

Configuring an ICMP flood attack defense policy

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter attack defense policy view.	**attack-defense policy** *policy-name*	N/A
3. Enable global ICMP flood attack detection.	**icmp-flood detect non-specific**	By default, global ICMP flood attack detection is disabled.
4. Set the global trigger threshold for ICMP flood attack prevention.	**icmp-flood threshold** *threshold-value*	The default setting is 1000.
5. Specify global actions against ICMP flood attacks.	**icmp-flood action** { **drop** | **logging** } *	By default, no global action is specified for ICMP flood attacks.
6. Configure IP address-specific ICMP flood attack detection.	**icmp-flood detect ip** *ip-address* [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { **drop** | **logging** } *]	By default, IP address-specific ICMP flood attack detection is not configured.

Configuring an ICMPv6 flood attack defense policy

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter attack defense policy view.	**attack-defense policy** *policy-name*	N/A
3. Enable global ICMPv6 flood attack detection.	**icmpv6-flood detect non-specific**	By default, global ICMPv6 flood attack detection is disabled.
4. Set the global trigger threshold for ICMPv6 flood attack prevention.	**icmpv6-flood threshold** *threshold-value*	The default setting is 1000.
5. Specify global actions against ICMPv6 flood attacks.	**icmpv6-flood action** { **drop** | **logging** } *	By default, no global action is specified for ICMPv6 flood attacks.
6. Configure IP address-specific ICMPv6 flood attack detection.	**icmpv6-flood detect ipv6** *ipv6-address* [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { **drop** | **logging** } *]	By default, IP address-specific ICMPv6 flood attack detection is not configured.

Configuring a UDP flood attack defense policy

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter attack defense policy view.	**attack-defense policy** *policy-name*	N/A
3. Enable global UDP flood attack detection.	**udp-flood detect non-specific**	By default, global UDP flood attack

Step	Command	Remarks
		detection is disabled.
4. Set the global trigger threshold for UDP flood attack prevention.	**udp-flood threshold** *threshold-value*	The default setting is 1000.
5. Specify global actions against UDP flood attacks.	**udp-flood action** { **drop** | **logging** } *	By default, no global action is specified for UDP flood attacks.
6. Configure IP address-specific UDP flood attack detection.	**udp-flood detect** { **ip** *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { **drop** | **logging** } *]	By default, IP address-specific UDP flood attack detection is not configured.

Configuring a DNS flood attack defense policy

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter attack defense policy view.	**attack-defense policy** *policy-name*	N/A
3. Enable global DNS flood attack detection.	**dns-flood detect non-specific**	By default, global DNS flood attack detection is disabled.
4. Set the global trigger threshold for DNS flood attack prevention.	**dns-flood threshold** *threshold-value*	The default setting is 1000.
5. (Optional.) Specify the global ports to be protected against DNS flood attacks.	**dns-flood port** *port-list*	By default, DNS flood attack prevention protects port 53.
6. Specify global actions against DNS flood attacks.	**dns-flood action** { **drop** | **logging** } *	By default, no global action is specified for DNS flood attacks.
7. Configure IP address-specific DNS flood attack detection.	**dns-flood detect** { **ip** *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**port** *port-list*] [**threshold** *threshold-value*] [**action** { **drop** | **logging** } *]	By default, IP address-specific DNS flood attack detection is not configured.

Configuring an HTTP flood attack defense policy

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter attack defense policy view.	**attack-defense policy** *policy-name*	N/A
3. Enable global HTTP flood attack detection.	**http-flood detect non-specific**	By default, global HTTP flood attack detection is disabled.
4. Set the global trigger threshold for HTTP flood attack prevention.	**http-flood threshold** *threshold-value*	The default setting is 1000.
5. (Optional.) Specify the global ports to be protected	**http-flood port** *port-list*	By default, HTTP flood attack prevention protects port 80.

Step	Command	Remarks
against HTTP flood attacks.		
6. Specify global actions against HTTP flood attacks.	**http-flood action** { **drop** | **logging** } *	By default, no global action is specified for HTTP flood attacks.
7. Configure IP address-specific HTTP flood attack detection.	**http-flood detect** { **ip** *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**port** *port-list*] [**threshold** *threshold-value*] [**action** { **drop** | **logging** } *]	By default, IP address-specific HTTP flood attack detection is not configured.

Configuring attack detection exemption

The attack defense policy uses the ACL to identify exempted packets. The policy does not check the packets permitted by the ACL. You can configure the ACL to identify packets from trusted hosts. The exemption feature reduces the false alarm rate and improves packet processing efficiency.

To configure attack detection exemption:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter attack defense policy view.	**attack-defense policy** *policy-name*	N/A
3. Configure attack detection exemption.	**exempt acl** [**ipv6**] { *acl-number* | **name** *acl-name* }	By default, the attack defense policy applies to all packets destined for the device.

Applying an attack defense policy to the device

An attack defense policy applied to the device itself detects packets destined for the device and prevents attacks targeted at the device.

A switch uses hardware to implement packet forwarding and uses software to process packets if the packets are destined for the switch. The software does not provide any attack defense features, so you can apply an attack defense policy to the switch to prevent attacks aimed at the switch.

To apply an attack defense policy to the device:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Apply an attack defense policy to the device.	**attack-defense local apply policy** *policy-name*	By default, no attack defense policy is applied to the device.

Disabling log aggregation for single-packet attack events

Log aggregation aggregates all logs generated in a period and sends one log. The logs with the same attributes for the following items can be aggregated:

- Interface where the attack is detected.

- Attack type.
- Attack defense action.
- Source and destination IP addresses.
- VPN instance to which the victim IP address belongs.

As a best practice, you not disable log aggregation. A large number of logs will consume the display resources of the console.

To disable log aggregation for single-packet attack events:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Disable log aggregation for single-packet attack events.	**attack-defense signature log non-aggregate**	By default, log aggregation is enabled for single-packet attack events.

Displaying and maintaining attack detection and prevention

Use the **display** commands in any view and the **reset** commands in user view.

To display and maintain attack detection and prevention:

Task	Command
Display attack detection and prevention statistics for the device.	**display attack-defense statistics local** [**slot** *slot-number*]
Display attack defense policy configuration.	**display attack-defense policy** [*policy-name*]
Display information about IPv4 scanning attackers.	**display attack-defense scan attacker ip** [**count**]
Display information about IPv6 scanning attackers.	**display attack-defense scan attacker ipv6** [**count**]
Display information about IPv4 scanning attack victims.	**display attack-defense scan victim ip** [**count**]
Display information about IPv6 scanning attack victims.	**display attack-defense scan victim ipv6** [**count**]
Display flood attack detection and prevention statistics for an IPv4 address.	**display attack-defense** { **ack-flood** | **dns-flood** | **fin-flood** | **flood** | **http-flood** | **icmp-flood** | **rst-flood** | **syn-ack-flood** | **syn-flood** | **udp-flood** } **statistics ip** [*ip-address* [**vpn** *vpn-instance-name*]] [**local** [**slot** *slot-number*]] [**count**]
Display flood attack detection and prevention statistics for an IPv6 address.	**display attack-defense** { **ack-flood** | **dns-flood** | **fin-flood** | **flood** | **http-flood** | **icmpv6-flood** | **rst-flood** | **syn-ack-flood** | **syn-flood** | **udp-flood** } **statistics ipv6** [*ipv6-address* [**vpn** *vpn-instance-name*]] [**local** [**slot** *slot-number*]] [**count**]
Display information about IPv4 addresses protected by flood attack detection and prevention.	**display attack-defense policy** *policy-name* { **ack-flood** | **dns-flood** | **fin-flood** | **flood** | **http-flood** | **icmp-flood** | **rst-flood** | **syn-ack-flood** | **syn-flood** | **udp-flood** } **ip** [*ip-address* [**vpn** *vpn-instance-name*]] [**slot** *slot-number*] [**count**]

Task	Command
Display information about IPv6 addresses protected by flood attack detection and prevention.	**display attack-defense policy** *policy-name* { **ack-flood** | **dns-flood** | **fin-flood** | **flood** | **http-flood** | **icmpv6-flood** | **rst-flood** | **syn-ack-flood** | **syn-flood** | **udp-flood** } **ipv6** [*ipv6-address* [**vpn** *vpn-instance-name*]] [**slot** *slot-number*] [**count**]
Clear attack detection and prevention statistics for the device.	**reset attack-defense statistics local**
Clear flood attack detection and prevention statistics.	**reset attack-defense policy** *policy-name* **flood protected** { **ip** | **ipv6** } **statistics**

Command reference

ack-flood action

Use **ack-flood action** to specify global actions against ACK flood attacks.

Use **undo ack-flood action** to restore the default.

Syntax

ack-flood action { **drop | logging** } *

undo ack-flood action

Default

No global action is specified for ACK flood attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

drop: Drops subsequent ACK packets destined for the victim IP addresses.

logging: Enables logging for ACK flood attack events. The log information records the victim IP address, MPLS L3VPN instance name, current packet statistics, prevention actions, and start time of the attack.

Examples

Specify **drop** as the global action against ACK flood attacks in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] ack-flood action drop
```

Related commands

- **ack-flood threshold**
- **ack-flood detect**
- **ack-flood detect non-specific**

ack-flood detect

Use **ack-flood detect** to configure IP address-specific ACK flood attack detection.

Use **undo ack-flood detect** to remove IP address-specific ACK flood attack detection configuration.

Syntax

ack-flood detect { **ip** *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { **drop** | **logging** } *]

undo ack-flood detect { **ip** *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

IP address-specific ACK flood attack detection is not configured.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Specifies the IPv4 address to be protected. The *ip-address* argument cannot be all 1s or 0s.

ipv6 *ipv6-address*: Specifies the IPv6 address to be protected.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IP address is on the public network.

threshold *threshold-value*: Sets the threshold for triggering ACK flood attack prevention. The value range is 1 to 1000000 in units of ACK packets sent to the specified IP address per second.

action: Specifies the actions when an ACK flood attack is detected. If no action is specified, the global actions set by the **ack-flood action** command apply.

drop: Drops subsequent ACK packets destined for the protected IP address.

logging: Enables logging for ACK flood attack events. The log information records the victim IP address, MPLS L3VPN instance name, current packet statistics, prevention action, and start time of the attack.

Usage guidelines

You can configure ACK flood attack detection for multiple IP addresses in one attack defense policy. The supported maximum number varies by device model.

With ACK flood attack detection configured, the device is in attack detection state. When the sending rate of ACK packets to a protected IP address reaches or exceeds the threshold, the device enters prevention state and takes the specified actions. When the rate is below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

Examples

Configure ACK flood attack detection for 192.168.1.2 in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] ack-flood detect ip 192.168.1.2 threshold
2000
```

Related commands

- **ack-flood action**

- **ack-flood detect non-specific**
- **ack-flood threshold**

ack-flood detect non-specific

Use **ack-flood detect non-specific** to enable global ACK flood attack detection.

Use **undo ack-flood detect non-specific** to restore the default.

Syntax

ack-flood detect non-specific

undo ack-flood detect non-specific

Default

Global ACK flood attack detection is disabled.

Views

Attack defense policy view

Predefined user roles

network-admin

Usage guidelines

The global ACK flood attack detection applies to all IP addresses except those specified by the **ack-flood detect** command. The global detection uses the global trigger threshold set by the **ack-flood threshold** command and global actions specified by the **ack-flood action** command.

Examples

Enable global ACK flood attack detection in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] ack-flood detect non-specific
```

Related commands

- **ack-flood action**
- **ack-flood detect**
- **ack-flood threshold**

ack-flood threshold

Use **ack-flood threshold** to set the global threshold for triggering ACK flood attack prevention.

Use **undo ack-flood threshold** to restore the default.

Syntax

ack-flood threshold *threshold-value*

undo ack-flood threshold

Default

The global threshold is 1000 for triggering ACK flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the threshold value. The value range is 1 to 1000000 in units of ACK packets sent to an IP address per second.

Usage guidelines

The device applies the global threshold to global ACK flood attack detection.

Adjust the threshold according to the application scenarios. If the number of ACK packets sent to a protected server, such as an HTTP or FTP server, is normally large, set a large threshold. A small threshold might affect the server services. For a network that is unstable or susceptible to attacks, set a small threshold.

Examples

Set the global threshold to 100 for triggering ACK flood attack prevention in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] ack-flood threshold 100
```

Related commands

- **ack-flood action**
- **ack-flood detect**
- **ack-flood detect non-specific**

attack-defense local apply policy

Use **attack-defense local apply policy** to apply an attack defense policy to the device.

Use **undo attack-defense local apply policy** to restore the default.

Syntax

attack-defense local apply policy *policy-name*

undo attack-defense local apply policy

Default

No attack defense policy is applied to the device.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies the name of an attack defense policy. The policy name is a case-insensitive string of 1 to 31 characters. Valid characters include uppercase and lowercase letters, digits, underscores (_), and hyphens (-).

Usage guidelines

An attack defense policy applied to the device itself detects packets destined for the device and prevents attacks targeted at the device.

A switch uses hardware to implement packet forwarding and uses software to process packets if the packets are destined for the switch. The software does not provide any attack defense features, so you can apply an attack defense policy to the switch to prevent attacks aimed at the switch.

Each device can have only one attack defense policy applied. If you use this command multiple times, the most recent configuration takes effect.

Examples

Apply the attack defense policy **atk-policy-1** to the device.

```
<Sysname> system-view
[Sysname] attack-defense local apply policy atk-policy-1
```

Related commands

- **attack-defense policy**
- **display attack-defense policy**

attack-defense policy

Use **attack-defense policy** to create an attack defense policy and enter its view.

Use **undo attack-defense policy** to delete an attack defense policy.

Syntax

attack-defense policy *policy-name*

undo attack-defense policy *policy-name*

Default

No an attack defense policy exists.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Assigns a name to the attack defense policy. The policy name is a case-insensitive string of 1 to 31 characters. Valid characters include uppercase and lowercase letters, digits, underscores (_), and hyphens (-).

Examples

Create the attack defense policy **atk-policy-1** and enter its view.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1]
```

Related commands

- **attack-defense apply policy**
- **display attack-defense policy**

attack-defense signature log non-aggregate

Use **attack-defense signature log non-aggregate** to disable log aggregation for single-packet attack events.

Use **undo attack-defense signature log non-aggregate** to restore the default.

Syntax

attack-defense signature log non-aggregate

undo attack-defense signature log non-aggregate

Default

Log aggregation is enabled for single-packet attack events.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Log aggregation aggregates all logs generated during a period of time and sends one log. The logs with the same attributes for the following items can be aggregated:

- Interface where the attack is detected.
- Attack type.
- Attack defense action.
- Source and destination IP addresses.
- VPN instance to which the victim IP address belongs.

As a best practice, you not disable log aggregation. A large number of logs will consume the display resources of the console.

Examples

Disable log aggregation for single-packet attack events.

```
<Sysname> system-view
[Sysname] attack-defense signature log non-aggregate
```

Related commands

signature detect

display attack-defense flood statistics ip

Use **display attack-defense flood statistics ip** to display flood attack detection and prevention statistics for a protected IPv4 address.

Syntax

display attack-defense { **ack-flood** | **dns-flood** | **fin-flood** | **flood** | **http-flood** | **icmp-flood** | **rst-flood** | **syn-ack-flood** | **syn-flood** | **udp-flood** } **statistics ip** [*ip-address* [**vpn** *vpn-instance-name*]] [**local** [**slot** *slot-number*]] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ack-flood: Specifies ACK flood attack.

dns-flood: Specifies DNS flood attack.

fin-flood: Specifies FIN flood attack.

flood: Specifies all IPv4 flood attacks.

http-flood: Specifies HTTP flood attack.

icmp-flood: Specifies ICMP flood attack.

rst-flood: Specifies RST flood attack.

syn-ack-flood: Specifies SYN-ACK flood attack.

syn-flood: Specifies SYN flood attack.

udp-flood: Specifies UDP flood attack.

ip-address: Specifies an IPv4 address. If you do not specify an IPv4 address, this command displays flood attack detection and prevention statistics for all protected IPv4 addresses.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IPv4 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IPv4 address is on the public network.

local: Specifies the device.

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

count: Displays the number of matching protected IPv4 addresses.

Usage guidelines

The device collects statistics about protected IP addresses for flood attack detection and prevention. The attackers' IP addresses are not recorded.

Examples

Display flood attack detection and prevention statistics for all IPv4 addresses.

```
<Switch>display attack-defense flood statistics ip
Slot 1:
IP Address      VPN          Detected on  Detect type   State    PPS   Dropped
255.255.255.255 --           Local        UDP-FLOOD     Normal   0      0
192.168.1.67    --           Local        SYN-FLOOD     Normal   0      0
192.168.1.67    --           Local        ACK-FLOOD     Normal   22     0
192.168.1.255   --           Local        UDP-FLOOD     Normal   7      0
```

Display the number of IPv4 addresses that are protected against flood attacks.

```
<Sysname> display attack-defense flood statistics ip count
Slot 1:
Totally 2 flood entries.
```

Table 23 Command output

Field	Description
IP address	Protected IPv4 address.
VPN	MPLS L3VPN instance to which the protected IPv4 address belongs. If the protected IPv4 address is on the public network, this field displays hyphens (--)
Detected on	Where the attack is detected. The value for this field can only be **Local**.
Detect type	Type of the detected flood attack.
State	Whether the device is attacked: • **Attacked**.

Field	Description
	• **Normal**.
PPS	Number of packets sent to the IPv4 address per second.
Dropped	Number of attack packets dropped by the device.
Totally 2 flood entries	Total number of IPv4 addresses that are protected.

display attack-defense flood statistics ipv6

Use **display attack-defense flood statistics ipv6** to display flood attack detection and prevention statistics for a protected IPv6 address.

Syntax

display attack-defense { **ack-flood** | **dns-flood** | **fin-flood** | **flood** | **http-flood** | **icmpv6-flood** | **rst-flood** | **syn-ack-flood** | **syn-flood** | **udp-flood** } **statistics ipv6** [*ipv6-address* [**vpn** *vpn-instance-name*]] [**local** [**slot** *slot-number*]] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ack-flood: Specifies ACK flood attack.

dns-flood: Specifies DNS flood attack.

fin-flood: Specifies FIN flood attack.

flood: Specifies all IPv6 flood attacks.

http-flood: Specifies HTTP flood attack.

icmpv6-flood: Specifies ICMPv6 flood attack.

rst-flood: Specifies RST flood attack.

syn-ack-flood: Specifies SYN-ACK flood attack.

syn-flood: Specifies SYN flood attack.

udp-flood: Specifies UDP flood attack.

ipv6-address: Specifies an IPv6 address. If you do not specify an IPv6 address, this command displays flood attack detection and prevention statistics for all protected IPv6 addresses.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IPv6 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IPv6 address is on the public network.

local: Specifies the device.

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

count: Displays the number of matching protected IPv6 addresses.

Usage guidelines

The device collects statistics about protected IP addresses for flood attack detection and prevention. The attackers' IP addresses are not recorded.

Examples

Display flood attack detection and prevention statistics for all IPv6 addresses.

```
<Sysname> display attack-defense flood statistics ipv6
Totally 5 flood entries.
IPv6 address    VPN         Detected on  Detect type   State    PPS     Dropped
1::3            --          Local        SYN-ACK-FLOOD Normal   0       0
1::4            --          Local        ACK-FLOOD     Normal   0       0
1::5            --          Local        SYN-FLOOD     Normal   20      0
```

Display the number of IPv6 addresses that are protected against flood attacks.

```
<Sysname> display attack-defense flood statistics ipv6 count
Slot 1:
Totally 5 flood entries.
```

Table 24 Command output

Field	Description
IPv6 address	Protected IPv6 address.
VPN	MPLS L3VPN instance to which the protected IPv6 address belongs. If the protected IPv6 address is on the public network, this field displays hyphens (--).
Detected on	Where the attack is detected. The value for this field can only be **Local**.
Detect type	Type of the detected flood attack.
State	Whether the device is attacked: • **Attacked**. • **Normal**.
PPS	Number of packets sent to the IPv6 address per second.
Dropped	Number of attack packets dropped by the device.
Totally 2 flood entries	Total number of IPv6 addresses that are protected.

display attack-defense policy

Use **display attack-defense policy** to display attack defense policy configuration.

Syntax

display attack-defense policy [*policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

policy-name: Specifies an attack defense policy by its name. The policy name is a case-insensitive string of 1 to 31 characters. Valid characters include uppercase and lowercase letters, digits, underscores (_), and hyphens (-). If no attack defense policy is specified, this command displays brief information about all attack defense policies.

Usage guidelines

This command output includes the following configuration information about an attack defense policy:

- Whether attack detection is enabled.
- Attack prevention actions.
- Attack prevention trigger thresholds.

Examples

Display the configuration of the attack defense policy **atk-policy-1**.

```
<Sysname> display attack-defense policy atk-policy-1
          Attack-defense Policy Information
--------------------------------------------------------------------------
Policy name                        : atk-policy-1
Applied list                       : None
--------------------------------------------------------------------------
Exempt IPv4 ACL                    : acl_1
Exempt IPv6 ACL                    : Not configured
--------------------------------------------------------------------------
  Actions: CV-Client verify  BS-Block source  L-Logging  D-Drop  N-None

Signature attack defense configuration:
Signature name                     Defense      Level             Actions
Fragment                           Disabled     low               L
Impossible                         Disabled     medium            L,D
Teardrop                           Disabled     medium            L,D
Tiny fragment                      Disabled     low               L
IP option abnormal                 Disabled     medium            L,D
Smurf                              Enabled      medium            D
Traceroute                         Disabled     low               L
Ping of death                      Disabled     medium            L,D
Large ICMP                         Disabled     info              D
  Max length                       50000 bytes
Large ICMPv6                       Disabled     info              D
  Max length                       4000 bytes
TCP invalid flags                  Disabled     medium            L,D
TCP null flag                      Disabled     medium            L,D
TCP all flags                      Disabled     medium            L,D
TCP SYN-FIN flags                  Disabled     medium            L,D
TCP FIN only flag                  Disabled     medium            L,D
TCP Land                           Disabled     medium            L,D
Winnuke                            Disabled     medium            L,D
UDP Bomb                           Disabled     medium            L,D
UDP Snork                          Disabled     medium            L,D
UDP Fraggle                        Disabled     medium            L,D
IP option record route             Disabled     info              D
IP option internet timestamp       Disabled     info              D
IP option security                 Disabled     info              D
IP option loose source routing     Disabled     info              D
```

```
IP option stream ID                Disabled     info             D
IP option strict source routing    Disabled     info             D
IP option route alert              Disabled     info             D
ICMP echo request                  Disabled     info             D
ICMP echo reply                    Disabled     info             D
ICMP source quench                 Disabled     info             D
ICMP destination unreachable       Disabled     info             D
ICMP redirect                      Disabled     info             D
ICMP time exceeded                 Disabled     info             D
ICMP parameter problem             Disabled     info             D
ICMP timestamp request             Disabled     info             D
ICMP timestamp reply               Disabled     info             D
ICMP information request           Disabled     info             D
ICMP information reply             Disabled     info             D
ICMP address mask request          Disabled     info             D
ICMP address mask reply            Disabled     info             D
ICMPv6 echo request                Disabled     info             D
ICMPv6 echo reply                  Disabled     info             D
ICMPv6 group membership query      Disabled     info             D
ICMPv6 group membership report     Disabled     info             D
ICMPv6 group membership reduction  Disabled     info             D
ICMPv6 destination unreachable     Disabled     info             D
ICMPv6 time exceeded               Disabled     info             D
ICMPv6 parameter problem           Disabled     info             D
ICMPv6 packet too big              Disabled     info             D

Scan attack defense configuration:
 Defense : Enabled
 Level   : high
 Actions : D

Flood attack defense configuration:
Flood type      Global thres(pps)  Global actions  Service ports   Non-specific
SYN flood       1000(default)      -               -               Disabled
ACK flood       1000(default)      -               -               Disabled
SYN-ACK flood   1000(default)      -               -               Disabled
RST flood       1000(default)      -               -               Disabled
FIN flood       1000(default)      -               -               Disabled
UDP flood       1000(default)      -               -               Disabled
ICMP flood      1000(default)      -               -               Disabled
ICMPv6 flood    1000(default)      -               -               Disabled
DNS flood       1000(default)      -               53              Disabled
HTTP flood      1000(default)      -               80              Disabled

Flood attack defense for protected IP addresses:
 Address                 VPN instance Flood type    Thres(pps) Actions Ports
```

Table 25 Command output

Field	Description
Policy name	Name of the attack defense policy.
Applied list	List of interfaces to which the attack defense policy is applied. If a device only supports applying the policy to the device, this field displays **None**.
Exempt IPv4 ACL	IPv4 ACL used for attack detection exemption.
Exempt IPv6 ACL	IPv6 ACL used for attack detection exemption.
Actions	Attack prevention actions: • **CV**—Client verification. • **BS**—Blocking sources. • **L**—Logging. • **D**—Dropping packets. • **N**—No action. The device does not support **CV** and **BS** in the current release.
Signature attack defense configuration	Configuration information about single-packet attack detection and prevention.
Signature name	Type of the single-packet attack.
Defense	Whether attack detection is enabled.
Level	Level of the single-packet attack, **info**, **low**, **medium**, or **high**.
Actions	Prevention actions against the single-packet attack: • **L**—Logging. • **D**—Dropping packets. • **N**—No action.
Scan attack defense configuration	Configuration information about scanning attack detection and prevention.
Defense	Whether attack detection is enabled.
Level	Level of the scanning attack detection, **low**, **medium**, or **high**.
Actions	Prevention actions against the scanning attack: • **BS**—Blocking sources. • **D**—Dropping packets. • **L**—Logging. The device does not support **BS** in the current release.
Flood attack defense configuration	Configuration information about flood attack detection and prevention.
Flood type	Type of the flood attack: • ACK flood. • DNS flood. • FIN flood. • ICMP flood. • ICMPv6 flood. • SYN flood. • SYN-ACK flood. • UDP flood. • RST flood. • HTTP flood.
Global thres (pps)	Global threshold for triggering the flood attack prevention, in units of

Field	Description
	packets sent to an IP address per second. The default is 1000 pps.
Global actions	Global prevention actions against the flood attack: • **D**—Dropping packets. • **L**—Logging. • **CV**—Client verification. • **-**—Not configured. The device does not support **CV** in the current release.
Service ports	Ports that are protected against the flood attack. This field is displays port numbers only for the DNS and HTTP flood attacks. For other flood attacks, this field displays a hyphen (-).
Non-specific	Whether the global flood attack detection is enabled.
Flood attack defense for protected IP addresses	Configuration of the IP address-specific flood attack detection and prevention.
Address	Protected IP address.
VPN instance	MPLS L3VPN instance to which the protected IP address belongs. If no MPLS L3VPN instance is specified, this field displays a hyphen (-).
Thres(pps)	Threshold for triggering the flood attack prevention, in units of packets sent to the IP address per second. If no threshold is specified, this field displays a hyphen (-).
Actions	Prevention actions against the flood attack: • **BS**—Blocking sources. • **CV**—Client verification. • **D**—Dropping packets. • **L**—Logging. • **N**—No action. The device does not support **CV** and **BS** in the current release.
Ports	Ports that are protected against the flood attack. This field displays port numbers only for the DNS and HTTP flood attacks. For other flood attacks, this field displays a hyphen (-).

Related commands

attack-defense policy

display attack-defense policy ip

Use **display attack-defense policy ip** to display information about IPv4 addresses protected by flood attack detection and prevention.

Syntax

display attack-defense policy *policy-name* { **ack-flood** | **dns-flood** | **fin-flood** | **flood** | **http-flood** | **icmp-flood** | **rst-flood** | **syn-ack-flood** | **syn-flood** | **udp-flood** } **ip** [*ip-address* [**vpn** *vpn-instance-name*]] [**slot** *slot-number*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

policy-name: Specifies an attack defense policy by its name. The policy name is a case-insensitive string of 1 to 31 characters. Valid characters include uppercase and lowercase letters, digits, underscores (_), and hyphens (-).

ack-flood: Specifies ACK flood attack.

dns-flood: Specifies DNS flood attack.

fin-flood: Specifies FIN flood attack.

flood: Specifies all IPv4 flood attacks.

http-flood: Specifies HTTP flood attack.

icmp-flood: Specifies ICMP flood attack.

rst-flood: Specifies RST flood attack.

syn-ack-flood: Specifies SYN-ACK flood attack.

syn-flood: Specifies SYN flood attack.

udp-flood: Specifies UDP flood attack.

ip-address: Specifies a protected IPv4 address. If you do not specify an IPv4 address, this command displays information about all protected IPv4 addresses.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the IPv4 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the IPv4 address is on the public network.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about IPv4 addresses protected by flood attack detection and prevention for all IRF member devices.

count: Displays the number of matching IPv4 addresses protected by flood attack detection and prevention.

Examples

Display information about all IPv4 addresses protected by flood attack detection and prevention in the attack defense policy **abc**.

```
<Sysname> display attack-defense policy abc flood ip
Slot 1:
IP address       VPN instance      Type          Rate threshold(PPS) Dropped
192.168.1.2      --                ACK-FLOOD     2000                0
192.168.1.2      --                RST-FLOOD     2000                0
192.168.1.2      --                FIN-FLOOD     2000                0
192.168.1.2      --                UDP-FLOOD     2000                0
192.168.1.2      --                ICMP-FLOOD    2000                0
192.168.1.2      --                DNS-FLOOD     2000                0
192.168.1.2      --                HTTP-FLOOD    2000                0
10.1.1.1         --                SYN-FLOOD     100                 0
```

Display the number of IPv4 addresses protected by flood attack detection and prevention in the attack defense policy **abc**.

```
<Sysname> display attack-defense policy abc flood ip count
Slot 1:
Totally 3 flood protected entries.
```

Table 26 Command output

Field	Description
Totally 3 flood protected IP addresses	Total number of the IPv4 addresses protected by flood attack detection and prevention.
IP address	Protected IPv4 address.
VPN instance	MPLS L3VPN instance to which the protected IPv4 address belongs. If the protected IPv4 address is on the public network, this field displays hyphens (--).
Type	Type of the flood attack.
Rate threshold(PPS)	Threshold for triggering the flood attack prevention, in units of packets sent to the IP address per second.
Dropped	Number of dropped attack packets. If the prevention action is logging, this field displays **0**.

display attack-defense policy ipv6

Use **display attack-defense policy ipv6** to display information about IPv6 addresses protected by flood attack detection and prevention.

Syntax

Distributed devices–Centralized IRF devices–In standalone mode:

display attack-defense policy *policy-name* { **ack-flood** | **dns-flood** | **fin-flood** | **flood** | **http-flood** | **icmpv6-flood** | **rst-flood** | **syn-ack-flood** | **syn-flood** | **udp-flood** } **ipv6** [*ipv6-address* [**vpn** *vpn-instance-name*]] [**slot** *slot-number*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

policy-name: Specifies an attack defense policy by its name. The policy name is a case-insensitive string of 1 to 31 characters. Valid characters include uppercase and lowercase letters, digits, underscores (_), and hyphens (-).

ack-flood: Specifies ACK flood attack.

dns-flood: Specifies DNS flood attack.

fin-flood: Specifies FIN flood attack.

flood: Specifies all IPv6 flood attacks.

http-flood: Specifies HTTP flood attack.

icmpv6-flood: Specifies ICMPv6 flood attack.

rst-flood: Specifies RST flood attack.

syn-ack-flood: Specifies SYN-ACK flood attack.

syn-flood: Specifies SYN flood attack.

udp-flood: Specifies UDP flood attack.

ipv6-address: Specifies a protected IPv6 address. If you do not specify an IPv6 address, this command displays information about all protected IPv6 addresses.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the IPv6 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the IPv6 address is on the public network.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about IPv6 addresses protected by flood attack detection and prevention for all IRF member devices.

count: Displays the number of matching IPv6 addresses protected by flood attack detection and prevention.

Examples

Display information about all IPv6 addresses protected by flood attack detection and prevention in the attack defense policy **abc**.

```
<Sysname> display attack-defense policy abc flood ipv6
Slot 1:
IPv6 address     VPN instance     Type          Rate threshold(PPS) Dropped
2012::12         --               ICMPV6-FLOOD  2000                0
```

Display the number of IPv6 addresses protected by flood attack detection and prevention in the attack defense policy **abc**.

```
<Sysname> display attack-defense policy abc flood ipv6 count
Slot 1:
Totally 3 flood protected IP addresses.
```

Table 27 Command output

Field	Description
Totally 3 flood protected IP addresses	Total number of the IPv6 addresses protected by flood attack detection and prevention.
IPv6 address	Protected IPv6 address.
VPN instance	MPLS L3VPN instance to which the protected IPv6 address belongs. If the protected IPv6 address is on the public network, this field displays hyphens (--).
Type	Type of the flood attack.
Rate threshold(PPS)	Threshold for triggering the flood attack prevention, in units of packets sent to the IPv6 address per second.
Dropped	Number of dropped attack packets. If the prevention action is logging, this field displays **0**.

display attack-defense scan attacker ip

Use **display attack-defense scan attacker ip** to display information about IPv4 scanning attackers.

Syntax

display attack-defense scan attacker ip [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

count: Displays the number of matching IPv4 scanning attackers.

Usage guidelines

If no parameter is specified, this command displays information about all IPv4 scanning attackers.

Examples

Display information about all IPv4 scanning attackers.

```
<Sysname> display attack-defense scan attacker ip
Slot 1:
IP address      VPN instance     DS-Lite tunnel peer  Detected on  Duration(min)
192.168.31.2    --               --                   Local        1284
2.2.2.3         --               --                   Local        23
```

Display the number of IPv4 scanning attackers.

```
<Sysname> display attack-defense scan attacker ip count
Slot 1:
Totally 3 attackers.
```

Table 28 Command output

Field	Description
Totally 3 attackers	Total number of IPv4 scanning attackers.
IP address	IPv4 address of the attacker.
VPN instance	MPLS L3VPN instance to which the attacker's IPv4 address belongs. If the IPv4 address is on the public network, this field displays hyphens (--).
DS-Lite tunnel peer	IPv6 address of the DS-Lite tunnel peer. If the device is the AFTR of a DS-Lite tunnel, this field displays the IPv6 address of the B4 element from which the packet comes. In other situations, this field displays hyphens (--).
Detected on	Where the attack is detected. The value for this field can only be **Local**.
Duration(min)	The amount of time the attack lasts, in minutes.

Related commands

- **display attack-defense scan victim ip**
- **scan detect**

display attack-defense scan attacker ipv6

Use **display attack-defense scan attacker ipv6** to display information about IPv6 scanning attackers.

Syntax

display attack-defense scan attacker ipv6 [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

count: Displays the number of matching IPv6 scanning attackers.

Usage guidelines

If no parameter is specified, this command displays information about all IPv6 scanning attackers.

Examples

Display information about all IPv6 scanning attackers.

```
<Sysname> display attack-defense scan attacker ipv6
Slot 1:
IPv6 address             VPN instance     Detected on               Duration(min)
2013::2                  --               Local                     1234
1230::22                 --               Local                     10
```

Display the number of IPv6 scanning attackers.

```
<Sysname> display attack-defense scan attacker ipv6 count
Slot 1:
Totally 3 attackers.
```

Table 29 Command output

Field	Description
Totally 3 attackers	Total number of IPv6 scanning attackers.
IPv6 address	IPv6 address of the attacker.
VPN instance	MPLS L3VPN instance to which the attacker IPv6 address belongs. If the attacker IPv6 address is on the public network, this field displays hyphens (--).
Detected on	Where the attack is detected. The value for this field can only be **Local**.
Duration(min)	The amount of time the attack lasts, in minutes.

Related commands

- **display attack-defense scan victim ipv6**
- **scan detect**

display attack-defense scan victim ip

Use **display attack-defense scan victim ip** to display information about IPv4 scanning attack victims.

Syntax

display attack-defense scan victim ip [**count**]

Any view

Predefined user roles

network-admin

network-operator

Parameters

count: Displays the number of matching IPv4 scanning attack victims.

Usage guidelines

If no parameter is specified, this command displays information about all IPv4 scanning attack victims.

Examples

Display information about all IPv4 scanning attack victims.

```
<Sysname> display attack-defense scan victim ip
Slot 1:
IP address      VPN instance                    Detected on       Duration(min)
192.168.31.2    --                              Local             21
2.2.2.3         --                              Local             1234
```

Display the number of IPv4 scanning attack victims.

```
<Sysname> display attack-defense scan victim ip count
Slot 1:
Totally 3 victim IP addresses.
```

Table 30 Command output

Field	Description
Totally 3 victim IP addresses	Total number of IPv4 scanning attack victims.
IP address	IPv4 address of the victim.
VPN instance	MPLS L3VPN instance to which the victim IPv4 address belongs. If the victim IPv4 address is on the public network, this field displays hyphens (--).
Detected on	Where the attack is detected. The value for this filed can only be **Local**.
Duration(min)	The amount of time the attack lasts, in minutes.

Related commands

- **display attack-defense scan attacker ip**
- **scan detect**

display attack-defense scan victim ipv6

Use **display attack-defense scan victim ipv6** to display information about IPv6 scanning attack victims.

Syntax

display attack-defense scan victim ipv6 [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

count: Displays the number of matching IPv6 scanning attack victims.

Usage guidelines

If no parameter is specified, this command displays information about all IPv6 scanning attack victims.

Examples

Display information about all IPv6 scanning attack victims.

```
<Sysname> display attack-defense scan victim ipv6
Slot 1:
IPv6 address              VPN instance     Detected on               Duration(min)
2013::2                   --               Local                     210
1230::22                  --               Local                     13
```

Display the number of IPv6 scanning attack victims.

```
<Sysname> display attack-defense scan victim ipv6 count
Slot 1:
Totally 3 victim IP addresses.
```

Table 31 Command output

Field	Description
Totally 3 victim IP addresses	Total number of IPv6 scanning attack victims.
IPv6 address	IPv6 address of the victim.
VPN instance	MPLS L3VPN instance to which the victim IPv6 address belongs. If the victim IPv6 address is on the public network, this field displays hyphens (--).
Detected on	Where the attack is detected. The value for this field can only be **Local**.
Duration(min)	The amount of time the attack lasts, in minutes.

Related commands

- **display attack-defense scan attacker ipv6**
- **scan detect**

display attack-defense statistics local

Use **display attack-defense statistics local** to display attack detection and prevention statistics for the device.

Syntax

display attack-defense statistics local [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays attack detection and prevention statistics for the device for all IRF member devices.

Examples

Display attack detection and prevention statistics for the device.

```
<Sysname> display attack-defense statistics local
Slot 1:
Attack policy name: abc
Scan attack defense statistics:
 AttackType                           AttackTimes Dropped
 Port scan                            2           23
 IP sweep                             3           33
 Distribute port scan                 1           10
Flood attack defense statistics:
 AttackType                           AttackTimes Dropped
 SYN flood                            1           0
 ACK flood                            1           0
 SYN-ACK flood                        3           5000
 RST flood                            2           0
 FIN flood                            2           0
 UDP flood                            1           0
 ICMP flood                           1           0
 ICMPv6 flood                         1           0
 DNS flood                            1           0
 HTTP flood                           1           0
Signature attack defense statistics:
 AttackType                           AttackTimes Dropped
 IP option record route               1           100
 IP option security                   2           0
 IP option stream ID                  3           0
 IP option internet timestamp         4           1
 IP option loose source routing       5           0
 IP option strict source routing      6           0
 IP option route alert                3           0
 Fragment                             1           0
 Impossible                           1           1
 Teardrop                             1           1
 Tiny fragment                        1           0
 IP options abnormal                  3           0
 Smurf                                1           0
 Ping of death                        1           0
 Traceroute                           1           0
 Large ICMP                           1           0
 TCP NULL flag                        1           0
 TCP all flags                        1           0
 TCP SYN-FIN flags                    1           0
 TCP FIN only flag                    1           0
 TCP invalid flag                     1           0
 TCP Land                             1           0
 Winnuke                              1           0
 UDP Bomb                             1           0
```

```
 Snork                                  1           0
 Fraggle                                1           0
 Large ICMPv6                           1           0
 ICMP echo request                      1           0
 ICMP echo reply                        1           0
 ICMP source quench                     1           0
 ICMP destination unreachable           1           0
 ICMP redirect                          2           0
 ICMP time exceeded                     3           0
 ICMP parameter problem                 4           0
 ICMP timestamp request                 5           0
 ICMP timestamp reply                   6           0
 ICMP information request               7           0
 ICMP information reply                 4           0
 ICMP address mask request              2           0
 ICMP address mask reply                1           0
 ICMPv6 echo request                    1           1
 ICMPv6 echo reply                      1           1
 ICMPv6 group membership query          1           0
 ICMPv6 group membership report         1           0
 ICMPv6 group membership reduction      1           0
 ICMPv6 destination unreachable         1           0
 ICMPv6 time exceeded                   1           0
 ICMPv6 parameter problem               1           0
 ICMPv6 packet too big                  1           0
Slot 1:
Attack policy name: abc
Scan attack defense statistics:
 AttackType                             AttackTimes Dropped
 Port scan                              2           23
 IP sweep                               3           33
 Distribute port scan                   1           10
Flood attack defense statistics:
 AttackType                             AttackTimes Dropped
 SYN flood                              1           0
 ACK flood                              1           0
 SYN-ACK flood                          3           5000
 RST flood                              2           0
 FIN flood                              2           0
 UDP flood                              1           0
 ICMP flood                             1           0
 ICMPv6 flood                           1           0
 DNS flood                              1           0
 HTTP flood                             1           0
Signature attack defense statistics:
 AttackType                             AttackTimes Dropped
 IP option record route                 1           100
 IP option security                     2           0
```

IP option stream ID	3	0
IP option internet timestamp	4	1
IP option loose source routing	5	0
IP option strict source routing	6	0
IP option route alert	3	0
Fragment	1	0
Impossible	1	1
Teardrop	1	1
Tiny fragment	1	0
IP options abnormal	3	0
Smurf	1	0
Ping of death	1	0
Traceroute	1	0
Large ICMP	1	0
TCP NULL flag	1	0
TCP all flags	1	0
TCP SYN-FIN flags	1	0
TCP FIN only flag	1	0
TCP invalid flag	1	0
TCP Land	1	0
Winnuke	1	0
UDP Bomb	1	0
Snork	1	0
Fraggle	1	0
Large ICMPv6	1	0
ICMP echo request	1	0
ICMP echo reply	1	0
ICMP source quench	1	0
ICMP destination unreachable	1	0
ICMP redirect	2	0
ICMP time exceeded	3	0
ICMP parameter problem	4	0
ICMP timestamp request	5	0
ICMP timestamp reply	6	0
ICMP information request	7	0
ICMP information reply	4	0
ICMP address mask request	2	0
ICMP address mask reply	1	0
ICMPv6 echo request	1	1
ICMPv6 echo reply	1	1
ICMPv6 group membership query	1	0
ICMPv6 group membership report	1	0
ICMPv6 group membership reduction	1	0
ICMPv6 destination unreachable	1	0
ICMPv6 time exceeded	1	0
ICMPv6 parameter problem	1	0
ICMPv6 packet too big	1	0

Table 32 Command output

Field	Description
Attack type	Type of the attack.
Attack times	Number of times that the attack occurred.
Dropped	Number of dropped packets.

Related commands

reset attack-defense statistics local

dns-flood action

Use **dns-flood action** to specify global actions against DNS flood attacks.

Use **undo dns-flood action** to restore the default.

Syntax

dns-flood action { **drop** | **logging** } *

undo dns-flood action

Default

No global action is specified for DNS flood attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

drop: Drops subsequent DNS packets destined for the victim IP addresses.

logging: Enables logging for DNS flood attack events. The log information records the victim IP address, MPLS L3VPN instance name, current packet statistics, prevention actions, and start time of the attack.

Examples

Specify **drop** as the global action against DNS flood attacks in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-flood action drop
```

Related commands

- **dns-flood detect**
- **dns-flood detect non-specific**
- **dns-flood threshold**

dns-flood detect

Use **dns-flood detect** to configure IP address-specific DNS flood attack detection.

Use **undo dns-flood detect** to remove IP address-specific DNS flood attack detection configuration.

Syntax

dns-flood detect { **ip** *ip-address* **| ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**port** *port-list*] [**threshold** *threshold-value*] [**action** { **drop | logging** } *]

undo dns-flood detect { **ip** *ip-address* **| ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

IP address-specific DNS flood attack detection is not configured.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Specifies the IPv4 address to be protected. The *ip-address* argument cannot be all 1s or 0s.

ipv6 *ipv6-address*: Specifies the IPv6 address to be protected.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IP address is on the public network.

port *port-list*: Specifies a space-separated list of up to 65535 port number items. Each item specifies a port by its port number or a range of ports in the form of *start-port-number* **to** *end-port-number*. The *end-port-number* cannot be smaller than the *start-port-number*. If you do not specify this option, the global ports apply.

threshold *threshold-value*: Sets the threshold for triggering DNS flood attack prevention. The value range is 1 to 1000000 in units of DNS packets sent to the specified IP address per second.

action: Specifies the actions when a DNS flood attack is detected. If no action is specified, the global actions set by the **dns-flood action** command apply.

drop: Drops subsequent DNS packets destined for the protected IP address.

logging: Enables logging for DNS flood attack events. The log information records the victim IP address, MPLS L3VPN instance name, current packet statistics, prevention action, and start time of the attack.

Usage guidelines

You can configure DNS flood attack detection for multiple IP addresses in one attack defense policy. The supported maximum number varies by the device model.

With DNS flood attack detection configured, the device is in attack detection state. When the sending rate of DNS packets to a protected IP address reaches or exceeds the threshold, the device enters prevention state and takes the specified actions. When the rate is below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

Examples

Configure DNS flood attack detection for 192.168.1.2 in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-flood detect ip 192.168.1.2 port 53
threshold 2000
```

Related commands

- **dns-flood action**
- **dns-flood detect non-specific**

- **dns-flood threshold**
- **dns-flood port**

dns-flood detect non-specific

Use **dns-flood detect non-specific** to enable global DNS flood attack detection.

Use **undo dns-flood detect non-specific** to restore the default.

Syntax

dns-flood detect non-specific

undo dns-flood detect non-specific

Default

Global DNS flood attack detection is disabled.

Views

Attack defense policy view

Predefined user roles

network-admin

Usage guidelines

The global DNS flood attack detection applies to all IP addresses except for those specified by the **dns-flood detect** command. The global detection uses the global trigger threshold set by the **dns-flood threshold** command and global actions specified by the **dns-flood action** command.

Examples

Enable global DNS flood attack detection in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-flood detect non-specific
```

Related commands

- **dns-flood action**
- **dns-flood detect**
- **dns-flood threshold**

dns-flood port

Use **dns-flood port** to specify the global ports to be protected against DNS flood attacks.

Use **undo dns-flood port** to restore the default.

Syntax

dns-flood port *port-list*

undo dns-flood port

Default

The DNS flood attack prevention protects port 53.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

port-list: Specifies a space-separated list of up to 65535 port number items. Each item specifies a port by its port number or a range of ports in the form of *start-port-number* **to** *end-port-number*. The *end-port-number* cannot be smaller than the *start-port-number*.

Usage guidelines

The device detects only DNS packets destined for the specified ports.

The global ports apply to global DNS flood attack detection and IP address-specific DNS flood attack detection with no port specified.

Examples

Specify the ports 53 and 61000 as the global ports to be protected against DNS flood attacks in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-flood port 53 61000
```

Related commands

- **dns-flood action**
- **dns-flood detect**
- **dns-flood detect non-specific**

dns-flood threshold

Use **dns-flood threshold** to set the global threshold for triggering DNS flood attack prevention.

Use **undo dns-flood threshold** to restore the default.

Syntax

dns-flood threshold *threshold-value*

undo dns-flood threshold

Default

The global threshold is 1000 for triggering DNS flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the threshold value. The value range is 1 to 1000000 in units of DNS packets sent to an IP address per second.

Usage guidelines

The global threshold applies to global DNS flood attack detection.

Adjust the threshold according to the application scenarios. If the number of DNS packets sent to a protected DNS server is normally large, set a large threshold. A small threshold might affect the server services. For a network that is unstable or susceptible to attacks, set a small threshold.

Examples

Set the global threshold to 100 for triggering DNS flood attack prevention in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-flood threshold 100
```

Related commands

- **dns-flood action**
- **dns-flood detect**
- **dns-flood detect non-specific**

exempt acl

Use **exempt acl** to configure attack detection exemption.

Use **undo exempt acl** to restore the default.

Syntax

exempt acl [**ipv6**] { *acl-number* **|** **name** *acl-name* }

undo exempt acl [**ipv6**]

Default

Attack detection exemption is not configured. The attack defense policy applies to all packets destined for the device.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

ipv6: Specifies an IPv6 ACL. Do not specify this keyword if you specify an IPv4 ACL.

acl-number: Specifies an ACL by its number:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**.

Usage guidelines

The attack defense policy uses an ACL to identify exempted packets. The policy does not check the packets permitted by the ACL. You can configure the ACL to identify packets from trusted hosts. The exemption feature reduces the false alarm rate and improves packet processing efficiency.

If the specified ACL does not exist or does not contain a rule, attack detection exemption does not take effect.

Examples

Configure an ACL to permit packets sourced from 1.1.1.1.

```
<Sysname> system-view
[Sysname] acl number 2001 name acl_1
[Sysname-acl-basic-2001] rule permit source 1.1.1.1 0
```

```
[Sysname-acl-basic-2001] quit
```

Configure attack detection exemption for packets matching the ACL.

```
[Sysname] attack-defense policy atk-policy-1
[attack-defense-policy-atk-policy-1] exempt acl name acl_1
```

Related commands

attack-defense policy

fin-flood action

Use **fin-flood action** to specify global actions against FIN flood attacks.

Use **undo fin-flood action** to restore the default.

Syntax

fin-flood action { **drop** | **logging** } *

undo fin-flood action

Default

No global action is specified for FIN flood attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

drop: Drops subsequent FIN packets destined for the victim IP addresses.

logging: Enables logging for FIN flood attack events. The log information records the victim IP address, MPLS L3VPN instance name, current packet statistics, prevention actions, and start time of the attack.

Examples

Specify **drop** as the global action against FIN flood attacks in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] fin-flood action drop
```

Related commands

- **fin-flood detect**
- **fin-flood detect non-specific**
- **fin-flood threshold**

fin-flood detect

Use **fin-flood detect** to configure IP address-specific FIN flood attack detection.

Use **undo fin-flood detect** to remove IP address-specific FIN flood attack detection configuration.

Syntax

fin-flood detect { **ip** *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { **drop** | **logging** } *]

undo fin-flood detect { **ip** *ip-address* **| ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

IP address-specific FIN flood attack detection is not configured.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Specifies the IPv4 address to be protected. The *ip-address* argument cannot be all 1s or 0s.

ipv6 *ipv6-address*: Specifies the IPv6 address to be protected.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IP address is on the public network.

threshold *threshold-value*: Sets the threshold for triggering FIN flood attack prevention. The value range is 1 to 1000000 in units of FIN packets sent to the specified IP address per second.

action: Specifies the actions when a FIN flood attack is detected. If no action is specified, the global actions set by the **fin-flood action** command apply.

drop: Drops subsequent FIN packets destined for the protected IP address.

logging: Enables logging for FIN flood attack events. The log information records the victim IP address, MPLS L3VPN instance name, current packet statistics, prevention action, and start time of the attack.

Usage guidelines

You can configure FIN flood attack detection for multiple IP addresses in one attack defense policy. The supported maximum number varies by device model.

With FIN flood attack detection configured, the device is in attack detection state. When the sending rate of FIN packets to a protected IP address reaches or exceeds the threshold, the device enters prevention state and takes the specified actions. When the rate is below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

Examples

Configure FIN flood attack detection for 192.168.1.2 in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] fin-flood detect ip 192.168.1.2 threshold
2000
```

Related commands

- **fin-flood action**
- **fin-flood detect non-specific**
- **fin-flood threshold**

fin-flood detect non-specific

Use **fin-flood detect non-specific** to enable global FIN flood attack detection.

Use **undo fin-flood detect non-specific** to restore the default.

Syntax

fin-flood detect non-specific

undo fin-flood detect non-specific

Default

Global FIN flood attack detection is disabled.

Views

Attack defense policy view

Predefined user roles

network-admin

Usage guidelines

The global FIN flood attack detection applies to all IP addresses except for those specified by the **fin-flood detect** command. The global detection uses the global trigger threshold set by the **fin-flood threshold** command and global actions specified by the **fin-flood action** command.

Examples

Enable global FIN flood attack detection in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] fin-flood detect non-specific
```

Related commands

- **fin-flood action**
- **fin-flood detect**
- **fin-flood threshold**

fin-flood threshold

Use **fin-flood threshold** to set the global threshold for triggering FIN flood attack prevention.

Use **undo fin-flood threshold** to restore the default.

Syntax

fin-flood threshold *threshold-value*

undo fin-flood threshold

Default

The global threshold is 1000 for triggering FIN flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the threshold value. The value range is 1 to 1000000 in units of FIN packets sent to an IP address per second.

Usage guidelines

The global threshold applies to global FIN flood attack detection.

Adjust the threshold according to the application scenarios. If the number of FIN packets sent to a protected server, such as an HTTP or FTP server, is normally large, set a large threshold. A small threshold might affect the server services. For a network that is unstable or susceptible to attacks, set a small threshold.

Examples

Set the global threshold to 100 for triggering FIN flood attack prevention in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] fin-flood threshold 100
```

Related commands

- **fin-flood action**
- **fin-flood detect**
- **fin-flood detect non-specific**

http-flood action

Use **http-flood action** to specify global actions against HTTP flood attacks.

Use **undo http-flood action** to restore the default.

Syntax

http-flood action { **drop** | **logging** } *

undo http-flood action

Default

No global action is specified for HTTP flood attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

drop: Drops subsequent HTTP packets destined for the victim IP addresses.

logging: Enables logging for HTTP flood attack events. The log information records the victim IP address, MPLS L3VPN instance name, current packet statistics, prevention actions, and start time of the attack.

Examples

Specify **drop** as the global action against HTTP flood attacks in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] http-flood action drop
```

Related commands

- **http-flood detect**
- **http-flood detect non-specific**
- **http-flood threshold**

http-flood detect

Use **http-flood detect** to configure IP address-specific HTTP flood attack detection.

Use **undo http-flood detect** to remove IP address-specific HTTP flood attack detection configuration.

Syntax

http-flood detect { **ip** *ip-address* **|** **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**port** *port-list*] [**threshold** *threshold-value*] [**action** { **drop** **|** **logging** } *]

undo http-flood detect { **ip** *ip-address* **|** **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

IP address-specific HTTP flood attack detection is not configured.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Specifies the IPv4 address to be protected. The *ip-address* argument cannot be all 1s or 0s.

ipv6 *ipv6-address*: Specifies the IPv6 address to be protected.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IP address is on the public network.

port *port-list*: Specifies a space-separated list of up to 65535 port number items. Each item specifies a port by its port number or a range of ports in the form of *start-port-number* **to** *end-port-number*. The *end-port-number* cannot be smaller than the *start-port-number*. If you do not specify this option, the global ports apply.

threshold *threshold-value*: Sets the threshold for triggering HTTP flood attack prevention. The value range is 1 to 1000000 in units of HTTP packets sent to the specified IP address per second.

action: Specifies the actions when an HTTP flood attack is detected. If no action is specified, the global actions set by the **http-flood action** command apply.

drop: Drops subsequent HTTP packets destined for the protected IP address.

logging: Enables logging for HTTP flood attack events. The log information records the victim IP address, MPLS L3VPN instance name, current packet statistics, prevention action, and start time of the attack.

Usage guidelines

You can configure HTTP flood attack detection for multiple IP addresses in one attack defense policy. The supported maximum number varies by device model.

With HTTP flood attack detection configured, the device is in attack detection state. When the sending rate of HTTP packets to a protected IP address reaches or exceeds the threshold, the device enters prevention state and takes the specified actions. When the rate is below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

Examples

Configure HTTP flood attack detection for 192.168.1.2 in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
```

```
[Sysname-attack-defense-policy-atk-policy-1] http-flood detect ip 192.168.1.2 port 80
8080 threshold 2000
```

Related commands

- **http-flood action**
- **http-flood detect non-specific**
- **http-flood threshold**
- **http-flood port**

http-flood detect non-specific

Use **http-flood detect non-specific** to enable global HTTP flood attack detection.

Use **undo http-flood detect non-specific** to restore the default.

Syntax

http-flood detect non-specific

undo http-flood detect non-specific

Default

Global HTTP flood attack detection is disabled.

Views

Attack defense policy view

Predefined user roles

network-admin

Usage guidelines

The global HTTP flood attack detection applies to all IP addresses except for those specified by the **http-flood detect** command. The global detection uses the global trigger threshold set by the **http-flood threshold** command and global actions specified by the **http-flood action** command.

Examples

Enable global HTTP flood attack detection in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-flood detect non-specific
```

Related commands

- **http-flood action**
- **http-flood detect**
- **http-flood threshold**

http-flood port

Use **http-flood port** to specify the global ports to be protected against HTTP flood attacks.

Use **undo http-flood port** to restore the default.

Syntax

http-flood port *port-list*

undo http-flood port

Default

The HTTP flood attack prevention protects port 80.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

port-list: Specifies a space-separated list of up to 65535 port number items. Each item specifies a port by its port number or a range of ports in the form of *start-port-number* **to** *end-port-number*. The *end-port-number* cannot be smaller than the *start-port-number*.

Usage guidelines

The device detects only HTTP packets destined for the specified ports.

The global ports apply to global HTTP flood attack detection and IP address-specific HTTP flood attack detection with no port specified.

Examples

Specify the ports 80 and 8080 as the global ports to be protected against HTTP flood attacks in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] http-flood port 80 8080
```

Related commands

- **http-flood action**
- **http-flood detect**
- **http-flood detect non-specific**

http-flood threshold

Use **http-flood threshold** to set the global threshold for triggering HTTP flood attack prevention.

Use **undo http-flood threshold** to restore the default.

Syntax

http-flood threshold *threshold-value*

undo http-flood threshold

Default

The global threshold is 1000 for triggering HTTP flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the threshold value. The value range is 1 to 1000000 in units of HTTP packets sent to an IP address per second.

Usage guidelines

The global threshold applies to global HTTP flood attack detection.

Adjust the threshold according to the application scenarios. If the number of HTTP packets sent to a protected HTTP server is normally large, set a large threshold. A small threshold might affect the server services. For a network that is unstable or susceptible to attacks, set a small threshold.

Examples

Set the global threshold to 100 for triggering HTTP flood attack prevention in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] http-flood threshold 100
```

Related commands

- **http-flood action**
- **http-flood detect**
- **http-flood detect non-specific**

icmp-flood action

Use **icmp-flood action** to specify global actions against ICMP flood attacks.

Use **undo icmp-flood action** to restore the default.

Syntax

icmp-flood action { **drop** | **logging** } *

undo icmp-flood action

Default

No global action is specified for ICMP flood attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

drop: Drops subsequent ICMP packets destined for the victim IP addresses.

logging: Enables logging for ICMP flood attack events. The log information records the victim IP address, MPLS L3VPN instance name, current packet statistics, prevention actions, and start time of the attack.

Examples

Specify **drop** as the global action against ICMP flood attacks in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmp-flood action drop
```

Related commands

- **icmp-flood detect non-specific**
- **icmp-flood detect ip**

- **icmp-flood threshold**

icmp-flood detect ip

Use **icmp-flood detect ip** to configure IP address-specific ICMP flood attack detection.

Use **undo icmp-flood detect ip** to remove IP address-specific ICMP flood attack detection configuration.

Syntax

icmp-flood detect ip *ip-address* [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { **drop** | **logging** } *]

undo icmp-flood detect ip *ip-address* [**vpn-instance** *vpn-instance-name*]

Default

IP address-specific ICMP flood attack detection is not configured.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IPv4 address to be protected. The *ip-address* argument cannot be all 1s or 0s.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IP address is on the public network.

threshold *threshold-value*: Sets the threshold for triggering ICMP flood attack prevention. The value range is 1 to 1000000 in units of ICMP packets sent to the specified IP address per second.

action: Specifies the actions when an ICMP flood attack is detected. If no action is specified, the global actions set by the **icmp-flood action** command apply.

drop: Drops subsequent ICMP packets destined for the protected IP address.

logging: Enables logging for ICMP flood attack events. The log records the victim IP address, MPLS L3VPN instance name, current packet statistics, prevention action, and start time of the attack.

Usage guidelines

You can configure ICMP flood attack detection for multiple IP addresses in one attack defense policy. The supported maximum number varies by device model.

With ICMP flood attack detection configured, the device is in attack detection state. When the sending rate of ICMP packets to a protected IP address reaches or exceeds the threshold, the device enters prevention state and takes the specified actions. When the rate is below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

Examples

Configure ICMP flood attack detection for 192.168.1.2 in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmp-flood detect ip 192.168.1.2 threshold
2000
```

Related commands

- **icmp-flood action**
- **icmp-flood detect non-specific**
- **icmp-flood threshold**

icmp-flood detect non-specific

Use **icmp-flood detect non-specific** to enable global ICMP flood attack detection.

Use **undo icmp-flood detect non-specific** to restore the default.

Syntax

icmp-flood detect non-specific

undo icmp-flood detect non-specific

Default

Global ICMP flood attack detection is disabled.

Views

Attack defense policy view

Predefined user roles

network-admin

Usage guidelines

The global ICMP flood attack detection applies to all IP addresses except for those specified by the **icmp-flood detect ip** command. The global detection uses the global trigger threshold set by the **icmp-flood threshold** command and global actions specified by the **icmp-flood action** command.

Examples

Enable global ICMP flood attack detection in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmp-flood detect non-specific
```

Related commands

- **icmp-flood action**
- **icmp-flood detect ip**
- **icmp-flood threshold**

icmp-flood threshold

Use **icmp-flood threshold** to set the global threshold for triggering ICMP flood attack prevention.

Use **undo icmp-flood threshold** to restore the default.

Syntax

icmp-flood threshold *threshold-value*

undo icmp-flood threshold

Default

The global threshold is 1000 for triggering ICMP flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the threshold value. The value range is 1 to 1000000 in units of ICMP packets sent to an IP address per second.

Usage guidelines

The global threshold applies to global ICMP flood attack detection.

Adjust the threshold according to the application scenarios. If the number of ICMP packets sent to a protected server, such as an HTTP or FTP server, is normally large, set a large threshold. A small threshold might affect the server services. For a network that is unstable or susceptible to attacks, set a small threshold.

Examples

Set the global threshold to 100 for triggering ICMP flood attack prevention in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmp-flood threshold 100
```

Related commands

- **icmp-flood action**
- **icmp-flood detect ip**
- **icmp-flood detect non-specific**

icmpv6-flood action

Use **icmpv6-flood action** to specify global actions against ICMPv6 flood attacks.

Use **undo icmpv6-flood action** to restore the default.

Syntax

icmpv6-flood action { **drop** | **logging** } *

undo icmpv6-flood action

Default

No global action is specified for ICMPv6 flood attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

drop: Drops subsequent ICMPv6 packets destined for the victim IP addresses.

logging: Enables logging for ICMPv6 flood attack events. The log information records the victim IP address, MPLS L3VPN instance name, current packet statistics, prevention actions, and start time of the attack.

Examples

Specify **drop** as the global action against ICMPv6 flood attacks in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmpv6-flood action drop
```

Related commands

- **icmpv6-flood detect ipv6**
- **icmpv6-flood detect non-specific**
- **icmpv6-flood threshold**

icmpv6-flood detect ipv6

Use **icmpv6-flood detect ipv6** to configure IPv6 address-specific ICMPv6 flood attack detection.

Use **undo icmpv6-flood detect ipv6** to remove IPv6 address-specific ICMPv6 flood attack detection configuration.

Syntax

icmpv6-flood detect ipv6 *ipv6-address* [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { **drop** | **logging** } *]

undo icmpv6-flood detect ipv6 *ipv6-address* [**vpn-instance** *vpn-instance-name*]

Default

IPv6 address-specific ICMPv6 flood attack detection is not configured.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address to be protected.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IPv6 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IPv6 address is on the public network.

threshold *threshold-value*: Sets the threshold for triggering ICMPv6 flood attack prevention. The value range is 1 to 1000000 in units of ICMPv6 packets sent to the specified IP address per second.

action: Specifies the actions when an ICMPv6 flood attack is detected. If no action is specified, the global actions set by the **icmpv6-flood action** command apply.

drop: Drops subsequent ICMPv6 packets destined for the protected IPv6 address.

logging: Enables logging for ICMPv6 flood attack events. The log information records the victim IP address, MPLS L3VPN instance name, current packet statistics, prevention action, and start time of the attack.

Usage guidelines

You can configure ICMPv6 flood attack detection for multiple IPv6 addresses in one attack defense policy. The supported maximum number varies by device model.

With ICMPv6 flood attack detection configured, the device is in attack detection state. When the sending rate of ICMPv6 packets to a protected IPv6 address reaches or exceeds the threshold, the device enters prevention state and takes the specified actions. When the rate is below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

Examples

Configure ICMPv6 flood attack detection for 2012::12 in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmpv6-flood detect ipv6 2012::12 threshold
2000
```

Related commands

- **icmpv6-flood action**
- **icmpv6-flood detect non-specific**
- **icmpv6-flood threshold**

icmpv6-flood detect non-specific

Use **icmpv6-flood detect non-specific** to enable global ICMPv6 flood attack detection.

Use **undo icmpv6-flood detect non-specific** to restore the default.

Syntax

icmpv6-flood detect non-specific

undo icmpv6-flood detect non-specific

Default

Global ICMPv6 flood attack detection is disabled.

Views

Attack defense policy view

Predefined user roles

network-admin

Usage guidelines

The global ICMPv6 flood attack detection applies to all IPv6 addresses except for those specified by the **icmpv6-flood detect ipv6** command. The global detection uses the global trigger threshold set by the **icmpv6-flood threshold** command and global actions specified by the **icmpv6-flood action** command.

Examples

Enable global ICMPv6 flood attack detection in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmpv6-flood detect non-specific
```

Related commands

- **icmpv6-flood action**
- **icmpv6-flood detect ipv6**
- **icmpv6-flood threshold**

icmpv6-flood threshold

Use **icmpv6-flood threshold** to set the global threshold for triggering ICMPv6 flood attack prevention.

Use **undo icmpv6-flood threshold** to restore the default.

Syntax

icmpv6-flood threshold *threshold-value*

undo icmpv6-flood threshold

Default

The global threshold is 1000 for triggering ICMPv6 flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the threshold value. The value range is 1 to 1000000 in units of ICMPv6 packets sent to an IP address per second.

Usage guidelines

The global threshold applies to global ICMPv6 flood attack detection.

Adjust the threshold according to the application scenarios. If the number of ICMPv6 packets sent to a protected server, such as an HTTP or FTP server, is normally large, set a large threshold. A small threshold might affect the server services. For a network that is unstable or susceptible to attacks, set a small threshold.

Examples

Set the global threshold to 100 for triggering ICMPv6 flood attack prevention in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmpv6-flood threshold 100
```

Related commands

- **icmpv6-flood action**
- **icmpv6-flood detect ipv6**
- **icmpv6-flood detect non-specific**

reset attack-defense policy flood

Use **reset attack-defense policy flood statistics** to clear flood attack detection and prevention statistics.

Syntax

reset attack-defense policy *policy-name* **flood protected** { **ip** | **ipv6** } **statistics**

Views

User view

Predefined user roles

network-admin

network-operator

Parameters

policy-name: Specifies an attack defense policy by its name. The policy name is a case-insensitive string of 1 to 31 characters. Valid characters include uppercase and lowercase letters, digits, underscores (_), and hyphens (-).

ip: Clears flood attack detection and prevention statistics for IPv4 addresses.

ipv6: Clears flood attack detection and prevention statistics for IPv6 addresses.

Examples

Clear flood attack detection and prevention statistics for IPv4 addresses in the attack defense policy **abc**.

```
<Sysname> reset attack-defense policy abc flood protected ip statistics
```

Clear flood attack detection and prevention statistics for IPv6 addresses in the attack defense policy **abc**.

```
<Sysname> reset attack-defense policy abc flood protected ipv6 statistics
```

Related commands

- **display attack-defense policy ip**
- **display attack-defense policy ipv6**

reset attack-defense statistics local

Use **reset attack-defense statistics local** to clear attack detection and prevention statistics for the device.

Syntax

reset attack-defense statistics local

Views

User view

Predefined user roles

network-admin

network-operator

Examples

Clear attack detection and prevention statistics for the device.

```
<Sysname> reset attack-defense statistics local
```

Related commands

display attack-defense statistics local

rst-flood action

Use **rst-flood action** to specify global actions against RST flood attacks.

Use **undo rst-flood action** to restore the default.

Syntax

rst-flood action { **drop** | **logging** } *

undo rst-flood action

Default

No global action is specified for RST flood attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

drop: Drops subsequent RST packets destined for the victim IP addresses.

logging: Enables logging for RST flood attack events. The log information records the victim IP address, MPLS L3VPN instance name, current packet statistics, prevention actions, and start time of the attack.

Examples

Specify **drop** as the global action against RST flood attacks in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] rst-flood action drop
```

Related commands

- **rst-flood detect**
- **rst-flood detect non-specific**
- **rst-flood threshold**

rst-flood detect

Use **rst-flood detect** to configure IP address-specific RST flood attack detection.

Use **undo rst-flood detect** to remove IP address-specific RST flood attack detection configuration.

Syntax

rst-flood detect { **ip** *ip-address* **|** **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { **drop** **|** **logging** } *]

undo rst-flood detect { **ip** *ip-address* **|** **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

IP address-specific RST flood attack detection is not configured.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Specifies the IPv4 address to be protected. The *ip-address* argument cannot be all 1s or 0s.

ipv6 *ipv6-address*: Specifies the IPv6 address to be protected.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IP address is on the public network.

threshold *threshold-value*: Sets the threshold for triggering RST flood attack prevention. The value range is 1 to 1000000 in units of RST packets sent to the specified IP address per second.

action: Specifies the actions when an RST flood attack is detected. If no action is specified, the global actions set by the **rst-flood action** command apply.

drop: Drops subsequent RST packets destined for the protected IP address.

logging: Enables logging for RST flood attack events. The log information records the victim IP address, MPLS L3VPN instance name, current packet statistics, prevention action, and start time of the attack.

Usage guidelines

You can configure RST flood attack detection for multiple IP addresses in one attack defense policy. The supported maximum number varies by device model.

With RST flood attack detection configured, the device is in attack detection state. When the sending rate of RST packets to a protected IP address reaches or exceeds the threshold, the device enters prevention state and takes the specified actions. When the rate is below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

Examples

Configure RST flood attack detection for 192.168.1.2 in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] rst-flood detect ip 192.168.1.2 threshold 2000
```

Related commands

- **rst-flood action**
- **rst-flood detect non-specific**
- **rst-flood threshold**

rst-flood detect non-specific

Use **rst-flood detect non-specific** to enable global RST flood attack detection.

Use **undo rst-flood detect non-specific** to restore the default.

Syntax

rst-flood detect non-specific

undo rst-flood detect non-specific

Default

Global RST flood attack detection is disabled.

Views

Attack defense policy view

Predefined user roles

network-admin

Usage guidelines

The global RST flood attack detection applies to all IP addresses except for those specified by the **rst-flood detect** command. The global detection uses the global trigger threshold set by the **rst-flood threshold** command and global actions specified by the **rst-flood action** command.

Examples

Enable global RST flood attack detection in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] rst-flood detect non-specific
```

Related commands

- **rst-flood action**
- **rst-flood detect**
- **rst-flood threshold**

rst-flood threshold

Use **rst-flood threshold** to set the global threshold for triggering RST flood attack prevention.

Use **undo rst-flood threshold** to restore the default.

Syntax

rst-flood threshold *threshold-value*

undo rst-flood threshold

Default

The global threshold is 1000 for triggering RST flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the threshold value. The value range is 1 to 1000000 in units of RST packets sent to an IP address per second.

Usage guidelines

The global threshold applies to global RST flood attack detection.

Adjust the threshold according to the application scenarios. If the number of RST packets sent to a protected server, such as an HTTP or FTP server, is normally large, set a large threshold. A small threshold might affect the server services. For a network that is unstable or susceptible to attacks, set a small threshold.

Examples

Set the global threshold to 100 for triggering RST flood attack prevention in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] rst-flood threshold 100
```

Related commands

- **rst-flood action**
- **rst-flood detect**
- **rst-flood detect non-specific**

scan detect

Use **scan detect** to configure scanning attack detection.

Use **undo scan detect** to restore the default.

Syntax

scan detect level { **high** | **low** | **medium** } **action** { **drop** | **logging** } *

undo scan detect level { **high** | **low** | **medium** }

Default

Scanning attack detection is disabled.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

level: Specifies the level of the scanning attack detection.

low: Specifies the low level. This level provides basic scanning attack detection. It has a low false alarm rate but many scanning attacks cannot be detected.

high: Specifies the high level. This level can detect most of the scanning attacks, but has a high false alarm rate. Some packets from active hosts might be considered as attack packets.

medium: Specifies the medium level. Compared with the high and low levels, this level has a medium false alarm rate and attack detection rate.

action: Specifies the actions against scanning attacks.

drop: Drops subsequent packets from detected scanning attack sources.

logging: Enables logging for scanning attack events. The log information records the victim IP address, MPLS L3VPN instance name, current packet statistics, prevention action, and start time of the attack.

Examples

Configure low level scanning attack detection in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] scan detect level low action drop
```

signature { large-icmp | large-icmpv6 } max-length

Use **signature { large-icmp | large-icmpv6 } max-length** to set the maximum length of safe ICMP or ICMPv6 packets. A large ICMP or ICMPv6 attack occurs if an ICMP or ICMPv6 packet larger than the specified length is detected.

Use **undo signature { large-icmp | large-icmpv6 } max-length** to restore the default.

Syntax

signature { large-icmp | large-icmpv6 } max-length *length*

undo signature { large-icmp | large-icmpv6 } max-length

Default

The maximum length of safe ICMP or ICMPv6 packets is 4000 bytes.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

large-icmp: Specifies large ICMP packet attack signature.

large-icmpv6: Specifies large ICMPv6 packet attack signature.

length: Specifies the maximum length of safe ICMP or ICMPv6 packets, in bytes. The value range for ICMP packet is 28 to 65534. The value range for ICMPv6 packet is 48 to 65534.

Examples

Set the maximum length of safe ICMP packets for large ICMP attack to 50000 bytes.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] signature large-icmp max-length 50000
```

Related commands

signature detect

signature detect

Use **signature detect** to configure signature detection for single-packet attacks.

Use **undo signature detect** to remove the signature detection configuration for single-packet attacks.

Syntax

signature detect { **fraggle** | **fragment** | **impossible** | **ip-option-abnormal** | **land** | **large-icmp** | **large-icmpv6** | **ping-of-death** | **smurf** | **snork** | **tcp-all-flags** | **tcp-fin-only** | **tcp-invalid-flags** | **tcp-null-flag** | **tcp-syn-fin** | **teardrop** | **tiny-fragment** | **traceroute** | **udp-bomb** | **winnuke** } [**action** { { **drop** | **logging** } * | **none** }]

undo signature detect { **fraggle** | **fragment** | **impossible** | **ip-option-abnormal** | **land** | **large-icmp** | **large-icmpv6** | **ping-of-death** | **smurf** | **snork** | **tcp-all-flags** | **tcp-fin-only** | **tcp-invalid-flags** | **tcp-null-flag** | **tcp-syn-fin** | **teardrop** | **tiny-fragment** | **traceroute** | **udp-bomb** | **winnuke** }

signature detect icmp-type { *icmp-type-value* | **address-mask-reply** | **address-mask-request** | **destination-unreachable** | **echo-reply** | **echo-request** | **information-reply** | **information-request** | **parameter-problem** | **redirect** | **source-quench** | **time-exceeded** | **timestamp-reply** | **timestamp-request** } [**action** { { **drop** | **logging** } * | **none** }]

undo signature detect icmp-type { *icmp-type-value* | **address-mask-reply** | **address-mask-request** | **destination-unreachable** | **echo-reply** | **echo-request** | **information-reply** | **information-request** | **parameter-problem** | **redirect** | **source-quench** | **time-exceeded** | **timestamp-reply** | **timestamp-request** }

signature detect icmpv6-type { *icmpv6-type-value* **| destination-unreachable | echo-reply | echo-request | group-query | group-reduction | group-report | packet-too-big | parameter-problem | time-exceeded** } [**action** { { **drop | logging** } * **| none** }]

undo signature detect icmpv6-type { *icmpv6-type-value* **| destination-unreachable | echo-reply | echo-request | group-query | group-reduction | group-report | packet-too-big | parameter-problem | time-exceeded** }

signature detect ip-option { *option-code* **| internet-timestamp | loose-source-routing | record-route | route-alert | security | stream-id | strict-source-routing** } [**action** { { **drop | logging** } * **| none** }]

undo signature detect ip-option { *option-code* **| internet-timestamp | loose-source-routing | record-route | route-alert | security | stream-id | strict-source-routing** }

signature detect ipv6-ext-header *ext-header-value* [**action** { { **drop | logging** } * **| none** }]

undo signature detect ipv6-ext-header *next-header-value*

Default

Signature detection is not configured for any single-packet attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

fraggle: Specifies the fraggle attack.

fragment: Specifies the fragment attack.

icmp-type: Specifies an ICMP packet attack by its signature type. You can specify the signature by the ICMP packet type value or keyword:

- *icmp-type-value*: Specifies the ICMP type value in the range of 0 to 255.
- **address-mask-reply**: Specifies the ICMP address mask reply type.
- **address-mask-request**: Specifies the ICMP address mask request type.
- **destination-unreachable**: Specifies the ICMP destination unreachable type.
- **echo-reply**: Specifies the ICMP echo reply type.
- **echo-request**: Specifies the ICMP echo request type.
- **information-reply**: Specifies the ICMP information reply type.
- **information-request**: Specifies the ICMP information request type.
- **parameter-problem**: Specifies the ICMP parameter problem type.
- **redirect**: Specifies the ICMP redirect type.
- **source-quench**: Specifies the ICMP source quench type.
- **time-exceeded**: Specifies the ICMP time exceeded type.
- **timestamp-reply**: Specifies the ICMP timestamp reply type.
- **timestamp-request**: Specifies the ICMP timestamp request type.

icmpv6-type: Specifies an ICMPv6 packet attack by its signature type. You can specify the signature by the ICMPv6 packet type value or keyword.

- *icmpv6-type-value*: Specifies the ICMPv6 type value in the range of 0 to 255.
- **destination-unreachable**: Specifies the ICMPv6 destination unreachable type.
- **echo-reply**: Specifies the ICMPv6 echo reply type.

- **echo-request**: Specifies the ICMPv6 echo request type.
- **group-query**: Specifies the ICMPv6 group query type.
- **group-reduction**: Specifies the ICMPv6 group reduction type.
- **group-report**: Specifies the ICMPv6 group report type.
- **packet-too-big**: Specifies the ICMPv6 packet too big type.
- **parameter-problem**: Specifies the ICMPv6 parameter problem type.
- **time-exceeded**: Specifies the ICMPv6 time exceeded type.

impossible: Specifies the IP impossible packet attack.

ip-option: Specifies an IP option. You can specify the IP option by its value or keyword:

- *option-code*: Specifies the IP option value in the range of 0 to 255.
- **internet-timestamp**: Specifies the timestamp option.
- **loose-source-routing**: Specifies the loose source routing option.
- **record-route**: Specifies the record route option.
- **route-alert**: Specifies the route alert option.
- **security**: Specifies the security option.
- **stream-id**: Specifies the stream identifier option.
- **strict-source-routing**: Specifies the strict source route option.

ip-option-abnormal: Specifies the abnormal IP option attack.

ipv6-ext-header *ext-header-value*: Specifies an IPv6 extension header by its value in the range of 0 to 255. An IPv6 extension header attack occurs when the specified IPv6 extension header value is detected.

land: Specifies the Land attack.

large-icmp: Specifies the large ICMP packet attack.

large-icmpv6: Specifies the large ICMPv6 packet attack.

ping-of-death: Specifies the ping-of-death attack.

smurf: Specifies the smurf attack.

snork: Specifies the UDP snork attack.

tcp-all-flags: Specifies the attack where a TCP packet has all flags set.

tcp-fin-only: Specifies the attack where a single TCP FIN packet is sent to a privileged port (port number lower than 1024).

tcp-invalid-flags: Specifies the attack that uses TCP packets with invalid flags.

tcp-null-flag: Specifies the attack where a single TCP packet has no TCP flags set.

tcp-syn-fin: Specifies the attack where a TCP packet has both SYN and FIN flags set.

teardrop: Specifies the teardrop attack.

tiny-fragment: Specifies the tiny fragment attack.

traceroute: Specifies the traceroute attack.

udp-bomb: Specifies the UDP bomb attack.

winnuke: Specifies the WinNuke attack.

action: Specifies the actions against the single-packet attack. If you do not specify this keyword, the default action of the attack level to which the single-packet attack belongs is used.

drop: Drops packets that match the specified signature.

logging: Enables logging for the specified single-packet attack.

none: Takes no action.

Usage guidelines

One command execution enables signature detection for only one single-packet attack type. You can use this command multiple times to configure signature detection for multiple single-packet attack types.

When you specify a packet type by its value, if the packet type has a corresponding keyword, the keyword is displayed in command output. Otherwise, the value is displayed.

Examples

Configure signature detection for smurf attack in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] signature detect smurf action drop
```

Related commands

signature level action

signature level action

Use **signature level action** to specify the actions against single-packet attacks of a specific level.

Use **undo signature level action** to restore the default.

Syntax

signature level { **high** | **info** | **low** | **medium** } **action** { { **drop** | **logging** } * | **none** }

undo signature level { **high** | **info** | **low** | **medium** } **action**

Default

For informational-level and low-level single-packet attacks, the action is **logging**.

For medium-level and high-level single-packet attacks, the actions are **logging** and **drop**.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

high: Specifies the high level. None of the currently supported single-packet attacks belongs to this level.

info: Specifies the informational level. For example, large ICMP packet attack is of this level.

low: Specifies the low level. For example, the traceroute attack is of this level.

medium: Specifies the medium level. For example, the WinNuke attack is of this level.

drop: Drops packets that match the specified level.

logging: Enable logging for single-packet attacks of the specified level.

none: Takes no action.

Usage guidelines

According to their severity, single-packet attacks are divided into four levels: **info**, **low**, **medium**, and **high**.

If you enable the level-specific signature detection for single-packet attacks, the signature detection is enabled for all single-packet attacks of the level. If you enable the signature detection for a single-packet attack by using the **signature detect** command, action parameters in the **signature detect** command take effect.

Examples

Specify the action against informational-level single-packet attacks as **drop** in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy 1
[Sysname-attack-defense-policy-1] signature level info action drop
```

Related commands

- **signature detect**
- **signature level detect**

signature level detect

Use **signature level detect** to enable signature detection for single-packet attacks of a specific level.

Use **undo signature level detect** to disable signature detection for single-packet attacks of a specific level.

Syntax

signature level { **high** | **info** | **low** | **medium** } **detect**

undo signature level { **high** | **info** | **low** | **medium** } **detect**

Default

Signature detection is disabled for all levels of single-packet attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

high: Specifies the high level. None of the currently supported single-packet attacks belongs to this level.

info: Specifies the informational level. For example, large ICMP packet attack is of this level.

low: Specifies the low level. For example, the traceroute attack is of this level.

medium: Specifies the medium level. For example, the WinNuke attack is of this level.

Usage guidelines

According to their severity, single-packet attacks fall into four levels: **info**, **low**, **medium**, and **high**.

If you enable the level-specific signature detection for single-packet attacks, the signature detection is enabled for all single-packet attacks of the level. If you enable the signature detection for a single-packet attack by using the **signature detect** command, action parameters in the **signature detect** command take effect.

Use the **signature level action** command to specify the actions against single-packet attacks of a specific level. To display the level to which a single-packet attack belongs, use the **display attack-defense policy** command.

Examples

Enable signature detection for informational level single-packet attacks in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy 1
[Sysname-attack-defense-policy-1] signature level info detect
```

Related commands

- **display attack-defense policy**
- **signature detect**
- **signature level action**

syn-ack-flood action

Use **syn-ack-flood action** to specify global actions against SYN-ACK flood attacks.

Use **undo syn-ack-flood action** to restore the default.

Syntax

syn-ack-flood action { **drop** | **logging** } *

undo syn-ack-flood action

Default

No global action is specified for SYN-ACK flood attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

drop: Drops subsequent SYN-ACK packets destined for the victim IP addresses.

logging: Enables logging for SYN-ACK flood attack events. The log information records the victim IP address, MPLS L3VPN instance name, current packet statistics, prevention actions, and start time of the attack.

Examples

Specify **drop** as the global action against SYN-ACK flood attacks in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-ack-flood action drop
```

Related commands

- **syn-ack-flood detect**
- **syn-ack-flood detect non-specific**
- **syn-ack-flood threshold**

syn-ack-flood detect

Use **syn-ack-flood detect** to configure IP address-specific SYN-ACK flood attack detection.

Use **undo syn-ack-flood detect** to remove IP address-specific SYN-ACK flood attack detection configuration.

Syntax

syn-ack-flood detect { **ip** *ip-address* **| ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { **drop | logging** } *]

undo syn-ack-flood detect { **ip** *ip-address* **| ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

IP address-specific SYN-ACK flood attack detection is not configured.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Specifies the IPv4 address to be protected. The *ip-address* argument cannot be all 1s or 0s.

ipv6 *ipv6-address*: Specifies the IPv6 address to be protected.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IP address is on the public network.

threshold *threshold-value*: Sets the threshold for triggering SYN-ACK flood attack prevention. The value range is 1 to 1000000 in units of SYN-ACK packets sent to the specified IP address per second.

action: Specifies the actions when a SYN-ACK flood attack is detected. If no action is specified, the global actions set by the **syn-ack-flood action** command apply.

drop: Drops subsequent SYN-ACK packets destined for the protected IP address.

logging: Enables logging for SYN-ACK flood attack events. The log information records the victim IP address, MPLS L3VPN instance name, current packet statistics, prevention action, and start time of the attack.

Usage guidelines

You can configure SYN-ACK flood attack detection for multiple IP addresses in one attack defense policy. The supported maximum number varies by device model.

With SYN-ACK flood attack detection configured, the device is in attack detection state. When the sending rate of SYN-ACK packets to a protected IP address reaches or exceeds the threshold, the device enters prevention state and takes the specified actions. When the rate is below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

Examples

Configure SYN-ACK flood attack detection for 192.168.1.2 in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-ack-flood detect ip 192.168.1.2
threshold 2000
```

Related commands

- **syn-ack-flood action**

- **syn-ack-flood detect non-specific**
- **syn-ack-flood threshold**

syn-ack-flood detect non-specific

Use **syn-ack-flood detect non-specific** to enable global SYN-ACK flood attack detection.

Use **undo syn-ack-flood detect non-specific** to restore the default.

Syntax

syn-ack-flood detect non-specific

undo syn-ack-flood detect non-specific

Default

Global SYN-ACK flood attack detection is disabled.

Views

Attack defense policy view

Predefined user roles

network-admin

Usage guidelines

The global SYN-ACK flood attack detection applies to all IP addresses except for those specified by the **syn-ack-flood detect** command. The global detection uses the global trigger threshold set by the **syn-ack-flood threshold** command and global actions specified by the **syn-ack-flood action** command.

Examples

Enable global SYN-ACK flood attack detection in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-ack-flood detect non-specific
```

Related commands

- **syn-ack-flood action**
- **syn-ack-flood detect**
- **syn-ack-flood threshold**

syn-ack-flood threshold

Use **syn-ack-flood threshold** to set the global threshold for triggering SYN-ACK flood attack prevention.

Use **undo syn-ack-flood threshold** to restore the default.

Syntax

syn-ack-flood threshold *threshold-value*

undo syn-ack-flood threshold

Default

The global threshold is 1000 for triggering SYN-ACK flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the threshold value. The value range is 1 to 1000000 in units of SYN-ACK packets sent to an IP address per second.

Usage guidelines

The global threshold applies to global SYN-ACK flood attack detection.

Adjust the threshold according to the application scenarios. If the number of SYN-ACK packets sent to a protected server, such as an HTTP or FTP server, is normally large, set a large threshold. A small threshold might affect the server services. For a network that is unstable or susceptible to attacks, set a small threshold.

Examples

Set the global threshold to 100 for triggering SYN-ACK flood attack prevention in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-ack-flood threshold 100
```

Related commands

- **syn-ack-flood action**
- **syn-ack-flood detect**
- **syn-ack-flood detect non-specific**

syn-flood action

Use **syn-flood action** to specify global actions against SYN flood attacks.

Use **undo syn-flood action** to restore the default.

Syntax

syn-flood action { **drop** | **logging** } *

undo syn-flood action

Default

No global action is specified SYN flood attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

drop: Drops subsequent SYN packets destined for the victim IP addresses.

logging: Enables logging for SYN flood attack events. The log information records the victim IP address, MPLS L3VPN instance name, current packet statistics, prevention actions, and start time of the attack.

Examples

Specify **drop** as the global action against SYN flood attacks in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-flood action drop
```

Related commands

- **syn-flood detect**
- **syn-flood detect non-specific**
- **syn-flood threshold**

syn-flood detect

Use **syn-flood detect** to configure IP address-specific SYN flood attack detection.

Use **undo syn-flood detect** to remove IP address-specific SYN flood attack detection configuration.

Syntax

syn-flood detect { **ip** *ip-address* **| ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { **drop | logging** } *]

undo syn-flood detect { **ip** *ip-address* **| ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

IP address-specific SYN flood attack detection is not configured.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Specifies the IPv4 address to be protected. The *ip-address* argument cannot be all 1s or 0s.

ipv6 *ipv6-address*: Specifies the IPv6 address to be protected.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IP address is on the public network.

threshold *threshold-value*: Sets the threshold for triggering SYN flood attack prevention. The value range is 1 to 1000000 in units of SYN packets sent to the specified IP address per second.

action: Specifies the actions when a SYN flood attack is detected. If no action is specified, the global actions set by the **syn-flood action** command apply.

drop: Drops subsequent SYN packets destined for the protected IP address.

logging: Enables logging for SYN flood attack events. The log information records the victim IP address, MPLS L3VPN instance name, current packet statistics, prevention action, and start time of the attack.

Usage guidelines

You can configure SYN flood attack detection for multiple IP addresses in one attack defense policy. The supported maximum number varies by device model.

With SYN flood attack detection configured, the device is in attack detection state. When the sending rate of SYN packets to a protected IP address reaches or exceeds the threshold, the device enters prevention state and takes the specified actions. When the rate is below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

Examples

Configure SYN flood attack detection for 192.168.1.2 in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-flood detect ip 192.168.1.2 threshold
2000
```

Related commands

- **syn-flood action**
- **syn-flood detect non-specific**
- **syn-flood threshold**

syn-flood detect non-specific

Use **syn-flood detect non-specific** to enable global SYN flood attack detection.

Use **undo syn-flood detect non-specific** to restore the default.

Syntax

syn-flood detect non-specific

undo syn-flood detect non-specific

Default

Global SYN flood attack detection is disabled.

Views

Attack defense policy view

Predefined user roles

network-admin

Usage guidelines

The global SYN flood attack detection applies to all IP addresses except for those specified by the **syn-flood detect** command. The global detection uses the global trigger threshold set by the **syn-flood threshold** command and global actions specified by the **syn-flood action** command.

Examples

Enable global SYN flood attack detection in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-flood detect non-specific
```

Related commands

- **syn-flood action**
- **syn-flood detect**
- **syn-flood threshold**

syn-flood threshold

Use **syn-flood threshold** to set the global threshold for triggering SYN flood attack prevention.

Use **undo syn-flood threshold** to restore the default.

Syntax

syn-flood threshold *threshold-value*

undo syn-flood threshold

Default

The global threshold is 1000 for triggering SYN flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the threshold value. The value range is 1 to 1000000 in units of SYN packets sent to an IP address per second.

Usage guidelines

The global threshold applies to global SYN flood attack detection.

Adjust the threshold according to the application scenarios. If the number of SYN packets sent to a protected server, such as an HTTP or FTP server, is normally large, set a large threshold. A small threshold might affect the server services. For a network that is unstable or susceptible to attacks, set a small threshold.

Examples

Set the global threshold to 100 for triggering SYN flood attack prevention in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-flood threshold 100
```

Related commands

- **syn-flood action**
- **syn-flood detect**
- **syn-flood detect non-specific**

udp-flood action

Use **udp-flood action** to specify global actions against UDP flood attacks.

Use **undo udp-flood action** to restore the default.

Syntax

udp-flood action { **drop** | **logging** } *

undo udp-flood action

Default

No global action is specified for UDP flood attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

drop: Drops subsequent UDP packets destined for the victim IP addresses.

logging: Enables logging for UDP flood attack events. The log information records the victim IP address, MPLS L3VPN instance name, current packet statistics, prevention actions, and start time of the attack.

Examples

Specify **drop** as the global action against UDP flood attacks in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] udp-flood action drop
```

Related commands

- **udp-flood detect**
- **udp-flood detect non-specific**
- **udp-flood threshold**

udp-flood detect

Use **udp-flood detect** to configure IP address-specific UDP flood attack detection.

Use **undo udp-flood detect** to remove IP address-specific UDP flood attack detection configuration.

Syntax

udp-flood detect { **ip** *ip-address* **|** **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { **drop** | **logging** } *]

undo udp-flood detect { **ip** *ip-address* **|** **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

IP address-specific UDP flood attack detection is not configured.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Specifies the IPv4 address to be protected. The *ip-address* argument cannot be all 1s or 0s.

ipv6 *ipv6-address*: Specifies the IPv6 address to be protected.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IP address is on the public network.

threshold *threshold-value*: Sets the threshold for triggering UDP flood attack prevention. The value range is 1 to 64000 in units of UDP packets sent to the specified IP address per second.

action: Specifies the actions when a UDP flood attack is detected. If no action is specified, the global actions set by the **udp-flood action** command apply.

drop: Drops subsequent UDP packets destined for the protected IP address.

logging: Enables logging for UDP flood attack events. The log information records the victim IP address, MPLS L3VPN instance name, current packet statistics, prevention action, and start time of the attack.

Usage guidelines

You can configure UDP flood attack detection for multiple IP addresses in one attack defense policy. The supported maximum number varies by device model.

With UDP flood attack detection configured, the device is in attack detection state. When the sending rate of UDP packets to a protected IP address reaches or exceeds the threshold, the device enters prevention state and takes the specified actions. When the rate is below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

Examples

Configure UDP flood attack detection for 192.168.1.2 in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] udp-flood detect ip 192.168.1.2 threshold
2000
```

Related commands

- **udp-flood action**
- **udp-flood detect non-specific**
- **udp-flood threshold**

udp-flood detect non-specific

Use **udp-flood detect non-specific** to enable global UDP flood attack detection.

Use **undo udp-flood detect non-specific** to restore the default.

Syntax

udp-flood detect non-specific

undo udp-flood detect non-specific

Default

Global UDP flood attack detection is disabled.

Views

Attack defense policy view

Predefined user roles

network-admin

Usage guidelines

The global UDP flood attack detection applies to all IP addresses except for those specified by the **udp-flood detect** command. The global detection uses the global trigger threshold set by the **udp-flood threshold** command and global actions specified by the **udp-flood action** command.

Examples

Enable global UDP flood attack detection in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
```

```
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] udp-flood detect non-specific
```

Related commands

- **udp-flood action**
- **udp-flood detect**
- **udp-flood threshold**

udp-flood threshold

Use **udp-flood threshold** to set the global threshold for triggering UDP flood attack prevention.

Use **undo udp-flood threshold** to restore the default.

Syntax

udp-flood threshold *threshold-value*

undo udp-flood threshold

Default

The global threshold is 1000 for triggering UDP flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the threshold value. The value range is 1 to 64000 in units of UDP packets sent to an IP address per second.

Usage guidelines

The global threshold applies to global UDP flood attack detection.

Adjust the threshold according to the application scenarios. If the number of UDP packets sent to a protected server, such as an HTTP or FTP server, is normally large, set a large threshold. A small threshold might affect the server services. For a network that is unstable or susceptible to attacks, set a small threshold.

Examples

Set the global threshold to 100 for triggering UDP flood attack prevention in the attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] rst-flood threshold 100
```

Related commands

- **udp-flood action**
- **udp-flood detect**
- **udp-flood detect non-specific**

New feature: Configuration commit delay

Configuring the configuration commit delay feature

This feature requires a manual commit within the allowed delay time to retain the settings configured after the **configuration commit delay** command was executed. If no manual commit is performed within the allowed delay time, the device rolls back the configuration to the settings before the **configuration commit delay** command was executed.

To configure the configuration commit delay feature:

Step	Command
1. Enter system view.	**system-view**
2. Set the allowed delay time for a manual commit to keep the settings configured subsequently in effect.	**configuration commit delay** *delay-time*
3. (Optional.) Commit the settings configured after the **configuration commit delay** command was executed.	**configuration commit**

Command reference

New command: configuration commit

Use **configuration commit** to commit the settings configured after the **configuration commit delay** command was executed.

Syntax

configuration commit

Views

System view

Predefined user roles

network-admin

Usage guidelines

You must execute the **configuration commit delay** command before executing this command.

As a best practice, you enable the information center and configure the information center to output logs to the console. Determine whether to commit the settings depending on the logs. For more information about the information center, see information center configuration in the network management and monitoring configuration guide for the device.

Examples

Set the allowed delay time to 10 minutes for a manual commit to keep the settings configured subsequently in effect.

```
<Sysname> system-view
[Sysname] configuration commit delay 10
```

Commit the settings configured after the **configuration commit delay** command was executed.

```
[Sysname] configuration commit
```

Commit the settings configured after the **configuration commit delay** command was executed. In this example, the commit operation fails, because the allowed delay time has expired. The device is rolling back the configuration to the settings before the **configuration commit delay** command was executed.

```
[Sysname] configuration commit
The system is rolling back configuration. Please wait…
```

New command: configuration commit delay

Use **configuration commit delay** to set the allowed delay time for a manual commit to keep the settings configured subsequently in effect.

Syntax

configuration commit delay *delay-time*

Views

System view

Predefined user roles

network-admin

Parameters

delay-time: Sets the allowed delay time in the range of 1 to 65535, in minutes.

Usage guidelines

Configure this command in a single-user environment.

If you do not execute the **configuration commit** command within the delay time, the device rolls back the configuration to the settings before the **configuration commit delay** command was executed. The device outputs logs to notify the user of the rollback operation. The user cannot perform other operations before the rollback is finished.

You can change the allowed delay time before the previous configured delay time expires. The new delay time configuration overwrites the previous delay time configuration after you enter **Y** to confirm the change. The allowed delay time is reset.

As a best practice, you execute this command in the following situations:

- The user configures the device remotely. The user might be disconnected from the device because of a setting. If the **configuration commit delay** command is configured and the setting is not committed, the user can reconnect to the device after the delay time expires.
- The user is not familiar with the device configuration. If any parameters are configured incorrectly, the rollback mechanism can remove the incorrect settings after the delay time expires.

Examples

Set the allowed delay time to 10 minutes for a manual commit to keep the settings configured subsequently in effect.

```
<Sysname> system-view
[Sysname] configuration commit delay 10
```

Re-set the allowed delay time to 60 minutes for a manual commit to keep the settings configured subsequently in effect.

```
[Sysname] configuration commit delay 60
The commit delay already set 10 minutes, overwrite it? [Y/N]:y
```

Re-set the allowed delay time to 20 minutes for a manual commit to keep the settings configured subsequently in effect. In this example, the configuration fails, because the previous configured delay time has expired. The device is rolling back the configuration to the settings before the **configuration commit delay** command was executed the previous time.

```
[Sysname] configuration commit delay 20
The system is rolling back configuration. Please wait…
```

New feature: IP address assignment to the management Ethernet port of an IRF member device

Assigning an IP address to the management Ethernet port of an IRF member device

In an IRF fabric, no IP addresses can be assigned to the management Ethernet ports of subordinates. If a subordinate is elected as the new master after an IRF fabric split, the management Ethernet port of the new master cannot be used for troubleshooting. To resolve the problem, this release allows you to assign an IP address to the management Ethernet port of each member in the management Ethernet port view of the master.

In an IRF fabric, only the IP address assigned to the management Ethernet port of the master takes effect. After an IRF fabric split, the IP address assigned to the management Ethernet port of the new master (original subordinate) takes effect. Then you can use this IP address to log in to the device for troubleshooting.

When you assign an IP address to the management Ethernet port of an IRF member device, follow these restrictions and guidelines:

- The following commands are mutually exclusive. You cannot configure all on the management Ethernet port of the master.
    - The **ip address** command with the **irf-member** *member-id* option that specifies the master.
    - The **ip address** command that does not contain the **irf-member** *member-id* option.
    - The **ip address dhcp-alloc** command.
- Avoid an IP address conflict when you assign IP addresses to the management Ethernet ports of subordinates. The system does not prompt an IP address conflict because the IP addresses assigned to the management Ethernet ports of subordinates do not take effect.
- Exclude the management Ethernet port of the master from being shut down when the MAD status transits to Recovery.

After an IRF split, the routing information on the original master might not be updated immediately. As a result, the management Ethernet port of the original master cannot be pinged from the master (original subordinate) in another IRF fabric. To resolve the problem, wait until route synchronization between the devices is completed or enable NSR for the routing protocol.

To assign an IP address to the management Ethernet port of an IRF member device:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable management Ethernet port view.	**interface M-GigabitEthernet** *interface-number*	N/A
3. Assign an IP address to	**ip address** *ip-address* { *mask-length*	By default, no IP address is

Step	Command	Remarks
the management Ethernet port of an IRF member device.	| *mask* } **irf-member** *member-id*	assigned to the management Ethernet port of an IRF member device. You can execute this command multiple times to assign an IP address to each IRF member device. The IP addresses assigned to the management Ethernet ports of all IRF member devices must be in the same subnet.

Command reference

Modified command: ip address

Old syntax

ip address *ip-address* { *mask-length* **|** *mask* } [**sub**]

undo ip address [*ip-address* { *mask-length* **|** *mask* } [**sub**]]

New syntax

ip address *ip-address* { *mask-length* **|** *mask* } [**irf-member** *member-id* **|** **sub**]

undo ip address [*ip-address* { *mask-length* **|** *mask* } [**irf-member** *member-id* **|** **sub**]]

Views

Management Ethernet port view

Parameters

irf-member *member-id*: Specifies an IRF member device by its member ID in the range of 1 to 10.

Change description

Before modification: The **irf-member** *member-id* option was not supported.

After modification: The **irf-member** *member-id* option was added. If you specify this option, this command assigns an IP address to the management Ethernet port of the specified IRF member device.

New feature: DHCP snooping logging

Enabling DHCP snooping logging

The DHCP snooping logging feature enables the DHCP snooping device to generate DHCP snooping log messages and send them to the information center. You can configure the log destination and output rule in the information center.

Disable this feature when the log generation affects the device performance.

To enable DHCP snooping logging:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Enable DHCP snooping logging.	**dhcp snooping log enable**	By default, DHCP snooping logging is disabled.

Command reference

dhcp snooping log enable

Use **dhcp snooping log enable** to enable DHCP snooping logging.

Use **undo dhcp snooping log enable** to restore the default.

Syntax

dhcp snooping log enable

undo dhcp snooping log enable

Default

DHCP snooping logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the DHCP snooping device to generate DHCP snooping log messages and send them to the information center. You can configure the log destination and output rule in the information center.

Disable this feature when the log generation affects the device performance.

Examples

Enable DHCP snooping logging.

```
<Sysname> system-view
[Sysname] dhcp snooping log enable
```

New feature: DHCPv6 snooping logging

Enabling DHCPv6 snooping logging

The DHCPv6 snooping logging feature enables the DHCPv6 snooping device to generate DHCPv6 snooping log messages and send them to the information center. You can configure the log destination and output rule in the information center.

Disable this feature when the log generation affects the device performance.

To enable DHCPv6 snooping logging:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable DHCPv6 snooping	**ipv6 dhcp snooping log enable**	By default, DHCPv6 snooping

Step	Command	Remarks
logging.		logging is disabled.

Command reference

ipv6 dhcp snooping log enable

Use **ipv6 dhcp snooping log enable** to enable DHCPv6 snooping logging.

Use **undo ipv6 dhcp snooping log enable** to restore the default.

Syntax

ipv6 dhcp snooping log enable

undo ipv6 dhcp snooping log enable

Default

DHCPv6 snooping logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the DHCPv6 snooping device to generate DHCPv6 snooping log messages and send them to the information center. You can configure the log destination and output rule in the information center.

Disable this feature when the log generation affects the device performance.

Examples

Enable DHCPv6 snooping logging.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping log enable
```

New feature: Logging of BGP route flapping

Enabling the logging of BGP route flapping

Perform this task to enable BGP to log route flapping events. The logs are sent to the information center. The output rules of the logs (whether to output the logs and where to output) are determined by the information center configuration.

For more information about information center configuration, see *Network Management and Monitoring Configuration Guide*.

To enable the logging of BGP route flapping (IPv4 unicast/VPNv4):

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter BGP IPv4 unicast address family view, BGP-VPN IPv4 unicast address family view, BGP VPNv4 address family view, or BGP-VPN VPNv4 address family view.	• Enter BGP IPv4 unicast address family view: **a.** **bgp** *as-number* **b.** **address-family ipv4** [**unicast**] • Enter BGP-VPN IPv4 unicast address family view: **c.** **bgp** *as-number* **d.** **ip vpn-instance** *vpn-instance-name* **e.** **address-family ipv4** [**unicast**] • Enter BGP VPNv4 address family view: **f.** **bgp** *as-number* **g.** **address-family vpnv4** • Enter BGP-VPN VPNv4 address family view: **h.** **bgp** *as-number* **i.** **ip vpn-instance** *vpn-instance-name* **j.** **address-family vpnv4**	N/A
3. Enable the logging of BGP route flapping.	**log-route-flap** *monitor-time* *monitor-count* [*log-count-limit* | **route-policy** *route-policy-name*] *	By default, logging of BGP route flapping is disabled.

To enable the logging of BGP route flapping (IPv6 unicast/VPNv6):

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter BGP IPv6 unicast address family view, BGP-VPN IPv6 unicast address family view, or BGP VPNv6 address family view.	• Enter BGP IPv6 unicast address family view: **a.** **bgp** *as-number* **b.** **address-family ipv6** [**unicast**] • Enter BGP-VPN IPv6 unicast address family view: **c.** **bgp** *as-number* **d.** **ip vpn-instance** *vpn-instance-name* **e.** **address-family ipv6** [**unicast**] • Enter BGP VPNv6 address family view: **f.** **bgp** *as-number* **g.** **address-family vpnv6**	N/A
3. Enable the logging of BGP route flapping.	**log-route-flap** *monitor-time* *monitor-count* [*log-count-limit* | **route-policy** *route-policy-name*] *	By default, logging of BGP route flapping is disabled.

Command reference

log-route-flap

Use **log-route-flap** to enable the logging of BGP route flapping.

Use **undo log-route-flap** to restore the default.

Syntax

log-route-flap *monitor-time monitor-count* [*log-count-limit* **|** **route-policy** *route-policy-name*] *

undo log-route-flap

Default

Logging of BGP route flapping is disabled.

Views

BGP IPv4 unicast address family view, BGP-VPN IPv4 unicast address family view, BGP-VPN IPv6 unicast address family view, BGP VPNv4 address family view, BGP-VPN VPNv4 address family view, BGP VPNv6 address family view, BGP IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

monitor-time: Specifies the monitoring interval for route flapping events, in the range of 1 to 600 minutes.

monitor-count: Specifies the number of route flapping events that triggers a log, in the range of 2 to 8.

log-count-limit: Specifies the maximum number of logs that can be generated every minute. The value range for this argument is 1 to 600 and the default value is 200.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

After you configure this command, BGP logs route flapping events. The logs are sent to the information center of the device. The output rules of the logs (whether to output the logs and where to output) are determined by the information center configuration. For more information about information center configuration, see *Network Management and Monitoring Configuration Guide*.

This command is applicable only to routes received from BGP peers of the specified address family.

Examples

In BGP IPv4 unicast address family view, enable the logging of BGP route flapping, and set the *monitor-time*, *monitor-count*, and *log-count-limit* arguments to 10 minutes, 5, and 100, respectively.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] log-route-flap 10 5 100
```

New feature: RADIUS DAE server

Configuring the RADIUS DAE server feature

Dynamic Authorization Extensions (DAE) to RADIUS, defined in RFC 5176, can log off online users or change their authorization information. DAE uses the client/server model.

In a RADIUS network, the RADIUS server typically acts as the DAE client and the NAS acts as the DAE server.

When the RADIUS DAE server feature is enabled, the NAS performs the following operations:

1. Listens to the default or specified UDP port to receive DAE requests.
2. Logs off online users who match the criteria in the requests, or changes their authorization information.
3. Sends DAE responses to the DAE client.

DAE defines the following types of packets:

- **Disconnect Messages (DMs)**—The DAE client sends DM requests to the DAE server to log off specific online users.
- **Change of Authorization Messages (CoA Messages)**—The DAE client sends CoA requests to the DAE server to change the authorization information of specific online users.

To configure the RADIUS DAE server feature:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable the RADIUS DAE server feature and enter RADIUS DAE server view.	**radius dynamic-author server**	By default, the RADIUS DAE server feature is disabled.
3. Specify a RADIUS DAE client.	**client** { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**key** { **cipher** | **simple** } *string* | **vpn-instance** *vpn-instance-name*] *	By default, no RADIUS DAE client is specified.
4. Specify the RADIUS DAE server port.	**port** *port-number*	By default, the RADIUS DAE server port is 3799.

Command reference

client

Use **client** to specify a RADIUS DAE client.

Use **undo client** to remove the specified RADIUS DAE client.

Syntax

client { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**key** { **cipher** | **simple** } *string* | **vpn-instance** *vpn-instance-name*] *

undo client { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

No RADIUS DAE client is specified.

Views

RADIUS DAE server view

Predefined user roles

network-admin

mdc-admin

Parameters

ip *ipv4-address*: Specifies a DAE client by its IPv4 address.

ipv6 *ipv6-address*: Specifies a DAE client by its IPv6 address.

key { **cipher | simple** } *string*: Sets the shared key for secure communication between the RADIUS DAE client and server. Make sure the shared key is the same as the key configured on the RADIUS DAE client. If the RADIUS DAE client does not have any shared key, do not specify this option.

- **cipher** *string*: Sets a ciphertext shared key. The *string* argument is case sensitive.
  - In non-FIPS mode, the key is a string of 1 to 117 characters.
  - In FIPS mode, the key is a string of 15 to 117 characters.
- **simple** *string*: Sets a plaintext shared key. The *string* argument is case sensitive.
  - In non-FIPS mode, the key is a string of 1 to 64 characters.
  - In FIPS mode, the key is a string of 15 to 64 characters. The string must contain characters from digits, uppercase letters, lowercase letters, and special characters.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN to which the RADIUS DAE client belongs, where the *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option. Support for this option depends on the device model.

Usage guidelines

The device discards DAE packets sent from DAE clients that are not specified for the DAE server.

You can execute the **client** command multiple times to specify multiple DAE clients for the DAE server.

Examples

Specify the DAE client as 10.110.1.2 in MPLS L3VPN **abc**. Set the shared key to **123456** in plain text for secure communication between the DAE server and client.

```
<Sysname> system-view
[Sysname] radius dynamic-author server
[Sysname-radius-da-server] client ip 10.110.1.2 key simple 123456 vpn-instance abc
```

port

Use **port** to specify the RADIUS DAE server port.

Use **undo port** to restore the default.

Syntax

port *port-number*

undo port

Default

The port number is 3799.

Views

RADIUS DAE server view

Predefined user roles

network-admin

mdc-admin

Parameters

port-number: Specifies a UDP port number in the range of 1 to 65535.

Usage guidelines

The destination port in DAE packets on the DAE client must be the same as the RADIUS DAE server port on the DAE server.

Examples

Enable the RADIUS DAE server to listen to UDP port 3790 for DAE requests.

```
<Sysname> system-view
[Sysname] radius dynamic-author server
[Sysname-radius-da-server] port 3790
```

radius dynamic-author server

Use **radius dynamic-author server** to enable the RADIUS DAE server feature and enter RADIUS DAE server view.

Use **undo radius dynamic-author server** to restore the default.

Syntax

radius dynamic-author server

undo radius dynamic-author server

Default

The RADIUS DAE server feature is disabled.

Views

System view

Predefined user roles

network-admin

mdc-admin

Usage guidelines

When you enable the RADIUS DAE server feature, the device listens to UDP port 3799 to receive DAE packets from specified DAE clients.

Examples

Enable the RADIUS DAE server feature and enter RADIUS DAE server view.

```
<Sysname> system-view
[Sysname] radius dynamic-author server
[Sysname-radius-da-server]
```

New feature: Configuring service loopback group-based remote flow mirroring

Configuring service loopback group-based remote flow mirroring

Service loopback group-based remote flow mirroring works as follows:

1. The source device mirrors packets to the interface specified in the **mirror-to** command.
2. The interface redirects the mirrored packets to its associated tunnel interface.
3. The tunnel interface sends the packets through the GRE tunnel to the tunnel interface on the destination device.
4. The destination device copies the received packets and forwards them out of the interface that connects to the monitor server.

To configure service loopback group-based remote flow mirroring:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a class and enter class view.	**traffic classifier** *tcl-name* [**operator** { **and** | **or** }]	By default, no traffic class exists.
3. Configure match criteria.	**if-match** [**not**] *match-criteria*	By default, no match criterion is configured in a traffic class.
4. Return to system view.	**quit**	N/A
5. Create a traffic behavior and enter traffic behavior view.	**traffic behavior** *behavior-name*	By default, no traffic behavior exists.
6. Configure a mirroring action for the traffic behavior.	**mirror-to interface** *interface-type interface-number* **loopback**	By default, no mirroring action is configured for a traffic behavior.
7. Configure and apply a QoS policy.	See *ACL and QoS Configuration Guide*.	N/A

Command reference

mirror-to loopback

Use **mirror-to loopback** to configure a mirroring action for a traffic behavior.

Use **undo mirror-to** to delete a mirroring action.

Syntax

mirror-to interface *interface-type interface-number* **loopback**

undo mirror-to interface *interface-type interface-number*

Default

No mirroring action is configured for a traffic behavior.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

Examples

Configure service loopback group-based remote flow mirroring to mirror traffic to the interface Ten-GigabitEthernet 1/0/1 for traffic behavior 1.

```
<Sysname> system-view
[Sysname] traffic behavior 1
[Sysname-behavior-1] mirror-to interface ten-gigabitethernet 1/0/1 loopback
```

New feature: Display the FCoE configuration of a VLAN

Display the FCoE configuration of a VLAN

Use **display fcoe vlan** to display the FCoE configuration of a VLAN.

Command reference

display fcoe vlan

Use **display fcoe vlan** to display the FCoE configuration of a VLAN.

Syntax

display fcoe vlan *vlan-id*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Specifies a VLAN by its ID in the range of 1 to 4094.

Usage guidelines

Only FCF-NPV switches support this command.

Examples

Display the FCoE configuration of VLAN 10.

```
<Sysname> display fcoe vlan 10
FCoE information of VLAN 10:
  FCoE MAC    : 0000-2345-0202
```

```
FC-MAP      : 0x0efc01
FCF Priority: 128
FKA period  : 8 seconds
```

Table 33 Command output

Field	Description
FCoE MAC	FCoE MAC address of the switch.
FC-MAP	FC-MAP value.
FCF Priority	System FCF priority.
FKA period	Interval at which a VFC interface sends Discovery Solicitations and unsolicited Discovery Advertisements.

New feature: Flow entry for filtering slow protocol packets

Creating a flow entry for filtering slow protocol packets

Perform this task to create a flow entry for filtering slow protocol (such as LACP, LAMP, and OAM) packets. The action of this entry is to drop packets. This entry has a higher priority than other flow entries deployed by the controller.

To create a flow entry for filtering slow protocol packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create an OpenFlow instance and enter its view.	**openflow instance** *instance-id*	By default, no OpenFlow instance exists.
3. Create a flow entry for filtering slow protocol packets.	**protocol-packet filter slow**	By default, an OpenFlow instance does not have a flow entry for filtering slow protocol packets.

Command reference

protocol-packet filter slow

Use **protocol-packet filter slow** to create a flow entry for filtering slow protocol packets.

Use **undo protocol-packet filter slow** to restore the default.

Syntax

protocol-packet filter slow

undo protocol-packet filter slow

Default

An OpenFlow instance does not have a flow entry for filtering slow protocol packets.

Views

OpenFlow instance view

Predefined user roles

network-admin

Parameters

slow: Specifies slow protocol packets. The slow protocols include LACP, LAMP, and OAM.

Examples

Create a flow entry for OpenFlow instance 1 to filter slow protocol packets.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] protocol-packet filter slow
```

New feature: Display the status of a VSAN

Display the status of a VSAN

Use **display vsan status** to display the status of a VSAN.

Command reference

display vsan status

Use **display vsan status** to display the status of a VSAN.

Syntax

display vsan [*vsan-id*] **status**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vsan-id: Specifies a VSAN by its ID in the range of 1 to 3839. If you do not specify a VSAN, this command displays the status of each VSAN.

Usage guidelines

Only FCF-NPV switches support this command.

Examples

Display the status of each VSAN.

```
<Sysname> display vsan status
VSAN 1:
```

```
  Name: VSAN0001
  Working mode: NPV

VSAN 10:
  Name: VSAN0010
  Working mode: NPV
```

New feature: Setting the operating mode for a VSAN

Setting the operating mode for a VSAN

This release added support for setting the operating mode for a VSAN.

Command reference

working-mode

Use **working-mode** to set the operating mode for a VSAN.

Use **undo working-mode** to restore the default.

Syntax

working-mode { **fcf** | **npv** }

undo working-mode

Default

The operating mode of a VSAN is NPV.

Views

VSAN view

Predefined user roles

network-admin

Parameters

fcf: Specifies the FCF mode.

npv: Specifies the NPV mode

Usage guidelines

Only FCF-NPV switches support this command.

A VSAN operating in FCF mode acts as an FCF switch. A VSAN operating in NPV mode acts as an NPV switch.

If the set mode of an interface is not supported by a VSAN of the interface, the mode does not take effect in the VSAN.

Examples

Set the operating mode to FCF for VSAN 10.

```
<Sysname> system-view
```

```
[Sysname] vsan 10
[Sysname-vsan10] working-mode fcf
```

New feature: Configuring automatic load balancing for FCoE

Configuring automatic load balancing for FCoE

This feature automatically redistributes downlink interfaces across all uplink interfaces if the system detects new operational uplink interfaces.

When the system detects a new operational uplink interface, the system starts a delay timer. When the timer expires, the system automatically redistributes downlink interfaces across all uplink interfaces. If another uplink interface becomes operational before the timer expires, the system resets the timer. The delay timer helps reduce network flapping caused by up/down events of uplink interfaces. If the link layer state of uplink interfaces is stable, set the delay timer to a smaller value. Otherwise, set the delay timer to a greater value.

This feature might trigger a load balancing process when a new uplink interface become operational, which causes traffic disruption.

When this feature is disabled, downlink-to-uplink interface mappings are not affected.

To configure automatic load balancing:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter VSAN view.	**vsan** *vsan-id*	N/A
3. Enable automatic load balancing.	**npv auto-load-balance enable**	By default, automatic load balancing is disabled.
4. Set the delay timer for automatic load balancing.	**npv auto-load-balance interval** *interval*	The default setting is 30 seconds.

Command reference

npv auto-load-balance enable

Use **npv auto-load-balance enable** to enable automatic load balancing in a VSAN.

Use **undo npv auto-load-balance enable** to disable automatic load balancing in a VSAN.

Syntax

npv auto-load-balance enable

undo npv auto-load-balance enable

Default

Automatic load balancing is disabled in a VSAN.

Views

VSAN view

Predefined user roles

network-admin

Usage guidelines

Only NPV switches and VSANs operating in NPV mode support this command.

The automatic load-balancing process is as follows:

1. The system starts a delay timer when it detects a new operational uplink interface.
2. The system automatically redistributes downlink interfaces across all uplink interfaces when the timer expires.

   If another uplink interface becomes operational before the timer expires, the system resets the timer.

The automatic load balancing feature might trigger a load-balancing process when a new uplink interface becomes operational, which causes traffic disruption. When this feature is disabled, downlink-to-uplink interface mappings are not affected.

Examples

Enable automatic load balancing in VSAN 1.

```
<Sysname> system-view
[Sysname] vsan 1
[Sysname-vsan1] npv auto-load-balance enable
```

npv auto-load-balance-interval

Use **npv auto-load-balance-interval** to set the delay timer for automatic load balancing in a VSAN.

Use **undo npv auto-load-balance-interval** to restore the default.

Syntax

npv auto-load-balance-interval *interval*

undo npv auto-load-balance-interval

Default

The delay timer is 30 seconds.

Views

VSAN view

Predefined user roles

network-admin

Parameters

interval: Specifies a value for the delay timer, in the range of 1 to 300 seconds.

Usage guidelines

Only NPV switches and VSANs operating in NPV mode support this command.

The delay timer helps reduce network flapping caused by up/down events of uplink interfaces. If the link layer state of uplink interfaces is stable, set the delay timer to a smaller value. Otherwise, set the delay timer to a greater value.

Examples

Set the delay timer for automatic load balancing to 20 seconds in VSAN 1.

```
<Sysname> system-view
[Sysname] vsan 1
```

```
[Sysname-vsan1] npv auto-load-balance-interval 20
```

Modified feature: Forbidding an OpenFlow instance to report the specified types of ports to controllers

Feature change description

This release added Layer 3 Ethernet interfaces to the ports that an OpenFlow instances was forbidden to report to controllers.

Command changes

Modified command: forbidden port

Old syntax

forbidden port { **vlan-interface** | **vsi-interface** } *

New syntax

forbidden port { **l3-physical-interface** | **vlan-interface** | **vsi-interface** } *

Views

OpenFlow instance view

Change description

The **l3-physical-interface** keyword was added. Layer 3 Ethernet interfaces were added to the ports that an OpenFlow instances was forbidden to report to controllers.

Modified feature: Support for Push-Tag and Pop-Tag in Packet-out messages

Feature change description

Support for Push-Tag and Pop-Tag was added for OpenFlow Packet-out messages.

Command changes

None.

Modified feature: Creating RMON statistics entries

Feature change description

The maximum number of RMON statistics entries was changed from 100 to 200.

Command changes

Modified command: rmon statistics

Syntax

rmon statistics *entry-number* [**owner** *text*]

undo rmon statistics *entry-number*

Views

Ethernet interface view

Change description

Before modification: You can create a maximum of 100 RMON statistics entries.

After modification: You can create a maximum of 200 RMON statistics entries.

Modified feature: Creating RMON history control entries

Feature change description

The maximum number of RMON history control entries was changed from 100 to 200.

Command changes

Modified command: rmon history

Syntax

rmon history *entry-number* **buckets** *number* **interval** *interval* [**owner** *text*]

undo rmon history *entry-number*

Views

Ethernet interface view

Change description

Before modification: You can create a maximum of 100 RMON history control entries.

After modification: You can create a maximum of 200 RMON history control entries.

Modified feature: Automatic configuration

Feature change description

Before modification: The device automatically obtains a set of configuration settings from a file server when it starts up without a configuration file.

After modification: The device checks the root directory of its default storage medium for the autocfg.py, autocfg.tcl, or autocfg.cfg file before starting to obtain configuration settings from a file server. If one of the files is found, the device executes the script or configuration file to complete automatic configuration.

Command changes

None.

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.

Modified feature: Support for broadcast, multicast, or unicast storm suppression in Layer 3 Ethernet interface view

Feature change description

Broadcast, multicast, or unicast storm suppression is supported in Layer 3 Ethernet interface view. You can configure an interface as a Layer 3 Ethernet interface by using the **port link-mode route** command.

Command changes

Modified command: broadcast-suppression

Syntax

broadcast-suppression { *ratio* **|** **pps** *max-pps* **|** **kbps** *max-kbps* }

undo broadcast-suppression

Views

Layer 2 Ethernet interface view, Layer 3 Ethernet interface view

Change description

Before modification: Broadcast storm suppression is supported only in Layer 2 Ethernet interface view.

After modification: Broadcast storm suppression is supported in both Layer 2 and Layer 3 Ethernet interface views.

Modified command: multicast-suppression

Syntax

multicast-suppression { *ratio* **|** **pps** *max-pps* **|** **kbps** *max-kbps* }

undo multicast-suppression

Views

Layer 2 Ethernet interface view, Layer 3 Ethernet interface view

Change description

Before modification: Multicast storm suppression is supported only in Layer 2 Ethernet interface view.

After modification: Multicast storm suppression is supported in both Layer 2 and Layer 3 Ethernet interface views.

Modified command: unicast-suppression

Syntax

unicast-suppression { *ratio* **|** **pps** *max-pps* **|** **kbps** *max-kbps* }

undo unicast-suppression

Views

Layer 2 Ethernet interface view, Layer 3 Ethernet interface view

Change description

Before modification: Unicast storm suppression is supported only in Layer 2 Ethernet interface view.

After modification: Unicast storm suppression is supported in both Layer 2 and Layer 3 Ethernet interface views.

Modified feature: Configuring BGP route update delay on reboot

Feature change description

The value range for the route update delay time was changed.

Command changes

Modified command: bgp update-delay on-startup

Syntax

bgp update-delay on-startup *seconds*

Views

BGP instance view

Change description

Before modification: The value range for the *seconds* argument is 1 to 3600 seconds.

After modification: The value range for the *seconds* argument is 0 to 3600 seconds. The value of 0 indicates that BGP does not send route updates after the device reboots.

Modified feature: 802.1X timers

Feature change description

This release modified the value range for the username request timeout timer.

Command changes

Modified command: dot1x timer

Syntax

dot1x timer { **ead-timeout** *ead-timeout-value* **| handshake-period** *handshake-period-value* **| quiet-period** *quiet-period-value* **| reauth-period** *reauth-period-value* **| server-timeout** *server-timeout-value* **| supp-timeout** *supp-timeout-value* **| tx-period** *tx-period-value* }

undo dot1x timer { **ead-timeout | handshake-period | quiet-period | reauth-period | server-timeout | supp-timeout | tx-period** }

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: MAC authentication timers

Feature change description

The value range for the offline detect timer changed.

Command changes

Modified command: mac-authentication timer

Syntax

mac-authentication timer { **offline-detect** *offline-detect-value* **| quiet** *quiet-value* **| server-timeout** *server-timeout-value* }

Views

System view

Change description

Before modification: The value range for the *offline-detect-value* argument is 60 to 65535, in seconds.

After modification: The value range for the *offline-detect-value* argument is 60 to 2147483647, in seconds.

Modified feature: Configuring the HTTPS listening port number for the local portal Web server

Feature change description

The **tcp-port** *port-number* option was added in the local portal Web server configuration command. Using this command option, you can specify the TCP port number on which the local portal Web server listens for HTTPS.

When you configure the HTTPS listening TCP port for the local portal Web server, follow these guidelines:

- For the local portal Web server that uses HTTPS and other services that use HTTPS:
  - If they use the same SSL server policy, they can use the same TCP port number to listen to HTTPS.
  - If they use different SSL server policies, they cannot use the same TCP port number to listen to HTTPS.
- Do not configure the HTTPS listening TCP port number as the port number used by a known protocol (except HTTPS). For example, do not specify port numbers 80 and 23, which are used by HTTP and Telnet, respectively.
- Do not configure the same TCP port number for HTTP and HTTPS local Web portal servers.

Command changes

Modified command: portal local-web-server

Old syntax

portal local-web-server { **http** | **https ssl-server-policy** *policy-name* }

New syntax

portal local-web-server { **http** | **https ssl-server-policy** *policy-name* [**tcp-port** *port-number*] }

Views

System view

Parameters

tcp-port *port-number*: Specifies the TCP port number on which the local portal server listens for HTTPS. The value range for the *port-number* argument is 1 to 65535. The default port number is 443.

Change description

Before modification: The command did not support configuring the HTTPS listening port number. The HTTPS listening port number can only be 443.

After modification: The **tcp-port** *port-number* option was added to configure the HTTPS listening port number.

Modified feature: Specifying a log host

Feature change description

The maximum number of log hosts was changed from 4 to 20.

Command changes

Modified command: info-center loghost

Syntax

info-center loghost [**vpn-instance** *vpn-instance-name*] { *loghost* **|** *ipv4-address* **| ipv6** *ipv6-address* } [**port** *port-number*] [**facility** *local-number*]

Views

System view

Change description

Before modification: The device supports a maximum of 4 log hosts.

After modification: The device supports a maximum of 20 log hosts.

Modified feature: Remote file copying

Feature change description

HTTP support was added to the **copy** command. You can use the command to remotely copy files through FTP, TFTP, and HTTP.

To remotely copy a file through HTTP, specify the URL in the **http://**[*HTTP username*[**:***password*]**@**]*server address*[**:***port number*]**/***filepath*[**/***file name*] format.

- The username and password in the URL must be the same as the username and password configured on the server.
- If only the username is required for authentication, you do not need to enter the password.
- If authentication is not required, you do not need to enter the username or password.

For example, the **startup.cfg** file is saved in the authorized directory on the HTTP server at 1.1.1.1. The HTTP account username and password are both **1**. To copy the file, specify the URL **http://1:1@1.1.1.1/startup.cfg**. If authentication is not required, specify the URL **http://1.1.1.1/startup.cfg**.

Command changes

Modified command: copy

Syntax

In non-FIPS mode:

copy *source-file* { *dest-file* **|** *dest-directory* } [**vpn-instance** *vpn-instance-name*] [**source interface** *interface-type interface-number*]

In FIPS mode:

copy *source-file* { *dest-file* **|** *dest-directory* }

Views

User view

Change description

Before modification: The command does not support using HTTP to copy a remote file.

After modification: The command supports using HTTP to copy a remote file.

Modified feature: Multicast VLAN

Feature change description

Before modification: Multicast VLAN implements only forward transmission. A Layer 2 device can forward multicast traffic only from the upstream Layer 3 device to downstream devices that are in sub-VLANs or have member ports. Downstream devices can connect to multicast receivers rather than multicast sources.

After modification: Multicast VLAN implements both forward transmission and reverse transmission. Reverse transmission implementation applies to multicast networks where multicast sources are connected to downstream devices of a Layer 2 device. Upon receiving multicast traffic from a downstream multicast source, the Layer 2 device changes the user VLAN of the traffic to the associated multicast VLAN. Then, it floods the traffic to the upstream Layer 3 device through the multicast VLAN. The upstream Layer 3 device forwards the traffic to receivers based on the associated Layer 3 multicast forwarding entry.

Command changes

None.

Modified feature: Enabling link-aggregation traffic redirection

Feature change description

Link-aggregation traffic redirection can be enabled in Layer 2 and Layer 3 aggregate interface views.

Command changes

Modified command: link-aggregation lacp traffic-redirect-notification enable

Syntax

link-aggregation lacp traffic-redirect-notification enable

Views

System view, Layer 2 aggregate interface view, Layer 3 aggregate interface view

Change description

Before modification: Link-aggregation traffic redirection is supported only in system view.

After modification: Link-aggregation traffic redirection can be enabled in Layer 2 and Layer 3 aggregate interface views.

Global link-aggregation traffic redirection settings take effect on all aggregation groups. A link aggregation group preferentially uses the group-specific link-aggregation traffic redirection settings. If group-specific link-aggregation traffic redirection is not configured, the group uses the global link-aggregation traffic redirection settings.

As a best practice, you enable link-aggregation traffic redirection on aggregate interfaces. If you enable this feature globally, communication with a third-party peer device might be affected if the peer is not compatible with this feature.

Modified feature: TCP maximum segment size (MSS) setting

Feature change description

The value range for the *value* argument changed.

Command changes

Modified command: tcp mss

Syntax

tcp mss *value*

Views

Interface view

Change description

Before modification: The value range for the *value* argument is 128 to 2048, in bytes.

After modification: The minimum value for the *value* argument is 128. The maximum value equals the maximum MTU that the interface supports minus 40.

Modified feature: Configuring a preemption mode for a smart link group

Feature change description

This release added support for the speed preemption mode for a smart link group.

Command changes

Modified command: preemption mode

Old syntax

preemption mode role

undo preemption mode

New syntax

preemption mode { **role** | **speed** [**threshold** *threshold-value*] }

undo preemption mode

Views

Smart link group view

Change description

speed: Specifies the speed preemption mode.

threshold *threshold-value*: Specifies the speed preemption threshold in percentage. The value range for the *threshold-value* argument is 1 to 10000.

If you specify the speed preemption mode, the following conditions occur when the primary link recovers:

- If you specify the **threshold** *threshold-value* option, the primary port transitions to forwarding state when the primary port speed minus the secondary port speed equals or exceeds the threshold value (in percentage).
- If you do not specify the **threshold** *threshold-value* option, the primary port transitions to forwarding state when the primary port speed exceeds the secondary port speed.

Modified feature: Creating a VSAN and entering VSAN view

Feature change description

This release added support for configuring a VSAN name.

Command changes

Modified command: vsan

Old syntax

vsan *vsan-id*

undo vsan *vsan-id*

New syntax

vsan *vsan-id* [**name** *vsan-name*]

undo vsan *vsan-id* [**name**]

Views

System view

Change description

name *vsan-name*: Specifies the name of the VSAN, a case-sensitive string of 1 to 32 characters. The name must start with a letter and can contain letters, numbers, and special symbols in Table 34.

Table 34 Special symbols

Name	Symbol
Caret	^
Dollar sign	$
Minus sign	-
Underscore	_

If you do not specify a VSAN name, the default VSAN name is VSAN plus a four-digit VSAN ID. For example, the default VSAN name of VSAN 10 is VSAN0010.

If you specify the **name** keyword, the **undo vsan** command restores the VSAN name to its default. If you do not specify the **name** keyword, the **undo vsan** command deletes the VSAN.

Modified feature: Configuring an FCoE mode for the switch

Feature change description

This release added support for the FCF-NPV mode.

Command changes

Modified command: fcoe-mode

Old syntax

fcoe-mode { **fcf** | **npv** | **transit** }

undo fcoe-mode

New syntax

fcoe-mode { **fcf** | **fcf-npv** | **npv** | **transit** }

undo fcoe-mode

Views

System view

Change description

fcf-npv: Specifies the FCF-NPV mode.

FCF-NPV mode—When the switch operates in this mode, it is an FCF-NPV switch. A VSAN on an FCF-NPV switch can operate in either of the following modes:

- **FCF mode**—When a VSAN operates in this mode, the VSAN acts as an FCF switch.

- **NPV mode**—When a VSAN operates in this mode, the VSAN acts as an NPV switch.

Modified feature: Setting the mode of a VFC interface

Feature change description

This release added support for the **fc mode** command for the FCF-NPV mode.

Command changes

Modified command: fc mode (VFC interface view)

Syntax

fc mode { **e** | **f** | **np** }

undo fc mode

Views

VFC interface view

Change description

An FCF-NPV switch supports E, F, and NP modes.

On an FCF-NPV switch, if the mode of a VFC interface is not supported by a VSAN of the interface, the mode does not take effect in the VSAN.

Modified feature: Setting an FC-MAP value

Feature change description

This release added VLAN view to the **fcoe fcmap** command.

Command changes

Modified command: fcoe fcmap

Syntax

fcoe fcmap *fc-map*

undo fcoe fcmap

Views

System view

VLAN view

Change description

Before modification: On FCF or NPV switches, you can set an FC-MAP value only in system view.

After modification: On FCF or NPV switches, you can set an FC-MAP value only in system view. On FCF-NPV switches, you can set an FC-MAP value only in VLAN view.

Modified feature: Setting an FKA advertisement interval

Feature change description

This release added VLAN view to the **fcoe fka-adv-period** command.

Command changes

Modified command: fcoe fka-adv-period

Syntax

fcoe fka-adv-period *fka-adv-period*

undo fcoe fka-adv-period

Views

System view

VLAN view

Change description

Before modification: On FCF or NPV switches, you can set an FC-MAP value only in system view.

After modification: On FCF or NPV switches, you can set an FC-MAP value only in system view. On FCF-NPV switches, you can set an FC-MAP value only in VLAN view.

Modified feature: Setting the system FCF priority

Feature change description

This release added VLAN view to the **fcoe global fcf-priority** command.

Command changes

Modified command: fcoe fcmap

Syntax

fcoe global fcf-priority *priority*

undo fcoe global fcf-priority

Views

System view

VLAN view

Change description

Before modification: On FCF or NPV switches, you can set an FC-MAP value only in system view.

After modification: On FCF or NPV switches, you can set an FC-MAP value only in system view. On FCF-NPV switches, you can set an FC-MAP value only in VLAN view.

Modified feature: Creating an OpenFlow table for an OpenFlow instance

Feature change description

The **ingress-vlan** *ingress-table-id* and **egress-vlan** *egress-table-id* options were added to the **flow-table** command. You can create VLAN tagging and untagging flow tables to process incoming and outgoing packets, respectively.

Command changes

Modified command: flow-table

Old syntax

flow-table { **extensibility** *extensibility-table-id* **|** **mac-ip** *mac-ip-table-id* }*

New syntax

flow-table { [**ingress-vlan** *ingress-table-id*] [**extensibility** *extensibility-table-id* **|** **mac-ip** *mac-ip-table-id*] * [**egress-vlan** *egress-table-id*] }

Views

OpenFlow instance view

Change description

The **ingress-vlan** *ingress-table-id* and **egress-vlan** *egress-table-id* options were added.

ingress-vlan *ingress-table-id*: Specifies a VLAN tagging flow table by its ID in the range of 0 to 254. If you specify this option, the device tags all incoming packets matching the table.

egress-vlan *egress-table-id*: Specifies a VLAN untagging flow table by its ID in the range of 0 to 254. If you specify this option, the device untags all outgoing packets matching the table.

Modified feature: Frame match criteria of Ethernet service instances

Feature change description

In this release, an Ethernet service instance can match both the inner and outer VLAN tags of frames. In the earlier releases, an Ethernet service instance can match only the outer VLAN tag of frames.

The device processes frames with matching inner and outer VLAN tags as follows:

- **VLAN access mode**—For an Ethernet frame received from the local site, the device removes all its VLAN tags before forwarding the frame. For an Ethernet frame destined for the local site, the device adds VLAN tags to the frame before forwarding the frame.
- **Ethernet access mode**—For an Ethernet frame received from the local site, the device forwards the frame with the VLAN tags intact. For an Ethernet frame destined for the local site, the device forwards the frame without adding VLAN tags.

Command changes

Modified command: encapsulation

Old syntax

encapsulation default

encapsulation { **tagged | untagged** }

encapsulation s-vid *vlan-id* [**only-tagged**]

undo encapsulation

New syntax

encapsulation default

encapsulation { **tagged | untagged** }

encapsulation s-vid *vlan-id* [**only-tagged**]

encapsulation s-vid *vlan-id* **c-vid** *vlan-id*

undo encapsulation

Views

Ethernet service instance view

Change description

The **encapsulation s-vid** *vlan-id* **c-vid** *vlan-id* command was added to match both the inner and outer VLAN tags of frames.

On an interface for Ethernet service instances configured with the **encapsulation s-vid** and **encapsulation s-vid c-vid** criteria that match the same outer VLAN ID, frames that match both frame match criteria are assigned to the Ethernet service instance configured with the **encapsulation s-vid c-vid** command.

About software feature changes

This document introduces the modification of software features on

- HPE 6125XLG-CMW710-R2422 from HPE 6125XLG-CMW710-R2418P01.
- Releases that follow HPE 6125XLG-CMW710-R2422.

For information about the software feature changes between releases before *HPE 6125XLG-CMW710-R2418P01*, see *Software Feature Changes* for the target release.