



Hewlett Packard
Enterprise

A5500HI-CMW520-R5501P36

Release Notes

The information in this document is subject to change without notice.
© Copyright 2015,2018 Hewlett Packard Enterprise Development LP

Contents

Introduction	1
Version information	1
Version number	1
Version history	1
Hardware and software compatibility matrix	9
ISSU Version Compatibility Matrix	11
Upgrade restrictions and guidelines	12
Hardware feature updates	12
Hardware feature updates in R5501P36	12
Hardware feature updates in R5501P35	12
Hardware feature updates in R5501P33	12
Hardware feature updates in R5501P32	12
Hardware feature updates in R5501P31	12
Hardware feature updates in R5501P30	12
Hardware feature updates in R5501P28	13
Hardware feature updates in R5501P27	13
Hardware feature updates in R5501P26	13
Hardware feature updates in R5501P25	13
Hardware feature updates in R5501P23	13
Hardware feature updates in R5501P22	13
Hardware feature updates in R5501P21	13
Hardware feature updates in R5501P20	13
Hardware feature updates in R5501P19	13
Hardware feature updates in R5501P17	14
Hardware feature updates in R5501P15	14
Hardware feature updates in R5501P13	14
Hardware feature updates in R5501P12	14
Hardware feature updates in R5501P11	14
Hardware feature updates in R5501P10	14
Hardware feature updates in R5501P06	14
Hardware feature updates in R5501P05	14
Hardware feature updates in R5501P03	15
Hardware feature updates in R5501P02	15
Hardware feature updates in R5501P01	15
Hardware feature updates in R5501	15
Hardware feature updates in R5206	15
Hardware feature updates in R5205L01	15

Hardware feature updates in R5203P01	15
Hardware feature updates in R5203	15
Hardware feature updates in E5201	16
Hardware feature updates in R5105	16
Hardware feature updates in F5103	16
Hardware feature updates in F5102	16
Hardware feature updates in R5101P01	16
Hardware feature updates in R5101	16
Hardware feature updates in E5101	16
Software feature and command updates	17
MIB updates	17
Operation changes	21
Operation changes in R5501P36	21
Operation changes in R5501P35	21
Operation changes in R5501P33	21
Operation changes in R5501P32	21
Operation changes in R5501P31	21
Operation changes in R5501P30	22
Operation changes in R5501P28	22
Operation changes in R5501P27	22
Operation changes in R5501P26	22
Operation changes in R5501P25	22
Operation changes in R5501P23	22
Operation changes in R5501P22	22
Operation changes in R5501P21	22
Operation changes in R5501P20	22
Operation changes in R5501P19	23
Operation changes in R5501P17	23
Operation changes in R5501P15	23
Operation changes in R5501P13	23
Operation changes in R5501P12	23
Operation changes in R5501P11	23
Operation changes in R5501P10	23
Operation changes in R5501P06	24
Operation changes in R5501P05	24
Operation changes in R5501P03	24
Operation changes in R5501P02	24
Operation changes in R5501P01	24
Operation changes in R5501	24

Operation changes in R5206	24
Operation changes in R5205L01	25
Operation changes in R5203P01	25
Operation changes in R5203	25
Operation changes in E5201	25
Operation changes in R5105	25
Operation changes in F5103	25
Operation changes in F5102	26
Operation changes in R5101P01	26
Operation changes in R5101	26
Operation changes in E5101	26
Restrictions and cautions	27
Open problems and workarounds	28
List of resolved problems	28
Resolved problems in R5501P36	28
Resolved problems in R5501P35	29
Resolved problems in R5501P33	30
Resolved problems in R5501P32	30
Resolved problems in R5501P31	31
Resolved problems in R5501P30	32
Resolved problems in R5501P28	33
Resolved problems in R5501P27	34
Resolved problems in R5501P26	34
Resolved problems in R5501P25	34
Resolved problems in R5501P23	34
Resolved problems in R5501P22	35
Resolved problems in R5501P21	36
Resolved problems in R5501P20	36
Resolved problems in R5501P19	37
Resolved problems in R5501P17	38
Resolved problems in R5501P15	38
Resolved problems in R5501P13	39
Resolved problems in R5501P12	39
Resolved problems in R5501P11	40
Resolved problems in R5501P10	41
Resolved problems in R5501P06	43
Resolved problems in R5501P05	46
Resolved problems in R5501P03	47
Resolved problems in R5501P02	48

Resolved problems in R5501P01	52
Resolved problems in R5501	53
Resolved problems in R5206	54
Resolved problems in R5205L01	56
Resolved problems in R5203P01	57
Resolved problems in R5203	57
Resolved problems in E5201	58
Resolved problems in R5105	59
Resolved problems in F5103	60
Resolved problems in F5102	60
Resolved problems in R5101P01	61
Resolved problems in R5101	61
Resolved problems in E5101	61
Support and other resources	61
Accessing Hewlett Packard Enterprise Support	61
Documents	62
Related documents	62
Documentation feedback	62
Appendix A Feature list	63
Hardware features	63
Hardware features	63
Software features	66
Appendix B Upgrading software	72
Upgrading software from Boot ROM menus	72
Accessing the basic Boot menu	74
Accessing the extended Boot menu	75
XMODEM download through the console port	77
TFTP download through an Ethernet port	85
FTP download through an Ethernet port	87
Upgrading at the CLI	89
FTP download from a server	89
TFTP download from a server	90

List of tables

Table 1 Version history	1
Table 2 Hardware and software compatibility matrix	10
Table 3 ISSU Compatibility matrix	11
Table 4 MIB updates	17
Table 5 HP 5500 HI Switch Series models	63
Table 6 HP 5500 HI Switch Series technical specifications	63
Table 7 Software features of the 5500 HI series	66
Table 8 Software upgrade methods	72
Table 9 Shortcut keys	73
Table 10 Basic Boot menu options	74
Table 11 BASIC-ASSISTANT menu options	75
Table 12 Extended Boot menu options	76
Table 13 EXTEND-ASSISTANT menu options	77
Table 14 Description of the TFTP parameters	86
Table 15 Description of the FTP parameters	88

Introduction

This document describes the features, restrictions and guidelines, open problems, and workarounds for version A5500HI-CMW520-R5501P36. Before you use this version on a live network, back up the configuration and test the version to avoid software upgrade affecting your live network.

Use this document in conjunction with *A5500HI-CMW520-R5501P36 Release Notes (Software Feature Changes)* and the documents listed in "[Related documents](#)."

Version information

Version number

Comware Software, Version 5.20.99, Release 5501P36

Note: You can see the version number with the command **display version** in any view. See **Note ①**.

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
A5500HI-CMW520-R5501P36	A5500HI-CMW520-R5501P35	2018-05-17	Release version	Fixed bugs.
A5500HI-CMW520-R5501P35	A5500HI-CMW520-R5501P33	2017-11-20	Release version	Fixed bugs.
A5500HI-CMW520-R5501P33	A5500HI-CMW520-R5501P32	2017-05-16	Release version	This version introduced feature changes. New features include: <ul style="list-style-type: none">Configuring a collaboration groupConfiguring the action a port takes after it receives an Ethernet OAM event from the remote end
A5500HI-CMW520-R5501P32	A5500HI-CMW520-R5501P31	2017-03-21	Release version	Fixed bugs.
A5500HI-CMW520-R5501P31	A5500HI-CMW520-R5501P30	2017-01-16	Release version	Fixed bugs.
A5500HI-CMW520-R5501P30	A5500HI-CMW520-R5501P28	2016-12-28	Release version	Fixed bugs.
A5500HI-CMW520-R5501P28	A5500HI-CMW520-R5501P27	2016-8-25	Release version	Fixed bugs.

A5500HI-CMW52 0-R5501P27	A5500HI-CMW52 0-R5501P26	2016-6-24	Release version	Fixed bugs. Added new features: <ul style="list-style-type: none"> RA guard
A5500HI-CMW52 0-R5501P26	A5500HI-CMW52 0-R5501P23	2016-4-22	Release version	Fixed bugs.
A5500HI-CMW52 0-R5501P25	A5500HI-CMW52 0-R5501P23	2016-4-7	Release version	Fixed bugs.
A5500HI-CMW52 0-R5501P23	A5500HI-CMW52 0-R5501P22	2016-3-22	Release version	Fixed bugs. Added new features: <ul style="list-style-type: none"> Default settings configuration for prefixes advertised in RA messages
A5500HI-CMW52 0-R5501P22	A5500HI-CMW52 0-R5501P21	2016-2-24	Release version	Fixed bugs.
A5500HI-CMW52 0-R5501P21	A5500HI-CMW52 0-R5501P20	2016-1-27	Release version	Fixed bugs.
A5500HI-CMW52 0-R5501P20	A5500HI-CMW52 0-R5501P19	2015-11-16	Release version	Fixed bugs.
A5500HI-CMW52 0-R5501P19	A5500HI-CMW52 0-R5501P17	2015-11-03	Release version	Fixed bugs. Added new features: <ul style="list-style-type: none"> Setting the router preference in RA messages Support for NTP configuration in IPv6 networks Enabling sending of ICMPv6 redirect messages Modified features: <ul style="list-style-type: none"> Disabling advertising prefix information in RA messages
A5500HI-CMW52 0-R5501P17	A5500HI-CMW52 0-R5501P15	2015-09-30	Release version	Fixed bugs. Added new features: <ul style="list-style-type: none"> Disabling reactivation for edge ports shut down by BPDU guard Data buffer monitoring Automatic PI reset Configuring the default action of the table-miss flow entry Modified features: <ul style="list-style-type: none"> Configuring the OpenFlow instance mode Creating an OpenFlow table for an OpenFlow instance
A5500HI-CMW52 0-R5501P15	A5500HI-CMW52 0-R5501P13	2015-09-07	Release version	Fixed bugs. Modified features:

				<ul style="list-style-type: none"> Storm control for known unicast packets Setting the maximum number of logs that can be stored in the log buffer VPN instance support for NQA server configuration
A5500HI-CMW52 0-R5501P13	A5500HI-CMW52 0-R5501P12	2015-08-12	Release version	Fixed bugs. Added new features: <ul style="list-style-type: none"> Sending EAP-Success packets to 802.1X users in critical VLAN
A5500HI-CMW52 0-R5501P12	A5500HI-CMW52 0-R5501P11	2015-07-08	Release version	Fixed bugs.
A5500HI-CMW52 0-R5501P11	A5500HI-CMW52 0-R5501P10	2015-05-31	Release version	Fixed bugs. Added new features: <ul style="list-style-type: none"> Login delay Modified feature: IPv6 address with a 127-bit prefix length
A5500HI-CMW52 0-R5501P10	A5500HI-CMW52 0-R5501P06	2015-04-30	Release version	Fixed bugs. Added new features: <ul style="list-style-type: none"> SNMP notifications for PVST topology changes
A5500HI-CMW52 0-R5501P06	A5500HI-CMW52 0-R5501P05	2015-01-31	Release version	Fixed bugs. Added new features: <ul style="list-style-type: none"> Disabling SSL 3.0 802.1X MAC address binding Web connection idle timeout Applicable scope of packet filtering on a VLAN interface
A5500HI-CMW52 0-R5501P05	A5500HI-CMW52 0-R5501P03	2014-10-31	Release version	Fixed bugs. Modified features: <ul style="list-style-type: none"> Executing interactive commands in interface range view Specifying RADIUS security policy servers by IP address
A5500HI-CMW52 0-R5501P03	A5500HI-CMW52 0-R5501P02	2014-08-29	Release version	Fixed bugs. Added new features: <ul style="list-style-type: none"> Per-flow load sharing Telnet/SSH user connection control Packet rate-limiting for the table-miss flow entry Modified features: Including time zone information in the timestamp of system

				<p>information sent to a log host</p> <ul style="list-style-type: none"> Configuring physical state change suppression on an Ethernet interface Configuring a tag and description for an IPv6 static route
A5500HI-CMW52 0-R5501P02	A5500HI-CMW52 0-R5501P01	2014-07-15	Release version	<p>Fixed bugs.</p> <p>Added new features:</p> <ul style="list-style-type: none"> 802.1X voice VLAN Configuring the uplink port to permit multiple isolate-user-VLANs TCP fragment attack protection Support for BPDU guard configuration in interface or port group view MAC re-authentication timer for users in guest VLAN Specifying the IPv4/IPv6 VRRP version MAC and port uniqueness check by the DHCP snooping device <p>Modified features:</p> <ul style="list-style-type: none"> Auto status transition of dynamic secure MAC addresses The maximum number of gateways supported in MFF automatic mode Username request timeout timer for 802.1X authentication
A5500HI-CMW52 0-R5501P01	A5500HI-CMW52 0-R5501	2014-02-28	Release version	<p>Fixed bugs.</p> <p>Added new features:</p> <ul style="list-style-type: none"> Discarding IPv6 packets that contain extension headers <p>Modified features:</p> <ul style="list-style-type: none"> Configuring IGMP SSM mappings Configuring MLD SSM mappings
A5500HI-CMW52 0-R5501	A5500HI-CMW52 0-R5206	2013-12-31	Release version	<p>Fixed bugs.</p> <p>Added new features:</p> <ul style="list-style-type: none"> OpenFlow <p>Modified features:</p> <ul style="list-style-type: none"> Setting the device name Specifying multiple public keys for an SSH user Disabling an untrusted port from recording

				<p>clients' IP-to-MAC bindings</p> <ul style="list-style-type: none"> • ARP packet rate limit • Specifying the username and password to log in to the SCP server • Customizing DHCP options • ACL-based packet filtering on a VLAN interface
A5500HI-CMW52 0-R5206	A5500HI-CMW52 0-R5205L01	2013-12-16	Release version	<p>Added new features:</p> <ul style="list-style-type: none"> • Configuring the ARP detection logging function • 802.1X-based dynamic IPv4 source guard binding entries • SSL server policy association with the FTP service • Enabling MAC authentication multi-VLAN mode <p>Modified features:</p> <ul style="list-style-type: none"> • Specifying multiple secondary HWTACACS servers • Displaying brief interface information • Displaying brief IP configuration for Layer 3 interfaces • Configuring static multicast MAC address entries
A5500HI-CMW52 0-R5205L01	A5500HI-CMW52 0-R5203P01	2013-04-28	Release version	<p>Added new features:</p> <ul style="list-style-type: none"> • Multicast ND • Configuring packet capture <p>Modified features:</p> <ul style="list-style-type: none"> • Configuring system information for the SNMP agent
A5500HI-CMW52 0-R5203P01	A5500HI-CMW52 0-R5203	2013-04-09	Release version	<p>Added new hardware:</p> <ul style="list-style-type: none"> • HP 5500-24G-PoE+-4SFP HI TAA-compliant Switch with 2 Interface Slots JG679A • HP 5500-48G-PoE+-4SFP HI TAA-compliant Switch with 2 Interface Slots JG680A • HP 5500-24G-SFP HI TAA-compliant Switch with 2 Interface Slots JG681A

A5500HI-CMW52 0-R5203	A5500HI-CMW52 0-E5201	2013-03-29	Release version	<p>Added new hardware:</p> <ul style="list-style-type: none"> HP 5500/5120 2-port 10GBASE-T Module JG535A <p>Modified features:</p> <ul style="list-style-type: none"> Enabling/disabling FIPS mode Setting the maximum number of the IPv4/IPv6 source guard binding entries on a port Setting the IRF link down report delay Setting the minimum password length Switching the user privilege level Upgrading a subordinate member Implementing ACL-based IPsec Cluster management Deleted feature: Disabling Boot ROM access
A5500HI-CMW52 0-E5201	A5500HI-CMW52 0-R5105	2013-01-15	Release version	<p>Added new hardware:</p> <ul style="list-style-type: none"> HP 5500-24G-PoE+-4SFP HI Switch with 2 Interface Slots JG541A HP 5500-48G-PoE+-4SFP HI Switch with 2 Interface Slots JG542A HP 5500-24G-SFP HI Switch with 2 Interface Slots JG543A X362 720W AC PoE Power Supply JG544A X362 1110W AC PoE Power Supply JG545A <p>Added new features:</p> <ul style="list-style-type: none"> Configuring a user validity check rule Enabling source IP conflict prompt Supporting IPv6 routes with a prefix length over 64 BGP MDT Configuring the maximum number of selected ports allowed for an aggregation group Enabling MAC address migration log notifying Disabling MAC entry aging timer refresh based

				<p>on destination MAC address</p> <ul style="list-style-type: none"> • PoE power negotiation through Power Via MDI TLV (supported only on PoE-capable switches) • Specifying a destination server in a VPN for UDP helper • Supporting using a self-signed certificate for HTTPS • Setting the maximum number of 802.1X authentication attempts for MAC authentication users • Support of 802.1X for issuing VLAN groups • Setting the deletion delay time for SAVI • Setting a DSCP value for an ISP domain • Advanced packet filtering logging • PoE • Supporting automatically creating RSA key pairs or SSH • Modified features: <p>SCP server name</p> <p>Configuring portal-free rules to support TCP/UDP port numbers</p> <p>Setting the time to wait for a DAD NS from a DHCPv6 client</p> <p>Support of voice VLAN for 128 OUI addresses</p> <p>Configuring CDP compatibility</p> <p>Ping ipv6</p> <p>Configuring the maximum number of operations that an NQA client can simultaneously perform</p> <p>Configuring parameters for an sFlow collector</p> <p>Configuring load-sharing criteria for a link aggregation group</p> <p>Implementing ACL-based IPsec</p> <p>Setting the IRF link down report delay</p> <p>Configuring the ABR to advertise a default route to the stub area</p>
A5500HI-CMW52	A5500HI-CMW52	2013-01-14	Release	Added new features:

0-R5105	0-F5103		version	<ul style="list-style-type: none"> Disabling password recovery capacity Configuring a port to forward 802.1X EAPOL packets untagged Configuring preferred tunnels in a tunneling policy <p>Modified features:</p> <ul style="list-style-type: none"> Configuring NDP globally and for specific ports Configuring NTDP globally and for specific ports Configuring the cluster function Default configuration
A5500HI-CMW52 0-F5103	A5500HI-CMW52 0-F5102	2012-08-31	Feature version	<p>Added new features:</p> <ul style="list-style-type: none"> Delaying the MAC authentication Specifying the source interface for DNS packets Configuring DHCPv6 snooping to support Option 18 and Option 37 Setting the subnet mask length to be 31 Setting the DSCP value for multiple types of protocol packets Automatic configuration file backup for software downgrading Configuring LLDP to advertise a specific voice VLAN Enabling LLDP to automatically discover IP phones MVRP Portal authentication in IPv6 networks SCP FIPS Configuring ACL-based IPsec <p>IKE</p> <ul style="list-style-type: none"> Configuring the log file overwrite-protection function Verifying the correctness and integrity of the file Displaying per-port queue-based traffic statistics <p>Modified features:</p> <ul style="list-style-type: none"> Configuring MAC

				<p>authentication timers</p> <ul style="list-style-type: none"> • NTP • Configuring a password for the local user • 802.1X critical VLAN • MAC authentication critical VLAN • Modifying CLI configuration commands executed in FIPS mode for CC evaluation • Modifying login management commands executed in FIPS mode for CC evaluation • Modifying software upgrade commands executed in FIPS mode for CC evaluation <p>Modifying configuration file management commands executed in FIPS mode for CC evaluation</p> <p>Modifying security commands executed in FIPS mode for CC evaluation</p> <p>Modifying SNMP commands executed in FIPS mode for CC evaluation</p> <p>Clearing all users from the password control blacklist</p> <p>Setting the interval for saving system information to the log file</p>
A5500HI-CMW52 0-F5102	A5500HI-CMW52 0-R5101P01	2012-03-31	Feature version	<ul style="list-style-type: none"> • Modified password/key related configuration. For more information, see Feature and Command Change History for HP A5500HI-CMW520-F5102
A5500HI-CMW52 0-R5101P01	A5500HI-CMW52 0-R5101	2011-12-21	Release version	Fixed bugs.
A5500HI-CMW52 0-R5101	A5500HI-CMW52 0-E5101	2011-10-26	Release version	Fixed bugs.
A5500HI-CMW52 0-E5101	First release	2011-08-22	Release version	N/A

Hardware and software compatibility matrix

CAUTION:

To avoid an upgrade failure, use [Table 2](#) to verify the hardware and software compatibility before performing an upgrade.

Table 2 Hardware and software compatibility matrix

Product family	HP 5500 HI Switch Series
Hardware platform	HP A5500-24G-4SFP HI Switch with 2 interface Slots JG311A HP A5500-48G-4SFP HI Switch with 2 interface Slots JG312A HP 5500-24G-PoE+-4SFP HI Switch with 2 Interface Slots JG541A HP 5500-48G-PoE+-4SFP HI Switch with 2 Interface Slots JG542A HP 5500-24G-SFP HI Switch with 2 Interface Slots JG543A HP 5500-24G-PoE+-4SFP HI TAA-compliant Switch with 2 Interface Slots JG679A HP 5500-48G-PoE+-4SFP HI TAA-compliant Switch with 2 Interface Slots JG680A HP 5500-24G-SFP HI TAA-compliant Switch with 2 Interface Slots JG681A
Minimum memory requirements	1024MB
Minimum Flash requirements	512 MB
Boot ROM version	Version 215 or higher (Note: Perform the command display version command in any view to view the version information. See Note②)
Host software	A5500HI-CMW520-R5501P36.bin
iMC version	iMC BIMS 7.3 (E0501) iMC EAD 7.3 (E0502) iMC TAM 7.3 (E0503) iMC UAM 7.3 (E0503) iMC NTA 7.3 (E0502) iMC PLAT 7.3 (E0605) iMC QoS 7.3 (E0502) iMC RAM 7.3 (E0501) iMC SHM 7.3 (E0502) iMC UBA 7.3 (E0502)
iNode version	iNode PC 7.3 (E0504)

Sample: To display the host software and Boot ROM version of the 5500 HI switch, perform the following:

```
<HP>display version
```

```
HPE Comware Platform Software
```

```
Comware Software, Version 5.20.99, Release 5501P36 ----- Note①
```

```
Copyright (c) 2010-2017 Hewlett Packard Enterprise Development LP
```

```
HP A5500-48G-4SFP HI Switch with 2 interface Slots uptime is 0 week, 4 days, 19
hours, 49 minutes
```

```
HP A5500-48G-4SFP HI Switch with 2 interface Slots with 2 Processors
```

```
1024M bytes SDRAM
```

```
4096K bytes Nor Flash Memory
```

```
512M bytes Nand Flash Memory
```

```
Hardware Version is REV.B
```

```
CPLD Version is 003
```


Bootrom Version is 215

----- Note②

[SubSlot 0] 48GE+4SFP+2SFP PLUS Hardware Version is REV.B

[SubSlot 2] 2 CX4 Hardware Version is REV.A

ISSU Version Compatibility Matrix

Table 3 ISSU Compatibility matrix

Current version	History version	ISSU compatibility
A5500HI-CMW520-R5501P36	A5500HI-CMW520-R5501P35	Incompatible
	A5500HI-CMW520-R5501P33	Incompatible
	A5500HI-CMW520-R5501P32	Incompatible
	A5500HI-CMW520-R5501P31	Incompatible
	A5500HI-CMW520-R5501P30	Incompatible
	A5500HI-CMW520-R5501P28	Incompatible
	A5500HI-CMW520-R5501P27	Incompatible
	A5500HI-CMW520-R5501P26	Incompatible
	A5500HI-CMW520-R5501P25	Incompatible
	A5500HI-CMW520-R5501P23	Incompatible
	A5500HI-CMW520-R5501P22	Incompatible
	A5500HI-CMW520-R5501P21	Incompatible
	A5500HI-CMW520-R5501P20	Incompatible
	A5500HI-CMW520-R5501P19	Incompatible
	A5500HI-CMW520-R5501P17	Incompatible
	A5500HI-CMW520-R5501P15	Incompatible
	A5500HI-CMW520-R5501P13	Incompatible
	A5500HI-CMW520-R5501P12	Incompatible
	A5500HI-CMW520-R5501P11	Incompatible
	A5500HI-CMW520-R5501P10	Incompatible
	A5500HI-CMW520-R5501P06	Incompatible
	A5500HI-CMW520-R5501P05	Incompatible
	A5500HI-CMW520-R5501P03	Incompatible
	A5500HI-CMW520-R5501P02	Incompatible
	A5500HI-CMW520-R5501P01	Incompatible
	A5500HI-CMW520-R5501	Incompatible
	A5500HI-CMW520-R5206	Incompatible
	A5500HI-CMW520-R5205L01	Incompatible
	A5500HI-CMW520-R5203P01	Incompatible
	A5500HI-CMW520-R5203	Incompatible

Current version	History version	ISSU compatibility
	A5500HI-CMW520-E5201	Incompatible
	A5500HI-CMW520-R5105	Incompatible
	A5500HI-CMW520-F5103	Incompatible
	A5500HI-CMW520-F5102	Incompatible
	A5500HI-CMW520-R5101P01	Incompatible
	A5500HI-CMW520-R5101	Incompatible
	A5500HI-CMW520-E5101	Incompatible

Upgrade restrictions and guidelines

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

Hardware feature updates

Hardware feature updates in R5501P36

None

Hardware feature updates in R5501P35

None

Hardware feature updates in R5501P33

None

Hardware feature updates in R5501P32

None

Hardware feature updates in R5501P31

New features: None

Hardware feature updates in R5501P30

New features: None

Hardware feature updates in R5501P28

New features: None

Deleted features: None

Hardware feature updates in R5501P27

New features: None

Deleted features: None

Hardware feature updates in R5501P26

New features: None

Deleted features: None

Hardware feature updates in R5501P25

New features: None

Deleted features: None

Hardware feature updates in R5501P23

New features: None

Deleted features: None

Hardware feature updates in R5501P22

New features: None

Deleted features: None

Hardware feature updates in R5501P21

New features: None

Deleted features: None

Hardware feature updates in R5501P20

New features: None

Deleted features: None

Hardware feature updates in R5501P19

New features: None

Deleted features: None

Hardware feature updates in R5501P17

New features: None

Deleted features: None

Hardware feature updates in R5501P15

New features: None

Deleted features: None

Hardware feature updates in R5501P13

New features: None

Deleted features: None

Hardware feature updates in R5501P12

New features: None

Deleted features: None

Hardware feature updates in R5501P11

New features: None

Deleted features: None

Hardware feature updates in R5501P10

New features: None

Deleted features: None

Hardware feature updates in R5501P06

New features: None

Deleted features: None

Hardware feature updates in R5501P05

New features: None

Deleted features: None

Hardware feature updates in R5501P03

New features: None

Deleted features: None

Hardware feature updates in R5501P02

New features: None

Deleted features: None

Hardware feature updates in R5501P01

New features: None

Deleted features: None

Hardware feature updates in R5501

New features: None

Deleted features: None

Hardware feature updates in R5206

New features: None

Deleted features: None

Hardware feature updates in R5205L01

New features: None

Deleted features: None

Hardware feature updates in R5203P01

1. R5203P01 supports the following new hardware:

HP 5500-24G-PoE+-4SFP HI TAA-compliant Switch with 2 Interface Slots JG679A

HP 5500-48G-PoE+-4SFP HI TAA-compliant Switch with 2 Interface Slots JG680A

HP 5500-24G-SFP HI TAA-compliant Switch with 2 Interface Slots JG681A

Hardware feature updates in R5203

1. R5203 supports the following new hardware:

HP 5500/5120 2-port 10GBASE-T Module JG535A

Hardware feature updates in E5201

1. E5201 supports the following new hardware:

HP 5500-24G-PoE+-4SFP HI Switch with 2 Interface Slots JG541A

HP 5500-48G-PoE+-4SFP HI Switch with 2 Interface Slots JG542A

HP 5500-24G-SFP HI Switch with 2 Interface Slots JG543A

X362 720W AC PoE Power Supply JG544A

X362 1110W AC PoE Power Supply JG545A

Hardware feature updates in R5105

New features: None

Deleted features: None

Hardware feature updates in F5103

1. F5103 supports the following new hardware:

HP X240 10G SFP+ SFP+ 0.65m DA Cable JD095C

HP X240 10G SFP+ SFP+ 1.2m DA Cable JD096C

HP X240 10G SFP+ SFP+ 3m DA Cable JD097C

HP X240 SFP+ SFP+ 5m Direct Attach Copper Cable JG081C

HP X240 10G SFP+ SFP+ 7m Direct Attach Copper Cable JC784C

Hardware feature updates in F5102

New features: None

Deleted features: None

Hardware feature updates in R5101P01

New features: None

Deleted features: None

Hardware feature updates in R5101

New features: None

Deleted features: None

Hardware feature updates in E5101

New features: First release

Deleted features: First release

Software feature and command updates

For more information about the software feature and command update history, see *HPE 5500HI-CMW520-R5501P36Release Notes (Software Feature Changes)*.

MIB updates

Table 4 MIB updates

Item	MIB file	Module	Description
A5500HI-CMW520-R5501P36			
New	None	None	None
Modified	None	None	None
A5500HI-CMW520-R5501P35			
New	None	None	None
Modified	None	None	None
A5500HI-CMW520-R5501P33			
New	None	None	None
Modified	None	None	None
A5500HI-CMW520-R5501P32			
New	None	None	None
Modified	None	None	None
A5500HI-CMW520-R5501P31			
New	None	None	
Modified	None	None	None
A5500HI-CMW520-R5501P30			
New	None	None	None
Modified	None	None	None
A5500HI-CMW520-R5501P28			
New	None	None	None
Modified	None	None	None
A5500HI-CMW520-R5501P27			
New	None	None	None
Modified	None	None	None
A5500HI-CMW520-R5501P26			
New	None	None	None
Modified	None	None	None
A5500HI-CMW520-R5501P25			
New	None	None	None

Item	MIB file	Module	Description
Modified	None	None	None
A5500HI-CMW520-R5501P23			
New	None	None	None
Modified	None	None	None
A5500HI-CMW520-R5501P22			
New	None	None	None
Modified	None	None	None
A5500HI-CMW520-R5501P21			
New	None	None	None
Modified	None	None	None
A5500HI-CMW520-R5501P20			
New	None	None	None
Modified	None	None	None
A5500HI-CMW520-R5501P19			
New	None	None	None
Modified	None	None	None
A5500HI-CMW520-R5501P17			
New	hh3c-splat-inf-new.mib	HH3C-LswINF-MIB	Added descriptions and support for the following MIBs: <ul style="list-style-type: none"> hh3cifPktBufEntry hh3cifQueuePktBufEntry
Modified	None	None	None
A5500HI-CMW520-R5501P15			
New	None	None	None
Modified	None	None	None
A5500HI-CMW520-R5501P13			
New	hh3c-tunnel.mib	HH3C-TUNNEL-MIB	Added descriptions and support for the following MIBs: <ul style="list-style-type: none"> hh3cTunnelGreTable
	hh3c-slb主.mib	HH3C-SLBG-MIB	Added descriptions and support for the following MIBs: <ul style="list-style-type: none"> hh3cSlbgGroupTable hh3cSlbgPortTable
Modified	None	None	None
A5500HI-CMW520-R5501P12			
New	None	None	None
Modified	None	None	None

Item	MIB file	Module	Description
A5500HI-CMW520-R5501P11			
New	None	None	None
Modified	None	None	None
A5500HI-CMW520-R5501P10			
New	hh3c-pvst.mib	HH3C-LswMSTP-MIB	Added descriptions and support for the following Trap: hh3cPvstVlanPortDetectedTC
Modified	rfc4293-ip.mib	IP-MIB	Changed the access attribution by the following MIBs from read-write to read-only: ipForwarding ipDefaultTTL
A5500HI-CMW520-R5501P06			
New	None	None	None
Modified	None	None	None
A5500HI-CMW520-R5501P05			
New	None	None	None
Modified	None	None	None
A5500HI-CMW520-R5501P03			
New	rfc2096-ip-forward.mib	IP-FORWARD-MIB	Added inetCidrRouteTable. (RFC 4292)
Modified	None	None	None
A5500HI-CMW520-R5501P02			
New	hh3c-ifqos2.mib	HH3C-IFQOS2-MIB	Added descriptions and support for the following MIBs: hh3cIfQoSQSMODETable hh3cIfQoSQSWeightTable hh3cIfQoSHardwareQueueRunInfoTable hh3cIfQoSPortPriorityTable hh3cIfQoSPortPriorityTrustTable
Modified	None	None	None
A5500HI-CMW520-R5501P01			
New	None	None	None
Modified	None	None	None
A5500HI-CMW520-R5501			
New	None	None	None
Modified	None	None	None

Item	MIB file	Module	Description
A5500HI-CMW520-R5206			
New	None	None	None
Modified	None	None	None
A5500HI-CMW520-R5205L01			
New	None	None	None
Modified	rfc1213.mib rfc3418-snmpv2.mib	RFC1213-MIB	The maximum character string length allowed by the sysLocation and sysContact nodes was changed from 200 to 255.
A5500HI-CMW520-R5203P01			
New	None	None	None
Modified	None	None	None
A5500HI-CMW520-R5203			
New	None	None	None
Modified	None	None	None
A5500HI-CMW520-E5201			
New	None	None	None
Modified	hh3c-radius.mib	HH3C-RADIUS-MIB	<p>Changed the value returned by the following MIBs from a plaintext or ciphertext password to empty or "*****".</p> <p>(1)hh3cUserPassword (2)hh3cRdKey (3)hh3cRdSecKey (4)hh3cRdAccKey (5)hh3cRdSecAccKey (6)hh3cRadiusSchAuthPrimKey (7)hh3cRadiusSchAuthSecKey (8)hh3cRadiusSchAccPrimKey (9)hh3cRadiusSchAccSecKey (10)hh3cDot11SrvSecurityPskKeyString (11)hh3cSecureRalmAuthPassword (12)hh3cDot11SecurityPskKeyString</p>
A5500HI-CMW520-R5105			
New	None	None	None
Modified	None	None	None

Item	MIB file	Module	Description
A5500HI-CMW520-F5103			
New	None	None	None
Modified	hh3c-config-man.mib	HH3C-CONFIG-MAN-MIB	Added hh3cCfgLogTable and hh3cCfgOperateTable.
A5500HI-CMW520-F5102			
New	None	None	None
Modified	None	None	None
A5500HI-CMW520-R5101P01			
New	None	None	None
Modified	None	None	None
A5500HI-CMW520-R5101			
New	None	None	None
Modified	hh3c-entity-ext.mib	HH3C-ENTITY-EXT-MIB	Supports node hh3cEntityExtCriticalTemperatureThreshold
A5500HI-CMW520-E5101			
New	First release	First release	First release
Modified	First release	First release	First release

Operation changes

Operation changes in R5501P36

None

Operation changes in R5501P35

None

Operation changes in R5501P33

None

Operation changes in R5501P32

None

Operation changes in R5501P31

None

Operation changes in R5501P30

1. Modified the output from the display current-configuration command

Before modification: The command does not display parameters that use the default values.

After modification: The command displays parameters that use the default values.

Operation changes in R5501P28

None

Operation changes in R5501P27

None

Operation changes in R5501P26

1. Power consumption is reduced due to CPU optimization.
2. CPU debugging functionality is enhanced.
3. The base version of R5501P26 is R5501P23. R5501P26 does not support the authorization VLAN auto-tagging for MAC authentication feature in R5501P25.

Operation changes in R5501P25

None

Operation changes in R5501P23

None

Operation changes in R5501P22

None

Operation changes in R5501P21

None

Operation changes in R5501P20

None

Operation changes in R5501P19

1. OpenFlow can mirror a flow to a maximum of four tunnel interfaces.
2. Added AUTOCFG function on management Ethernet port.

Operation changes in R5501P17

1. Added support of OpenFlow for mirroring traffic to a tunnel interface.
2. Added support of OpenFlow flow tables for counting packets and bytes.

Operation changes in R5501P15

None

Operation changes in R5501P13

1. 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.
2. Change to VLAN assignment for voice users and data users when the server is unreachable
Before modification: When the server is unreachable, both voice users and data users join the critical VLAN.
After modification: When the server is unreachable, voice users join the voice VLAN and data users join the critical VLAN.

Operation changes in R5501P12

None

Operation changes in R5501P11

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

Operation changes in R5501P10

1. Change to route learning after the **ipv6 address dhcp-alloc** command is configured
Before modification, the switch can learn only IPv6 addresses with the prefix as 128 and cannot generate network routes after the **ipv6 address dhcp-alloc** command is configured on an interface.
After modification, the switch can actively send RS messages and RA learning is enabled after the **ipv6 address dhcp-alloc** command is configured on an interface. Then, the following events occur on the switch:
 - The switch can request addresses from a DHCPv6 server and can learn IPv6 addresses with the prefix as 64.
 - The switch can learn the default gateway based on RA messages and add the default gateway to routes.

- The switch can learn a prefix based on RA messages and add the prefix to routes.

Operation changes in R5501P06

1. Change to the PoE feature of 5500HI.

Before modification, when another power supply is supplying power to an Ethernet interface of a PoE switch, the other Ethernet interfaces that are not supplying power on the switch cannot supply power through PoE.

After modification, when another power supply is supplying power to an Ethernet interface of a PoE switch, the other Ethernet interfaces that are not supplying power on the switch still can supply power through PoE. Syslogs are displayed when an Ethernet interface of a PoE switch is supplied with power or Ethernet interfaces of the switch are affected by this modification.

Operation changes in R5501P05

None

Operation changes in R5501P03

Changed the OpenFlow packet-in rate limit from 200 PPS to 1000 PPS.

Added a meter action for Openflow table miss.

Operation changes in R5501P02

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

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

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

Operation changes in R5501P01

None

Operation changes in R5501

Added the function of switching the brand of the device by using the brand command.

Operation changes in R5206

1. Changed the flow control configuration policy.

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

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

2. Added support for displaying log information for ARP attacks found by ARP detection.

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

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

Operation changes in R5205L01

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

Operation changes in R5203P01

None

Operation changes in R5203

None

Operation changes in E5201

Changed the maximum number of static multicast MAC addresses on interfaces from 24 to 32.

Operation changes in R5105

1. Added the following attributes for CDP packets sent by the device: Addresses, Capabilities, Software Version, Platform, Duplex, MTU, and System Name.
2. The default state for all TCP/UDP ports, including TCP ports 23, 80, and 7547 and UDP ports 68, 1812, 3318, and 3799, was changed to disabled.
3. The cluster management feature provides a simple method to manage multiple units using a single IP address, however it does use some protocols that are not considered totally secure. In this release, the cluster management protocols, including NDP, NTDP, and Cluster, are disabled by default to avoid any possible security risks.

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

4. Changed the maximum number of Free IP addresses for 802.1X authentication from 4 to 16.
5. Suffix requirement change for execute batch files
6. Changed the default cluster state from enabled to disabled.
7. Added TCP/UDP ports configuration for portal free rule.

Operation changes in F5103

1. The maximum number of OUIs that the voice VLAN supports was modified from 16 to 128.

2. The maximum number of secondary VLANs that can be associated with an isolate-user-VLAN was modified from 64 to 192.
3. The maximum number of NQA operations that NQA supports was modified from 10 to 64, and the maximum number of concurrent NQA operations was modified from 5 to 30.
4. The patch operation method was modified.
 Before modification: When the device is installing a patch, if the patch has been installed on the device, the device will replace the installed patch with the new patch without any prompts. This causes risks.
 After modification: When the device is installing a patch, if the patch has been installed on the device, the device prompts that "Another patch loaded, please uninstall it first," and you must first uninstall the installed patch and then install the new patch.
5. After the quiet time expires, whether a port is triggered to leave the critical VLAN was modified.
 After a port is assigned to the critical VLAN, the RADIUS server transitions to the block state, and starts the quiet timer, which is configurable and 5 minutes by default.
 Before modification:
 - When the port uses 802.1X authentication and the quiet timer expires, the port leaves the critical VLAN. If the port is configured with the **dot1x critical recovery-action** command, the port triggers 802.1X authentication again after leaving the critical VLAN.
 - When the port uses MAC authentication and the quiet timer expires, the port leaves the critical VLAN.
 After modification:
 When the port uses 802.1X authentication and the quiet timer expires, the port does not leave the critical VLAN. If the port is configured with the **dot1x critical recovery-action** command, the port triggers 802.1X authentication again.
 When the port uses MAC authentication and the quiet timer expires, the port does not leave the critical VLAN and triggers MAC authentication again.
6. If a save operation is performed on a switch where a software version of F5103 or later is running and the version number in the configuration file is lower than F5102, the system first backs up the startup configuration file and then saves the current configuration. For example, suppose the startup configuration file is a.cfg. When a save operation is performed, the system first backs up a.cfg into _a_bak.cfg and then saves the current configuration into a.cfg.

Operation changes in F5102

None

Operation changes in R5101P01

None

Operation changes in R5101

None

Operation changes in E5101

First release

Restrictions and cautions

1. Due to implementation limitations, VLAN ACL does not take effect on ports enabled with QinQ.
2. The priority of a port isolation group is higher than that of the redirect behavior. For example, assume ports GE1/0/1 and GE1/0/2 belong to a port isolation group. If a flow rule is configured on GE1/0/1 to redirect the flow to GE1/0/2, the flow inbound on GE1/0/1 matching the rule for redirection to GE1/0/2 will not be redirected to GE1/0/2 because of a port isolation group is configured.
3. When a policy is applied on a port to implement Committed Access Rate (CAR) for outbound traffic, the queue scheduling on the port fails.
4. In the port mode, the suppression of broadcasts, multicasts, and unknown unicasts in the percentage mode is correct only for 64-byte packets. This is because the chip only supports broadcast suppression by PPS, and the system converts the percentage into PPS per 64 bytes in the percentage mode. The PPS mode is recommended.
5. VCT fails if the connected peer port works in the forced mode and has a rate of 100 Mbps.
6. After QoS policy is applied on almost all the ACL bottom-layer entries, and you save the configuration and restart the system, the order of application may be changed and some applied QoS policy configurations may be lost.
7. GR restrictions in the case of a master/slave switchover: When the master fails and leaves the stack, an interface unplugging event surely occurs because the master provides service interfaces. As a result, the network topology will change. Because the GR feature of routing protocols such as OSPF and ISIS is based on constant topology, the GR feature cannot take effect in this case. To use the GR feature of routing protocols on a stack and thus avoid traffic forwarding interruption after a master/slave switchover, make sure that the protocol interface information does not change due to the master/slave switchover. You can achieve this by inter-device aggregation or inter-device VLAN. That is, on an IRF device, any routing protocol-enabled Layer-3 logical interface must have at least one port on the master and the slave respectively, so that all the routing protocol-enabled Layer-3 logical interfaces keep their state after the master/slave switchover.
8. MAC switchover affects ISIS after master/slave switchover: When a new master is elected, the MAC address of the new master is used, so that the MAC address changes, which is different from the distributed system. The MAC address change will cause neighbor interruption and reestablishment for ISIS, which uses MAC addresses to identify neighbors. As a result, the traffic is interrupted for about 40 seconds. At the same time, the MAC address change will cause IPv6 link-local address changes and thus cause neighbor interruption and reestablishment for all IPv6 routing protocols. As a result, the traffic is interrupted by the master/slave switchover. To solve this problem, IRF introduces the **irf mac-address persistent** command. By default, the MAC changes after a master/slave switchover. A MAC address configured with the timer keyword does not change for six minutes, and a MAC address configured with the always keyword never changes. To avoid traffic interruption caused by a master/slave switchover, use the command to keep the MAC unchanged after the master/slave switchover.
9. Due to route changes, it is normal that the FIB of the new master is inconsistent with that of the old master after a master/slave switchover. If the master is rebooted, a master/slave switchover occurs. In this case, the previous master functions as a newly plugged-in device. Because some routes are canceled, some aged FIB entries will not be synchronized to the newly plugged-in device. Due to route changes, it is normal that the FIB of the new master is inconsistent with that of the old master after the master/slave switchover. After routes on the master become stable, apply the FIB entries again and the new FIB entries will be synchronized to all stack members. The entries to be aged will be deleted in 10 minutes.
10. Release F5102 adopts a new password encryption algorithm. The password saved in the configuration file has been processed by the new algorithm. If you roll back the software from Release F5102 to a version before F5102 the password cannot be restored, and login will fail.

11. MPLS label-based load sharing for link aggregation takes effect only on MPLS intermediate transit nodes.

Open problems and workarounds

201510270393

- Symptom: The mirrored packets are still mirrored to the tunnel interface specified for the deleted Layer 3 remote mirroring configuration.
- Condition: If the following operations have been performed:
 - Configure Layer 3 remote mirroring, and specify a tunnel interface for Layer 3 remote mirroring.
 - Delete the Layer 3 remote mirroring configuration.
 - Configure Layer 3 remote mirroring with another tunnel interface.
- Workaround: Save the configuration and reboot the switch.

List of resolved problems

Resolved problems in R5501P36

201804190493

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

201804280589

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

201712190289

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

201801030312

- Symptom: The role of a device in a VRRP group might frequently switch between Master and Backup.
- Condition: This symptom occurs if the device has been continuously running for 355 weeks.

201712050157

- Symptom: An IRF fabric splits.
- Condition: This symptom occurs if the following operations are performed:
 - a. Service port interface Ethernet xx/0/1 on IRF member devices is assigned to an aggregation group.
 - b. The qinq transparent-vlan command is used to enable transparent transmission for a list of VLANs on the corresponding aggregate interface.

201712120172

- Symptom: The account of a login user is locked.

- Condition: This symptom occurs if the following operations are performed:
 - a. Use the Cisco ISE AAA authentication server to authenticate access users.
 - b. When the login user logs in, the user inputs incorrect login passwords for multiple times.

Resolved problems in R5501P35

201704280459

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

201704270120

- Symptom: CVE-2014-9297
- Condition: An attacker can exploit this issue. When an NTP client decrypted a secret received from an NTP server.

201704270120

- Symptom: CVE-2015-9298
- Condition: An attacker could bypass source IP restrictions and send malicious control and configuration packets.

201707040634

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

201706200187

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

201706200187

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

201706200187

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

201706200187

- Symptom: CVE-2012-2110

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

201708140543

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

201712050136

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

201710230642

- Symptom: In an MPLS network, the routes with 32-bit masks for loopback interfaces are added and deleted multiple times.
- Condition: This symptom occurs if routes or LDP sessions flap.

201611030454

- Symptom: MPLS LDP neighborship fails to be established.
- Condition: This symptom occurs if the device connects to a device of another vendor and tries to establish MPLS LDP neighborship with it.

201709200539

- Symptom: Memory leak occurs when the switch receives specific traffic.
- Condition: This symptom might occur if the switch that enables Openflow receives one type of the following traffic:
 - a. Packet-out messages;
 - b. OFPT_FLOW_MOD messages for adding flow table entries that contain a valid buffer ID;
 - c. ARP or LLDP packets sent from other devices.

Resolved problems in R5501P33

None

Resolved problems in R5501P32

201611220384

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

201612220015

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

201612050252

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

201612050252

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

201703130667

- Symptom: The loopback mode might be automatically enabled for an XFP module.
- Condition: This symptom might occur if an XFP module is installed on the switch.

Resolved problems in R5501P31

201612080502

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

201612220512

- Symptom: A 10G_BASE_ZR_SFP transceiver module is displayed as unidentified in the Web interface.
- Condition: This symptom occurs after you log in to the Web interface for device management and install a 10G_BASE_ZR_SFP transceiver module into an interface.

201701060096

- Symptom: An interface cannot learn the MAC address of a PC connected to an IP phone on an interface when the IP phone and the PC cannot reach the authentication server.
- Condition: This symptom occurs if the following operations are performed:
 - a. Enable port security, and set the port security mode to **userLoginSecure** or **userLoginSecureExt** for the interface.
 - b. Configure a MAC authentication voice VLAN on the interface.

The MAC address of the IP phone is learned in the voice VLAN after the IP phone passes authentication.
 - c. Modify the MAC authentication voice VLAN ID, and configure the MAC authentication critical VLAN or 802.1X critical VLAN as the original MAC authentication voice VLAN ID.

Resolved problems in R5501P30

201609010432

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

201609010374

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

201608290241

- 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.

201609130077

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

201608160021

- Symptom: After an IRF master/subordinate switchover, DHCP snooping entries cannot be restored on the new master from the file used for backing up DHCP snooping entries.
- Condition: This symptom might occur if the following conditions exist:
 - a. The **`dhcp snooping binding database filename`** command is used to specify the file for backing up DHCP snooping entries on an IRF fabric.
 - b. A master/subordinate switchover occurs.

201609070163

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

201609190248

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

201608220435

- Symptom: The **`mac-address max-mac-count`** command is executed to set the MAC learning limit for an interface. When the limit is reached, the system outputs an incorrect message.

- Condition: This symptom might occur if the MAC learning limit of an interface is reached.

201606170069

- Symptom: It takes about 120 seconds to synchronize a new MAC address entry to other slots.
- Condition: This symptom occurs if the **undo mac-address** command is used to delete a MAC address entry on an IRF fabric and then the device learns a new MAC address entry.

Resolved problems in R5501P28

201608180290

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

201608180290

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

201605170555

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

201605170555

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

201607050187

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

201606270469

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

201606280333

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

Transfer Distance(km): 80(9um)

Ordering Name: SFP-GE-LH80-SM1550

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

201607150108

- Symptom: The device reboots unexpectedly.
- Condition: This symptom occurs if the following conditions exist:
 - The number of ECMP routes allowed is 1.
 - Multiple static routes with the same destination address, mask, and preference are configured.

Resolved problems in R5501P27

201606130061

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

Resolved problems in R5501P26

None

Resolved problems in R5501P25

201603040060

- Symptom: When the switch is displaying diagnostic statistics, IRF physical interface flapping, LLDP state changes, and link aggregation group member port state changes might occur.
- Condition: This symptom might occur if the switch displays diagnostic statistics.

Resolved problems in R5501P23

201601040443

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

201603140431

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

201603140376

- Symptom: MFF accesses invalid memory and the switch reboots unexpectedly if certain conditions exist.

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

LSD64848

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

201507090353

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

201601190549

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

201511110159

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

Resolved problems in R5501P22

201601080614

- Symptom: BGP routes cannot be summarized when the labels of the routes change.
- Condition: This symptom might occur if BGP route summarization is enabled and the labels of BGP routes change.

201602010047

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

201512010460

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

201511190090

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

Resolved problems in R5501P21

201501060439

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

201601180342

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

201511100130

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

201512290216

- 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.

Resolved problems in R5501P20

201511120027

- Symptom: The MIB management tool returns 0 as the value of the ifInDiscards node for a non-IRF physical interface on the following types of devices
 - A5500-24G-4SFP HI Switch with 2 interface Slots,
 - 5500-24G-PoE+-4SFP HI Switch with 2 Interface Slots,
 - 5500-24G-SFP HI Switch with 2 Interface Slots,
 - 5500-24G-PoE+-4SFP HI TAA-compliant Switch with 2 Interface Slots,
 - 5500-24G-SFP HI TAA-compliant Switch with 2 Interface Slots switch.
- Condition: This symptom might occur if the MIB management tool is used to obtain the ifInDiscards value for a non-IRF physical interface.

Resolved problems in R5501P19

201507280105

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

201510230173

- Symptom: The CPU usage for a switch in an OpenFlow network exceeds 90%.
- Condition: This symptom occurs if the switch sends a large number of packet-in messages and receives a large number of packet-out messages.

201510210123

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

201510280615

- Symptom: A 10 GE copper port on a subcard always goes down and then comes up after operating for a period of time.
- Condition: This symptom might occur if the 10 GE copper port connects to an NEC server.

201510200101

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

201509300381

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

201510150262

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

201510220542

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

201508310366

- Symptom: The **display storm-constrain** command does not display the known unicast storm control settings.
- Condition: This symptom occurs if the **display storm-constrain** command is executed in interface view to display all storm control settings of the interface.

Resolved problems in R5501P17

201507170252

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

201507160220

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

201507160220

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

201507160220

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

201509160406

- Symptom: The value of the entPhysicalSerialNum node is not updated for a transceiver module in a combo interface when the transceiver module is removed or replaced by another transceiver module.
- Condition: This symptom occurs if the transceiver module is not H3C certified.

201509160406

- Symptom: The entPhysicalSerialNum node returns the serial number of the transceiver module for both the transceiver module and copper port of a combo interface.
- Condition: This symptom occurs if the following operations are performed:
 - Install a transceiver module in a combo interface.
 - Obtain the value of the entPhysicalSerialNum node.

Resolved problems in R5501P15

201506180403

- Symptom: The switch fails to cooperate with a specific authentication server.

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

201507100159

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

201306280329

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

Resolved problems in R5501P13

201506250206

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

201505120391

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

Resolved problems in R5501P12

201505140479

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

201505260034

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

201506080236

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

201406180102

- Symptom: The display transceiver manuinfo command does not display the serial numbers for transceiver modules of WTD that use all-F passwords.
- Condition: This symptom occurs when the display transceiver manuinfo command is executed.

201506270158

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

Resolved problems in R5501P11

201504170082

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

201504170082

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

201505110036

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

201504240250

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

201504140243

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

201504070107

- Symptoms: CVE-2015-0209

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

201504070107

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

201504070107

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

201504070107

- 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.

201504070107

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

Resolved problems in R5501P10

201412080394

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

201501070534

- Symptom: When the HP A5500 HI switch is reading asset management information for power supplies, the system is stuck for about 20 seconds.
- Condition: This symptom occurs when the HP A5500 HI switch uses 150W pluggable power supplies that support asset management (JD362A or JD366A).

201501290196

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

201412260360

- Symptom: The controller receives a `multipart_reply` message 30 seconds after sending a `multipart_request` to a switch.

- Condition: This symptom occurs if the controller sends a multipart_request message to an IRF fabric.

201412260364

- Symptom: After an IRF member switch is rebooted, it keeps rebooting unexpectedly and cannot join an IRF fabric.
- Condition: This symptom occurs when the following conditions exist:
 - OpenFlow is configured on the IRF fabric.
 - An OpenFlow instance is successfully activated and connected to a controller.

201502270218

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

201502160179

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

201503230385

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

201503300039

- Symptom: After the **ipv6 address dhcp-alloc** command is executed on a VLAN interface, the following conditions exist:
 - The switch cannot add routes based on the prefixes learned from RA messages.
 - The prefix length is not displayed in the output from the **display ipv6 interface** command.
- Condition: This symptom might occur if the **ipv6 address dhcp-alloc** command is executed on the VLAN interface.

201503250314

- Symptom: When a configuration file with the **cwmp enable** command is used to recover the configuration, the configuration recovery fails, and the configuration file after recovery still contains the **undo cwmp enable** command. The message showing that "Command cwmp enable fails to recover configuration." appears in the log buffer.
- Condition: This symptom occurs after the following operations are performed:
 - The switch starts with the automatic configuration feature.
 - The switch automatically obtains an IP address from a DHCP server after startup.
 - The switch automatically downloads a configuration file from the TFTP server to recover the configuration. The configuration file contains the **cwmp enable** command.

201501200392

- Symptom: CVE-2015-0205

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

201501200392

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

201501200392

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

201501200392

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

201501200392

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

201501200392

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

Resolved problems in R5501P06

201501130135

- Symptom: BFD peers go down every 24 hours on the switch.
- Condition: This symptom occurs when BFD is enabled on the switch.

201411060566

- Symptom: Some files in the nandflash of the switch are lost.
- Condition: This symptom occurs when errors exist in the nandflash of the switch.

201411190163

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

201410110181

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

201410110326

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

201410110429

- Symptom: After a certain period, the memory is exhausted, and the switch reboots abnormally.
- Condition: This symptom occurs when the following conditions exist:
 - SSL resources are configured in the Web interface for the switch.
 - SSL VPN is not enabled.
 - OSPF is enabled on the switch.

201411190489

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

201411030489

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

201411180434

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

201501060439

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

201412310368

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

201410230229

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

201501120301

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

201412190129

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

201412090423

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

201412220343

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

201501160266

- Symptom: The switch reboots unexpectedly.
- Condition: This symptom can be seen when the following conditions exist in a tunneling network:

- The switch receives an IP packet with a specific option. The option is not IPOPT_EOL (0) or IPOPT_NOP (1). The second byte of the option is 0.
- The IP packet is too long and needs to be fragmented.

201412230355

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

201409050021

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

Resolved problems in R5501P05

201409150368

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

201409010197

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

201408280078

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

201408140565

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

201409040331

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

201409040318

- Symptom: The switch reboots unexpectedly.
- Condition: This symptom occurs when the switch receives abnormal MPLS Echo Replies in an MPLS network.

Resolved problems in R5501P03

201408050475

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

201408050489

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

201407030446

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

201408050575

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

201405230224

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

201407030392

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

201407250142

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

201408040236

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

201407280518

- Symptom: The **voice vlan qos** command does not take effect on a port.
- Condition: This symptom can be seen if the port is configured with **lldp voice-vlan**.

201407220494

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

201407160145

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

201407080366

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

201406200507

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

201407240303

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

201407150532

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

Resolved problems in R5501P02

201405070212

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

201404160027

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

201404250075

- Symptom: A walk on entPhysicalSerialNum MIB returns incorrect fiber module information.

- Condition: This symptom can be seen during a walk on entPhysicalSerialNum MIB.

201404240078

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

201404160434

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

201405190421

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

201406040506

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

201404290204

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

201405270108

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

201406130469

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

201405190429

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

201405270395

- Symptom: The switch fails to deliver LLDP packets to the controller when OpenFlow is enabled.
- Condition: This symptom can be seen if the controller assigns two flow entries. The first entry with low priority has a drop action. The second flow entry with high priority has an action of outputting packets to the controller.

201405130384

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

201404020445

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

201404020414

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

201404020474

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

201404040414

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

201404030004

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

201402110424

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

201404020238

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

201401100054

- Symptom: When a duplicate flow entry is deployed to an OpenFlow switch, the switch prompts "add flow entry", which should be "add duplicate flow entry".

- Condition: This symptom can be seen when a duplicate flow entry is deployed to an OpenFlow switch.

201402250517

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

201403040400

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

201402270224

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

201403010118

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

201404100060

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

201406100280

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

201406180296

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

201406230110

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

201406240634

- Symptom: The **undo transceiver phony-alarm-disable** command is unnecessary and must be deleted.
- Condition: None.

201405220609

- Symptom: The switch fails to deliver VRRP/BGP/OSPF/ISIS/RIP packets to the controller.
- Condition: This symptom can be seen if both VRRP/BGP/OSPF/ISIS/RIP and OpenFlow are enabled on the switch that connects to the controller.

Resolved problems in R5501P01

201312270108

- Symptom: After an IRF master/subordinate switchover, traffic forwarding through new IP flow entries assigned by OpenFlow fails.
- Condition: This symptom can be seen after an IRF master subordinate switchover.

201312220008

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

201311210017

- Symptom: Configuring a next hop for an MPLS L2VPN CCC connection fails.
- Condition: This symptom occurs if the next hop is in the x.x.x.0 format when an x.x.x.0/24 IP address already exists.

201311280479

- Symptom: The switch does not send an ICMPv6 packet upon receiving an IPv6 packet where the Option Type field is 10.
- Condition: This symptom can be seen when the switch enabled with IPv6 receives an IPv6 packet where the Option Type field is 10.

201401070024

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

201401210297

- Symptom: An interface might be set to loopback state.
- Condition: This symptom might occur if the interface continually goes up and down.

201401150513

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

201401130043

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

201401100124

- Symptom: A Table Miss rule in the MAC-IP flow table exists in software but does not exist in hardware.
- Condition: This symptom can be seen if the following conditions exist:

- All hardware ACL resources are used up.
- The action of the assigned Table Miss rule is gototable, and then the Table Miss rule is deleted.

201312230375

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

201401150506

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

Resolved problems in R5501

201311220379

- 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.

201309060056

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

201308290108

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

201305210418

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

201308300169

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

201308060203

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

201308010339

- Symptom: The system repeatedly prompts "The default route has been changed or deleted, protocol is OSPF" when the optimal default route is not changed.

- Condition: This symptom occurs if a non-optimal default route is deleted.

201308080248

- Symptom: NLB does not work for packets destined to a multicast MAC address starting with 01005E.
- Condition: This symptom can be seen when an NLB-enabled switch receives packets destined to a multicast MAC address starting with 01005E.

201312040369

- Symptom: The switch unexpectedly reboots when a packet that includes multiple GRE headers is delivered to the CPU.
- Condition: This symptom occurs when a packet that includes multiple GRE headers is delivered to the CPU.

201311150133

- Symptom: A DHCP response is discarded during inter-VLAN forwarding. The DHCP client thus fails to obtain an IP address.
- Condition: This symptom can be seen when DHCP snooping is globally enabled and multiple VLANs are configured.

201310230091

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

201311280368

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

Resolved problems in R5206

LSD075062

- Symptom: The memory space for hardware entries might have parity errors, resulting in forwarding failures for some packets.
- Conditions: None.

LSD074215

- Symptom: Using HTTPS-based CWMP to upload or download a file fails.
- Conditions: This symptom occurs when you use HTTPS-based CWMP to upload or download a file.

LSD075250

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

ZDD06222

- Symptom: MPLS FRR fails to perform a link switchover.
- Condition: This symptom occurs if the primary path and the backup path overlap on some links.

ZDTB00320

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

ZDTB00321

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

ZDTB00323

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

ZDTB00324

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

ZDD06392

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

LSD075609

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

LSD075361

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

LSD075443

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

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

LSD075171

- Symptom: After an IRF master/subordinate switchover, the network management port cannot be pinged.
- Condition: This symptom occurs if the IRF fabric has multiple routes.

LSD075014

- Symptom: Uploading a configuration file through CWMP fails.
- Condition: This symptom occurs if username/password authentication is adopted and the configuration file exceeds 14 KB.

LSD075271

- Symptom: The switch unexpectedly reboots when the **display diagnostic-information** command is executed.
- Condition: This symptom occurs if the following procedure is performed:
 - a. Configure a command that contains %n.
 - b. Reboot the switch.
 - c. Execute the **display diagnostic-information** command.

LSD074857

- Symptom: The CPU usage on a PoE switch is 100 % when IMC performs device information synchronization.
- Condition: This symptom occurs if the electrical label information stored on the power supply is corrupted.

Resolved problems in R5205L01

LSD074592

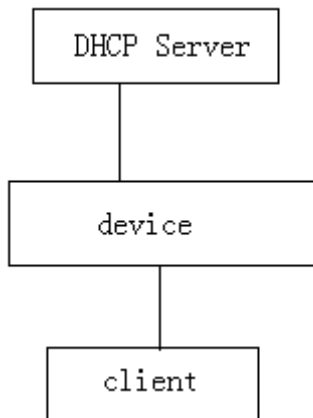
- Symptom: The software drops the multi-tagged ARP packets received from a QinQ-enabled port.
- Condition: Configure the link type of a port as trunk or hybrid, enable QinQ on the port, and assign the port to a VLAN with ARP detection or ARP snooping enabled.

LSD074756

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

LSD074348

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



LSD075076

- Symptom: It takes about 15 seconds for the LSPM1XGT2P (JG535A) to be identified. A normal speed is 5 seconds.
- Condition: The LSPM1XGT2P (JG535A) uses a firmware version higher than 163.

Resolved problems in R5203P01

None.

Resolved problems in R5203

ZDTB00315

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

ZDTB00312

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

ZDTB00309

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

LSD074256

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

LSD074279

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

LSD074423

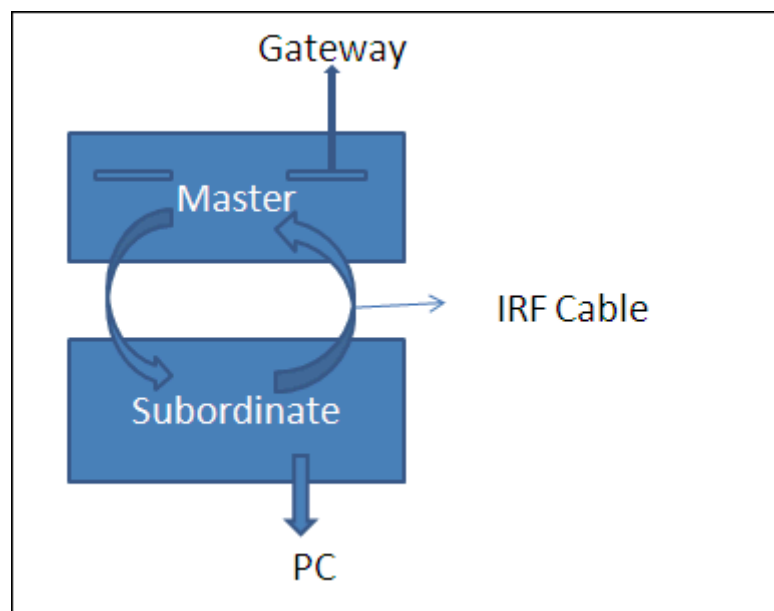
- Symptom: After a PC passes MAC authentication on a port, the port still discards IGMP report packets from the PC.
- Condition: This symptom occurs if the port works in userlogin-secure-or-mac-ext mode and is enabled with both MAC authentication and 802.1X authentication.

ZDTB00308

- Symptom: LDP fails to establish a session with a device if the packets received from that device contain a non-zero label.
- Condition: This symptom occurs if the packets received from a device contain a non-zero label.

LSD074444

- Symptom: A ring-topology IRF fabric, as shown in the following figure, discards ARP responses from the gateway, and thus cannot learn the MAC address of the gateway.
- Condition: This symptom occurs when the following conditions exist:
 - The master in the IRF fabric is an A5500-48G-4SFP HI or 5500-48G-PoE+-4SFP HI switch where a port with a port ID larger than 24 connects to the gateway.
 - ARP packets are processed by the software (for example, ARP detection).



Resolved problems in E5201

None.

Resolved problems in R5105

LSD073080

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

ZDTB00305

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

ZDTB00304

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

LSD073254

- Symptom: The memory space for hardware entries such as Layer 3 forwarding entries might have parity errors, resulting in forwarding failures for some packets or system reboot.
- Condition: This symptom might occur to the memory space for hardware entries.

ZDTB00301

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

ZDTB00302

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

ZDTB00298

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

LSD074033

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

LSD073845

- Symptom: ARP does not learn the addresses in an ARP reply in which the target MAC address in the message body is different from the destination MAC address in the message header.

- Condition: This symptom can be seen when the switch receives an ARP reply in which the target MAC address in the message body is different from the destination MAC address in the message header.

LSD073696

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

Resolved problems in F5103

LSD071258

- Symptom: If a link goes up and down, packet loss occurs to some flows for five to seven minutes.
- Condition: In the network, there are multiple BGP route reflectors and a large number of routes which have the same prefix but are from different neighbors or have different next hops.

LSD070340

- Symptom: When an illegal user accesses the device through an NMS, the device reboots.
- Condition: Configure SNMPv3 to permit legal users by using an ACL that is configured with the logging keyword

ZDTB00288

- Symptom: The IP address of a Null interface can be assigned through SNMP but cannot be deleted through SNMP or CLI.
- Condition: This symptom occurs if the IP address of the Null interface is assigned by the MIB browser.

ZDTB00293

- Symptom: An SNMP walk on the lldpRemSysName MIB node returns "No Such Instance currently exists at this OID."
- Condition: This symptom occurs if the port has LLDP neighbors, the TimeFilter value is set to 0, and the SNMP tool is used to walk on the lldpRemSysName MIB node.

ZDTB00287

- Symptom: When the BGP routes must be filtered by a large number of filtering policies which contain as-path and community attributes and also contain regular expressions, the processing efficiency is low. When a certain number of BGP routes mentioned above flap, the CPU usage remains high.
- Condition: This symptom occurs when a large number of BGP route filtering policies which contain as-path and community attributes and also contain regular expressions are configured and the BGP routes flap.

Resolved problems in F5102

None.

Resolved problems in R5101P01

LSD66075

- Symptom: The transceiver cannot go up.
- Condition: Insert a non-HP transceiver and connect the fiber.

Resolved problems in R5101

LSD59831

- Symptom: After the reboot, the 10GE port on the local device cannot go up.
- Condition: Connect a 10GE port of an SFP+ subcard on the local device to a peer device by using an IRF cable. Then, the peer device reboots.

LSD63811

- Symptom: Memory leaks occur.
- Condition: When a large number of VSI MAC addresses exist, enable MAC address roaming, and perform the **undo mac-address** command repeatedly.

Resolved problems in E5101

First release

Support and other resources

Accessing Hewlett Packard Enterprise Support

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

Information to collect:

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

Documents

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

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

Related documents

The following documents provide related information:

- HP 5500 HI Switch Series Installation Guide
- HP 5500 HI Switch Series Command References - Release 52xx
- HP 5500 HI Switch Series Configuration Guides - Release 52xx
- HP PSR150-A & PSR150-D Series Power Supplies User Guide
- HP PSR720-56A Power Supply User Guide
- HP PSR1110-56A Power Supply User Guide

Documentation feedback

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

Appendix A Feature list

Hardware features

Table 5 HP 5500 HI Switch Series models

Type	Product code	HP description	Alias
Non PoE+ type	JG311A	HP A5500-24G-4SFP HI Switch with 2 interface Slots	A5500-24G-4SFP HI (2 slots)
	JG312A	HP A5500-48G-4SFP HI Switch with 2 interface Slots	A5500-48G-4SFP HI (2 slots)
	JG543A	HP 5500-24G-SFP HI Switch with 2 Interface Slots	5500-24G-SFP HI (2 slots)
	JG681A	HP 5500-24G-SFP HI TAA-compliant Switch with 2 Interface Slots	5500-24G-SFP HI TAA (2 slots)
PoE+ type	JG541A	HP 5500-24G-PoE+-4SFP HI Switch with 2 Interface Slots	5500-24G-PoE+-4SFP HI (2 slots)
	JG542A	HP 5500-48G-PoE+-4SFP HI Switch with 2 Interface Slots	5500-48G-PoE+-4SFP HI (2 slots)
	JG679A	HP 5500-24G-PoE+-4SFP HI TAA-compliant Switch with 2 Interface Slots	5500-24G-PoE+-4SFP HI TAA (2 slots)
	JG680A	HP 5500-48G-PoE+-4SFP HI TAA-compliant Switch with 2 Interface Slots	5500-48G-PoE+-4SFP HI TAA (2 slots)

Hardware features

Table 6 HP 5500 HI Switch Series technical specifications

Item	A5500-24G-4 SFP HI (2 slots)	A5500-48G-4 SFP HI (2 slots)	5500-24G-SFP HI (2 slots) 5500-24G-SFP HI TAA (2 slots)	5500-24G-PoE+-4SFP HI (2 slots) 5500-24G-PoE+-4SFP HI TAA (2 slots)	5500-48G-PoE+-4SFP HI (2 slots) 5500-48G-PoE+-4SFP HI TAA (2 slots)
Dimensions (H × W × D)	43.6 × 440 × 360 mm (1.72 × 17.32 × 14.17 in)	43.6 × 440 × 420 mm (1.72 × 17.32 × 16.54 in)	43.6 × 440 × 360 mm (1.72 × 17.32 × 14.17 in)	43.6 × 440 × 460 mm (1.72 × 17.32 × 18.11 in)	43.6 × 440 × 460 mm (1.72 × 17.32 × 18.11 in)
Weight	< 7.5 kg (16.53 lb)	< 8.5 kg (18.74 lb)	< 7.5 kg (16.53 lb)	< 10 kg (22.05 lb)	<10.5 kg (23.15 lb)
Management ports	1 console port, 1 management Ethernet port, both on the front panel				

Item	A5500-24G-4 SFP HI (2 slots)	A5500-48G-4 SFP HI (2 slots)	5500-24G-SFP HI (2 slots) 5500-24G-SFP HI TAA (2 slots)	5500-24G-PoE+-4SFP HI (2 slots) 5500-24G-PoE+-4SFP HI TAA (2 slots)	5500-48G-PoE+-4SFP HI (2 slots) 5500-48G-PoE+-4SFP HI TAA (2 slots)
Fixed network ports (on the front panel)	24 × 10/100/1000Base-T auto-sensing Ethernet ports 4 × 100/1000Base-X SFP ports 2 × 1/10 Gbps SFP+ ports	48 × 10/100/1000Base-T auto-sensing Ethernet ports 4 × 100/1000Base-X SFP ports 2 × 1/10 Gbps SFP+ ports	24 × 100/1000Base-X Gigabit SFP ports + 4 × 10/100/1000Base-T Ethernet ports + 2 × SFP plus ports	24 × 10/100/1000Base-T Ethernet ports(POE) + 4 × 100/1000Base-X Gigabit SFP ports + 2 × SFP plus ports	48 × 10/100/1000Base-T Ethernet ports(POE) + 4 × 100/1000Base-X Gigabit SFP ports + 2 × SFP plus ports
Interface card slots	2 (SLOT1 and SLOT2), on the rear panel	2 (SLOT1 and SLOT2), on the rear panel	2 (SLOT1 and SLOT2), on the rear panel	2 (SLOT1 and SLOT2), on the rear panel	2 (SLOT1 and SLOT2), on the rear panel
Interface card options	<ul style="list-style-type: none"> LSPM2GP2P (JD367A) (not supporting IRF) LSPM1CX2P (JD360B) (supporting IRF) LSPM2SP2P (JD368B) (supporting IRF) LSPM1XP2P (JD359B) (supporting IRF) LSPM1XP1P (JD361B) (supporting IRF) LSPM1XGT2P (JG535A) (supporting IRF) LSP5GP8P0 (JG314A) (not supporting IRF) LSP5GT8P (JG313A) (not supporting IRF) <p>NOTE: On the A5500-24G-4SFP HI/ 5500-24G-SFP HI/ 5500-24G-SFP HI TAA (2 slots)/ 5500-24G-PoE+-4SFP HI/ 5500-24G-PoE+-4SFP HI TAA (2 slots) switches, you can install the LSP5GP8P0 or LSP5GT8P interface card only in SLOT1.</p>				
Power supply slots	2, on the rear panel				
Hot-swappable power supply options	PSR150-A (JD362A) (AC-input), PSR150-D (JD366A) (DC-input) NOTE: <ul style="list-style-type: none"> You can install one power supply, or for redundancy, two power supplies for your switch. The HP 5500 HI Switch Series supports a mix of PSR150-A and PSR150-D power supplies.			X362 720W AC PoE Power Supply (JG544A) (AC-input), X362 1110W AC PoE Power Supply (JG545A) (AC-input) NOTE: <ul style="list-style-type: none"> You can install one power supply, or for redundancy, two power supplies for your switch. The HP 5500 HI Switch Series supports a mix of 720W and 1100W power supplies.	

Item	A5500-24G-4 SFP HI (2 slots)	A5500-48G-4 SFP HI (2 slots)	5500-24G-SF P HI (2 slots) 5500-24G-SF P HI TAA (2 slots)	5500-24G-Po E+-4SFP HI (2 slots) 5500-24G-Po E+-4SFP HI TAA (2 slots)	5500-48G-Po E+-4SFP HI (2 slots) 5500-48G-Po E+-4SFP HI TAA (2 slots)
Input voltage	<div>1. AC-input</div> <ul style="list-style-type: none">Rated voltage range: 100 VAC to 240 VAC, 50 Hz or 60 HzMax voltage range: 90 VAC to 264 VAC, 47 Hz to 63 Hz <div>2. –48 VDC input</div> <ul style="list-style-type: none">Rated voltage range: –48 VDC to –60 VDCMax voltage range: –36 VDC to –72 VDC <div>NOTE:</div> <div>You can use the site –48 VDC power supply, or an external RPS power supply unit—A-RPS800 (JD183A) or A-RPS1600 (JG136A)—recommended by HP to provide power supply.</div>			<ul style="list-style-type: none">For 720 W power modules:<ul style="list-style-type: none">Rated input voltage: 100 VAC to 240 VAC @ 50 or 60 HzMaximum input voltage: 90 VAC to 264 VAC @ 47 or 63 HzFor 1110 W power modules:<ul style="list-style-type: none">Rated input voltage: 115 VAC to 240 VAC @ 50 or 60 Hz <div>Maximum input voltage: 102.5 VAC to 264 VAC @ 47 or 63 Hz</div>	
Minimum power consumption	62 W	94 W	60 W	80 W	115 W
Maximum power consumption	141 W	191 W	135 W	950 W	1840 W
Cooling system	4 built-in fans (3 for the chassis, 1 for interface card slot 1) 1 fan on each power supply Side-to-side air flow			2 built-in fans (for the chassis) 1 fan on each power supply Side-to-side air flow	3 built-in fans (for the chassis) 1 fan on each power supply Side-to-side air flow
Operating temperature	0°C to 50°C (32°F to 122°F) (at most 45°C/113°F when the 40KM/80KM XFP transceiver module is used)			0°C to 45°C (32°F to 113°F)	
Relative humidity	5% to 95%, noncondensing				

Software features

Table 7 Software features of the 5500 HI series

Feature	A5500-24G-4SFP HI (2 slots)	5500-24G-SFP HI (2 slots) 5500-24G-SFP HI TAA (2 slots)	5500-24G-PoE+-4SFP HI (2 slots) 5500-24G-PoE+-4SFP HI TAA (2 slots)	A5500-48G-4SFP HI (2 slots)	5500-48G-PoE+-4SFP HI (2 slots) 5500-48G-PoE+-4SFP HI TAA (2 slots)
Switching capacity (Full duplex)	176 Gbps			224 Gbps	
Packet forwarding rate (whole system)	130.9 Mpps			166.6 Mpps	
Link aggregation	<ul style="list-style-type: none">Link aggregation control protocol (LACP)Static link aggregationSupports up to 128 aggregation groups, each supporting up to eight GE ports or eight 10-GE ports				
Flow control	<ul style="list-style-type: none">IEEE 802.3x flow control (full duplex)Storm control based on the port rate ratioStorm control based on pps				
Jumbo Frame	Supports a maximum frame size of 12 KB				
MAC address table	<ul style="list-style-type: none">32K MAC addresses1K static MAC addressesBlackhole MAC addressesLimit to the number of MAC addresses learned on a portStatic multicast MAC addresses				
VLAN	<ul style="list-style-type: none">Port-based VLANs (4094 VLANs)QinQ and selective QinQVoice VLANProtocol-based VLANsMAC-based VLANsIP subnet-based VLANsGVRPIsolate User VLANSuper VLAN				
VLAN mapping	<ul style="list-style-type: none">One-to-one VLAN mappingMany-to-one VLAN mappingTwo-to-two VLAN mapping				
ARP	<ul style="list-style-type: none">16K entries1K static entriesGratuitous ARPStandard proxy ARP and local proxy ARPARP source suppressionARP detection (based on DHCP snooping entries/802.1X security entries/static IP source guard binding Entries/OUI MAC addresses)				

Feature	A5500-24G-4SFP HI (2 slots)	5500-24G-SFP HI (2 slots) 5500-24G-SFP HI TAA (2 slots)	5500-24G-PoE+4SFP HI (2 slots) 5500-24G-PoE+4SFP HI TAA (2 slots)	A5500-48G-4SFP HI (2 slots)	5500-48G-PoE+4SFP HI (2 slots) 5500-48G-PoE+4SFP HI TAA (2 slots)
ND	<ul style="list-style-type: none"> • 8K entries • 1K static entries • ND proxy • IPv6 ND detection • IPv6 ND snooping 				
VLAN interface	1K				
Layer 3 routing interface	Routing interface				
DHCP	<ul style="list-style-type: none"> • DHCP client • DHCP snooping • DHCP relay agent • DHCP server • DHCP snooping Option 82 support/DHCP relay agent Option 82 support • DHCPv6 client • DHCPv6 snooping • DHCPv6 relay agent • DHCPv6 server 				
UDP Helper	UDP Helper				
DNS	<ul style="list-style-type: none"> • Static domain name resolution • Dynamic domain name resolution client • IPv4/IPv6 addresses 				
IPv4 route	<ul style="list-style-type: none"> • 1K static routes • RIP v1/2; up to 2K IPv4 routes • OSPF v1/v2; up to 12K IPv4 routes • BGP; up to 12K IPv4 routes • ISIS; up to 12K IPv4 routes • Up to eight equal-cost routes • Routing policy • VRRP • Policy-based routing 				
IPv6 route	<ul style="list-style-type: none"> • 1K static routes • RIPng; up to 2K IPv6 routes • OSPF v3; up to 6K IPv6 routes • BGP4+ for IPV6; up to 6K IPv6 routes • ISIS for IPV6; up to 6K IPv6 routes • Up to eight equal-cost routes • Routing policy • VRRP • Policy-based routing 				
URPF	Reverse route check				
MCE	Supported				

Feature	A5500-24G-4SFP HI (2 slots)	5500-24G-SFP HI (2 slots) 5500-24G-SFP HI TAA (2 slots)	5500-24G-PoE+-4SFP HI (2 slots) 5500-24G-PoE+-4SFP HI TAA (2 slots)	A5500-48G-4SFP HI (2 slots)	5500-48G-PoE+-4SFP HI (2 slots) 5500-48G-PoE+-4SFP HI TAA (2 slots)
BFD	<ul style="list-style-type: none"> • OSPF • BGP • IS-IS • Static route 				
IPv6 over IPv4 Tunnel	<ul style="list-style-type: none"> • IPv6 manual tunnel • 6to4 tunnel • ISATAP (Intra-Site Automatic Tunneling Protocol) tunnel • IPv6 in IPv6 tunnel • IPv4 in IPv6 tunnel • GRE tunnel 				
IPv4 multicast	<ul style="list-style-type: none"> • IGMP snooping v1/v2/v3 • Multicast VLAN • Multicast VLAN+ • IGMP v1/v2/v3 • PIM-DM • PIM-SM • PIM-SSM • MSDP • MBGP • PIM snooping • Multicast control • IGMP snooping proxy • BIDIR-PIM • VPN support for multicast 				
IPv6 multicast	<ul style="list-style-type: none"> • MLD Snooping v1/v2 • MLD v1/v2 • MLD proxy • PIM-DM/SM/SSM for IPv6 • IPv6 multicast VLAN • IPv6 multicast VLAN+ • MBGP for IPv6 • IPv6 multicast control • MLD snooping proxy 				
MPLS	<ul style="list-style-type: none"> • MPLS forwarding, including MPLS LER and MPLS LSR • LSR • LDP • MPLS TE • L2VPN • L3VPN • VPLS 				
Broadcast/multicast/unicast storm control	<ul style="list-style-type: none"> • Storm control based on port rate ratio • PPS-based storm control 				

Feature	A5500-24G-4SFP HI (2 slots)	5500-24G-SFP HI (2 slots) 5500-24G-SFP HI TAA (2 slots)	5500-24G-PoE+4SFP HI (2 slots) 5500-24G-PoE+4SFP HI TAA (2 slots)	A5500-48G-4SFP HI (2 slots)	5500-48G-PoE+4SFP HI (2 slots) 5500-48G-PoE+4SFP HI TAA (2 slots)
MSTP	<ul style="list-style-type: none"> • STP/RSTP/MSTP protocol • STP Root Guard • BPDU Guard 				
RRPP	<ul style="list-style-type: none"> • RRPP protocol • Multi-instance RRPP 				
Smart link	<ul style="list-style-type: none"> • Supports smart link • Multi-instance Smart Link 				
Monitor link	Supported				
QoS/ACL	<ul style="list-style-type: none"> • Restriction of the rates at which a port sends and receives packets, with a granularity of 8 kbps. • Packet redirection • 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 round robin (WRR), WFQ (Weighted Fair Queuing), SP + WRR 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 • Ingress ACL and egress ACL • Applying ACL to VLANs • Weighted Random Early Detection (WRED) • Traffic shaping • User Profile • 48 queues for sending packets to the CPU 				
Mirroring	<ul style="list-style-type: none"> • Traffic mirroring • Port mirroring • Multiple monitor ports per mirroring group • Local port mirroring and remote port mirroring • Support of remote port mirroring for multiple monitor ports and reflector ports 				
PoE	<ul style="list-style-type: none"> • Each PoE port can provide up to 30 W power at the same time (only available on an 5500-24G-PoE+4SFP HI (2 slots)/ 5500-24G-PoE+4SFP HI TAA (2 slots)/ 5500-48G-PoE+4SFP HI (2 slots)/ 5500-48G-PoE+4SFP HI TAA (2 slots). 				

Feature	A5500-24G-4SFP HI (2 slots)	5500-24G-SFP HI (2 slots) 5500-24G-SFP HI TAA (2 slots)	5500-24G-PoE+-4SFP HI (2 slots) 5500-24G-PoE+-4SFP HI TAA (2 slots)	A5500-48G-4SFP HI (2 slots)	5500-48G-PoE+-4SFP HI (2 slots) 5500-48G-PoE+-4SFP HI TAA (2 slots)
Security	<ul style="list-style-type: none"> • Hierarchical management and password protection of users • AAA authentication • RADIUS authentication • HWTACACS • SSH 2.0 • Port isolation • Port security • MAC address authentication • IP-MAC-port binding • IP Source Guard • HTTPS • SSL • PKI • Portal • EAD • Boot ROM access control (password recovery) • Triple authentication • Redundant RADIUS servers • IPv6 RADIUS server • IPv6 port binding 				
802.1X	<ul style="list-style-type: none"> • Up to 2K users • Port-based and MAC address-based authentication • Guest VLAN • Trunk port authentication • 802.1x-based dynamic QoS/ACL/VLAN delivery 				
IRF2	<ul style="list-style-type: none"> • IRF2 • Distributed device management, distributed link aggregation, and distributed resilient routing • Forming an IRF through SFP+/XFP/CX4 ports • Local IRF and remote IRF • 120 Gbps of bandwidth per IRF virtual device • 60 Gbps of bandwidth per extended IRF port • ISSU 				
Loading and upgrading	<ul style="list-style-type: none"> • Loading and upgrading through XModem protocol • Loading and upgrading through FTP • Loading and upgrading through TFTP 				

Feature	A5500-24G-4SFP HI (2 slots)	5500-24G-SFP HI (2 slots) 5500-24G-SFP HI TAA (2 slots)	5500-24G-PoE+-4SFP HI (2 slots) 5500-24G-PoE+-4SFP HI TAA (2 slots)	A5500-48G-4SFP HI (2 slots)	5500-48G-PoE+-4SFP HI (2 slots) 5500-48G-PoE+-4SFP HI TAA (2 slots)
Management	<ul style="list-style-type: none"> • Configuration at the command line interface • Remote configuration through Telnet • Configuration through Console port • Simple network management protocol (SNMP) • Remote monitoring (RMON) alarm, event and history recording • RMON2 • intelligent management center (iMC) • Web-based network management • System log • Hierarchical alarms • Huawei group management protocol (HGMP) v2 • NTP • Power supply alarm function • Fan and temperature alarms 				
Maintenance	<ul style="list-style-type: none"> • Debugging information output • Ping and Tracert • NQA • Track • Remote maintenance through Telnet • Virtual cable test • 802.1ag • 802.3ah • DLDP • NetStream • sFlow • IRDP 				
Energy saving	<ul style="list-style-type: none"> • One-key energy saving • Energy Efficient Ethernet, IEEE 802.3az • Automatic port power down • Scheduled port down (scheduled job) 				

Appendix B Upgrading software

You can upgrade software from Boot ROM menus or the CLI.

Table 8 Software upgrade methods

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

Software images include the system software image and the Boot ROM image. They are packaged in a .bin file. You can download this file to upgrade both Boot ROM and system software, or upgrade only Boot ROM.

The Boot ROM image in the .bin package file consists of a basic segment and an extended segment. The basic segment is the minimum boot image. The extended segment enables the Boot ROM to bootstrap the system and upgrade system software.



IMPORTANT:

When upgrading Boot ROM, upgrade both segments to ensure the functionality of the entire system.

NOTE:

- For the 5500 HI switches, HP recommends that you use the management Ethernet port to download image files. This port can work even if all network ports have failed.
- You download files through the management Ethernet port in the same way as through a common Ethernet network port. This appendix uses a common Ethernet network port as an example.

Upgrading software from Boot ROM menus

The Boot ROM menus include a basic Boot menu and an extended Boot menu.

The basic Boot menu is provided by the basic Boot ROM segment. From this menu, you can upgrade Boot ROM and run the extended Boot ROM. For more information, see "[Accessing the basic Boot menu](#)."

The extended Boot menu is provided by the extended Boot ROM segment. From this menu, you can perform various tasks, including upgrading Boot ROM, upgrading and managing system software images, and managing files. For more information, see "[Accessing the extended Boot menu](#)."

Both the basic Boot menu and extended Boot menu support using XMODEM to upgrade Boot ROM through the console port.

If the extended Boot ROM segment has corrupted, you can repair or upgrade it from the basic Boot menu.

NOTE:

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

To upgrade software from Boot ROM menus:

1. Connect a configuration terminal such as a PC to the console port of the switch with a console cable.
2. Run the terminal emulation program on the PC.
3. Power on the switch.

The switch starts up and displays the following message:

```
Starting.....
Press Ctrl+D to access BASIC BOOT MENU
Press Ctrl+T to start memory test
Press Ctrl+E to start heavy memory test

*****
*
*   HP A5500-48G-4SFP HI Switch with 2 interface Slots BOOTROM, Version 209   *
*
*****
Copyright (c) 2010-2012 Hewlett-Packard Development Company, L.P.

Creation Date   : Dec 28 2012,14:10:14
CPU Clock Speed : 750MHz
Memory Size     : 1024MB
Flash Size      : 512MB
CPLD Version    : 003
PCB Version     : Ver.B
Mac Address     : AA1122334455

Press Ctrl-B to enter Extended Boot menu...1
```

4. Press one of the shortcut key combinations at prompt.

Table 9 Shortcut keys

Shortcut keys	Prompt message	Function	Remarks
Ctrl+B	Press Ctrl-B to enter Extended Boot menu...	Accesses the extended Boot menu.	Press the keys within 1 second (in fast startup mode) or 5 seconds (in full startup mode) after the message appears. You can upgrade and manage system software and Boot ROM from this menu.
Ctrl+D	Press Ctrl+D to access	Accesses the basic Boot	Press the keys within 1

	BASIC BOOT MENU	menu.	second after the message appears. You can upgrade Boot ROM or access the extended Boot ROM segment from this menu.
Ctrl+E	Press Ctrl+E to start heavy memory test	Performs a RAM pressure test.	Press the keys within 1 seconds after the message appears.
Ctrl+T	Press Ctrl+T to start memory test	Performs a RAM self-test.	Press the keys within 1 seconds after the message appears. Alternatively, you can choose option 1 from the BASIC-ASSISTANT menu to perform the task.

Accessing the basic Boot menu

To access the basic Boot menu:

1. Press Ctrl+D within 1 second after the "Press Ctrl+D to access BASIC BOOT MENU" prompt message appears. If you fail to do this within the time limit, the system starts to run the extended Boot ROM segment.

```
*****
*
*                               *
*                BASIC BOOTROM, Version 211                *
*                               *
*
*****

BASIC BOOT MENU

1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
4. Boot extended BootRom
0. Reboot
Ctrl+U: Access BASIC-ASSISTANT MENU

Enter your choice(0-4):
```

Table 10 Basic Boot menu options

Option	Task
1. Update full BootRom	Update the entire Boot ROM, including the basic segment and the extended segment. To do so, you must use XMODEM and the console port. For more information, see xxx.
2. Update extended BootRom	Update the extended Boot ROM segment. To do so, you must use XMODEM and the console port. For more information, see xxx.

Option	Task
3. Update basic BootRom	Update the basic Boot ROM segment. To do so, you must use XMODEM and the console port. For more information, see xxx.
4. Boot extended BootRom	Access the extended Boot ROM segment. For more information, see Accessing the extended Boot menu .
0. Reboot	Reboot the switch.
Ctrl+U: Access BASIC-ASSISTANT MENU	Press Ctrl + U to access the BASIC-ASSISTANT menu (see Table 11).

Table 11 BASIC-ASSISTANT menu options

Option	Task
1. RAM Test	Perform a RAM self-test.
2. Reserved	Reserved option field.
3. Reserved	Reserved option field.
4. Reserved	Reserved option field.
0. Return to boot menu	Return to the basic Boot menu.

Accessing the extended Boot menu

To access the extended Boot menu:

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

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

Alternatively, you can enter **4** in the basic Boot menu to access the extended Boot menu.

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

The "Password recovery capability is enabled." or "Password recovery capability is disabled." message appears, followed by the extended Boot menu. Availability of some menu options depends on the state of password recovery capability (see [Table 12](#)). For more information about password recovery capability, see *HP 5500 HI Switch Series Fundamentals Configuration Guide*.

Password recovery capability is enabled.

BOOT MENU

1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Reserved
9. Set switch startup mode

0. Reboot
 Ctrl+F: Format File System
 Ctrl+P: Skip Super Password
 Ctrl+R: Download application to SDRAM and Run
 Ctrl+Z: Access EXTEND-ASSISTANT MENU

Enter your choice(0-9):

Table 12 Extended Boot menu options

Option	Tasks
1. Download application file to flash	Download a .bin software package file to the flash. If password recovery capability is enabled, you can use any version of the system software image for upgrade. If password recovery capability is disabled, you can use only the Release 5105 version (or higher) for upgrade.
2. Select application file to boot	<ul style="list-style-type: none"> Specify the main and backup system software images for the next startup: <ul style="list-style-type: none"> If password recovery capability is enabled, you can specify a system software image of any version. If password recovery capability is disabled, the system software image version must be Release 5105 or higher. Specify the main and backup configuration files for the next startup. This task can be performed only if password recovery capability is enabled.
3. Display all files in flash	Display files on the flash.
4. Delete file from flash	Delete files to free storage space.
5. Restore to factory default configuration	Delete the current next-startup configuration files and restore the factory-default configuration. This option is available only if password recovery capability is disabled.
6. Enter BootRom upgrade menu	Access the Boot ROM upgrade menu. If password recovery capability is enabled, you can upgrade the Boot ROM to any version. If password recovery capability is disabled, you can upgrade the Boot ROM to only Version 120 or higher.
7. Skip current system configuration	Start the switch without loading any configuration file. This is a one-time operation and takes effect only for the first system boot or reboot after you choose this option. This option is available only if password recovery capability is enabled.
8. Reserved	Reserved option field.
9. Set switch startup mode	Set the startup mode to fast startup mode or full startup mode.
0. Reboot	Reboot the switch.
Ctrl+F: Format File System	Format the current storage medium.
Ctrl+P: Skip Super Password	Load the next-startup configuration file with all user privilege passwords configured with the super password command ignored. This is a one-time operation and takes effect only for the first system boot or reboot after you choose this option. This option is available only if password recovery capability is enabled.

Option	Tasks
Ctrl+R: Download application to SDRAM and Run	Download a system software image and start the switch with the image. This option is available only if password recovery capability is enabled.
Ctrl+Z: Access EXTEND-ASSISTANT MENU	Access the EXTEND-ASSISTANT menu. For options in the menu, see Table 13 .

Table 13 EXTEND-ASSISTANT menu options

Option	Task
1. Display Memory	Display data in the memory.
2. Search Memory	Search the memory for a specific data segment.
0. Return to boot menu	Return to the extended Boot menu.

NOTE:

The procedure of upgrading Boot ROM is the same as upgrading system software. This guide takes upgrading Boot ROM as an example.

XMODEM download through the console port

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

Setting terminal parameters

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

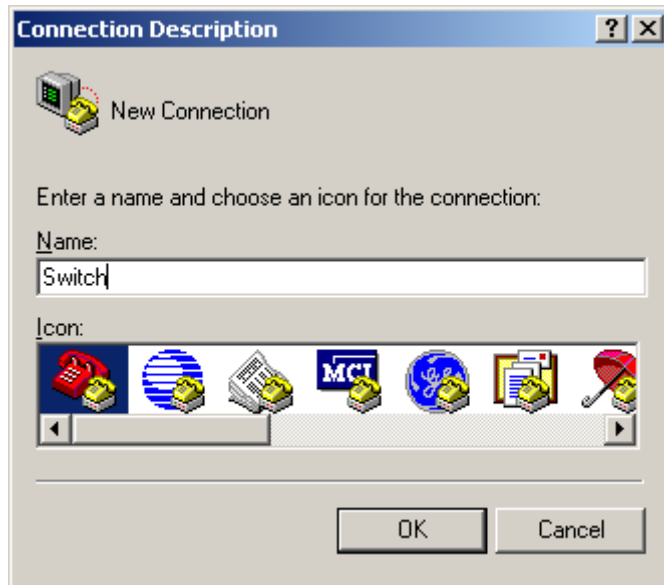
The following are the required terminal settings:

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

To set terminal parameters, for example, on a Windows XP HyperTerminal:

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

Figure 1 Connection description of the HyperTerminal



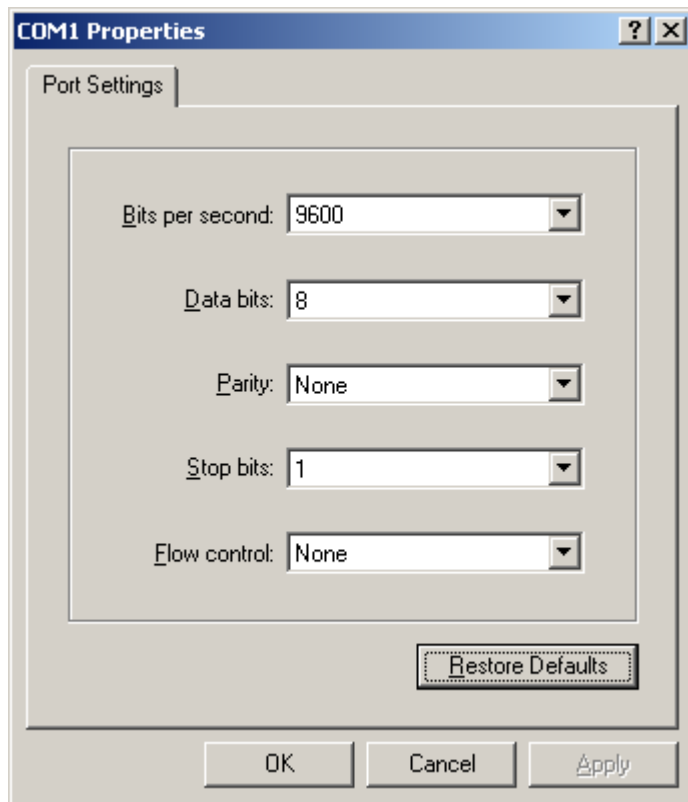
2. Select the serial port to be used from the **Connect using** drop-down list, and click **OK**.

Figure 2 Setting the serial port used by the HyperTerminal connection



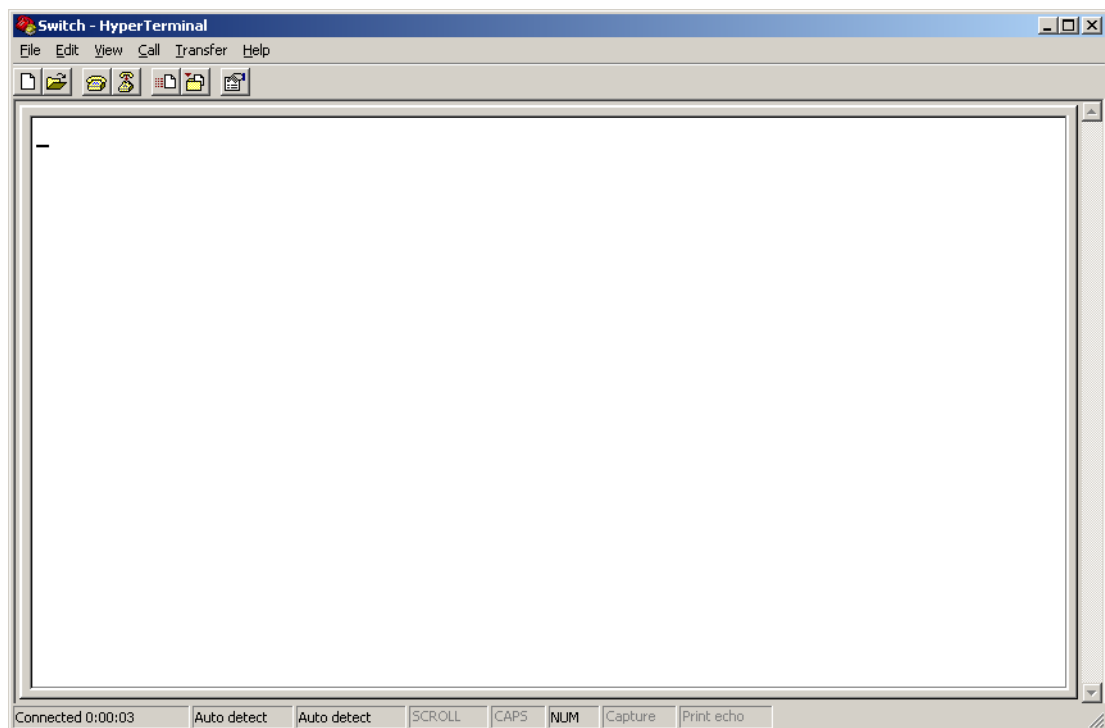
3. Set **Bits per second** to **9600**, **Data bits** to **8**, **Parity** to **None**, **Stop bits** to **1**, and **Flow control** to **None**, and click **OK**.

Figure 3 Setting the serial port parameters



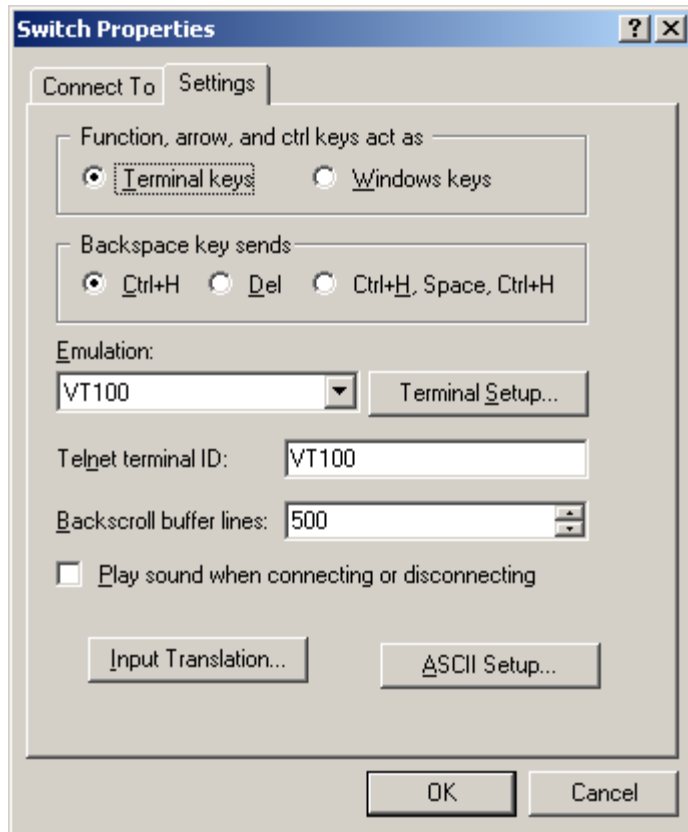
4. Select **File > Properties** in the HyperTerminal window.

Figure 4 HyperTerminal window



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

Figure 5 Setting terminal emulation in Switch Properties dialog box



Upgrading Boot ROM

To upgrade Boot ROM by using XMODEM through the console port:

1. Access the Boot menu, and enter **6** to enter the Boot ROM update menu:

1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu

Enter your choice(0-3):

! IMPORTANT:

Always select option **1** to upgrade the entire Boot ROM. You can use option **2** or option **3** only under the guidance of an HP engineer.

2. Enter **1** at the Boot ROM update menu to set the protocol parameters.

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

Enter your choice(0-3):

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

Please select your download baudrate:

- 1.* 9600

- 2. 19200
- 3. 38400
- 4. 57600
- 5. 115200
- 0. Return

Enter your choice (0-5):

4. Select an appropriate download rate. For example, enter **5** to select 115200 bps.

Download baudrate is 115200 bps

Please change the terminal's baudrate to 115200 bps and select XMODEM protocol

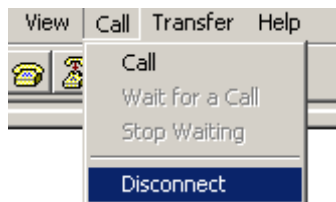
Press enter key when ready

NOTE:

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

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

Figure 6 Disconnecting the terminal from the switch

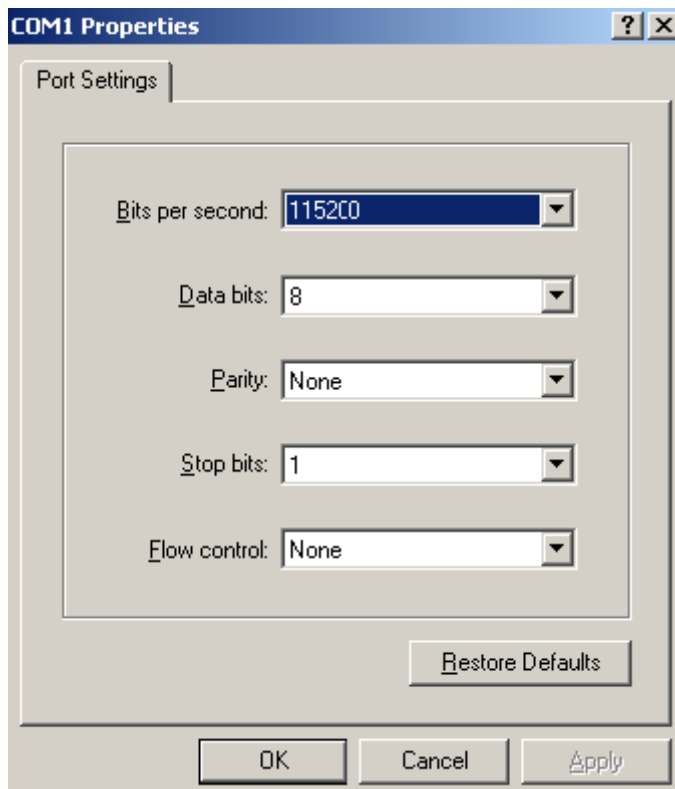


7. Select **File > Properties**. In the **Properties** dialog box, click **Configure** (see [Figure 7](#)), and then select **115200** from the **Bits per second** drop-down list box (see [Figure 8](#)).

Figure 7 Properties dialog box

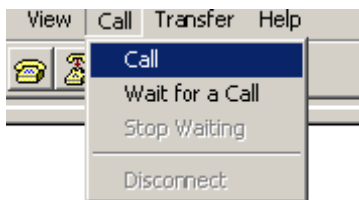


Figure 8 Modifying the baud rate



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

Figure 9 Reestablishing the connection



NOTE:

The new settings can take effect only after you reestablish the connection.

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

Now please start transfer file with XMODEM protocol.

If you want to exit, Press <Ctrl+X>.

Loading ...CCCCCCCCC

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

Figure 10 Transfer menu

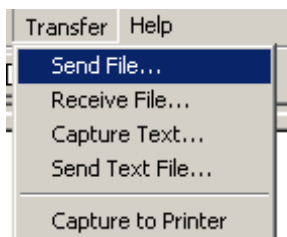
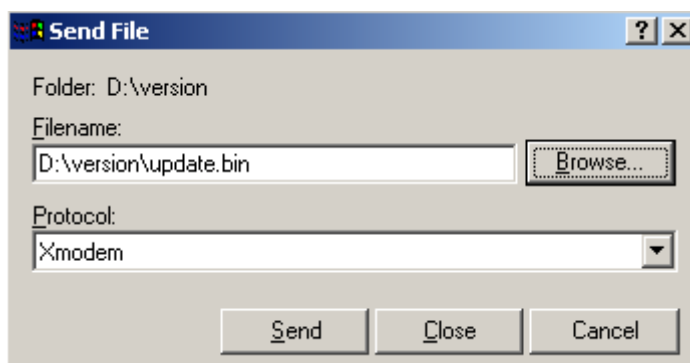
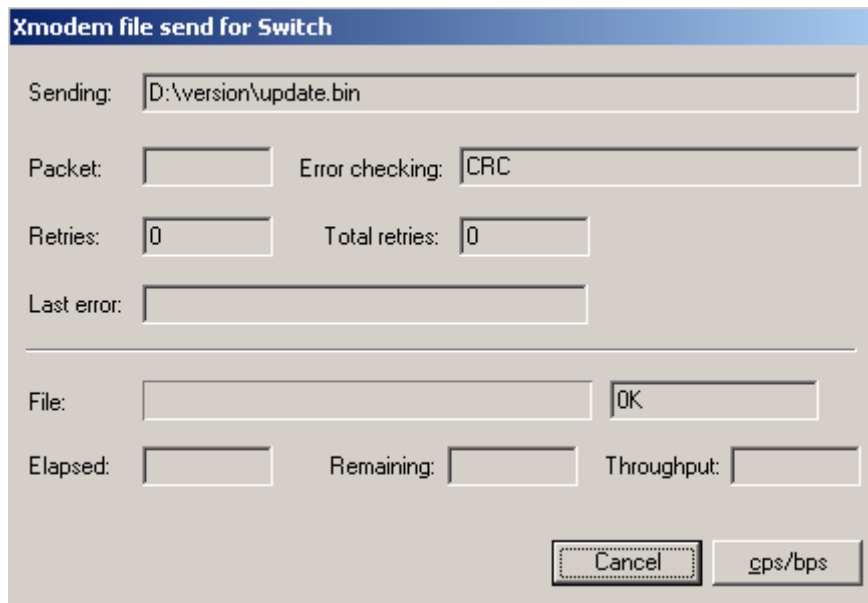


Figure 11 File transmission dialog box



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

Figure 12 Sending the software file using XMODEM



The image shows a Windows-style dialog box titled "Xmodem file send for Switch". It has a blue header bar. The main area is light gray and contains several input fields and buttons. At the top, there's a "Sending:" label followed by a text box containing "D:\version\update.bin". Below this, there are two rows of controls. The first row has a "Packet:" label with a small text box, and an "Error checking:" label with a text box containing "CRC". The second row has a "Retries:" label with a text box containing "0", and a "Total retries:" label with a text box containing "0". Below these is a "Last error:" label with a text box. A horizontal line separates the top section from the bottom section. In the bottom section, there's a "File:" label with a text box, and an "OK" button to its right. Below that, there are three labels: "Elapsed:", "Remaining:", and "Throughput:", each followed by a text box. At the bottom right, there are two buttons: "Cancel" and "cps/bps".

13. Upgrade Boot ROM on the switch.

When the terminal displays the following prompt, enter **Y** to update the basic Boot ROM segment:

```
Loading ...CCCC Done!
```

```
Will you Update Basic BootRom? (Y/N):Y
```

When the terminal displays the following prompt, enter **Y** to update the extended Boot ROM segment:

```
Updating Basic BootRom.....Done!
```

```
Updating extended BootRom? (Y/N):Y
```

When the Boot ROM upgrade is completed, the terminal displays the following information:

```
Updating extended BootRom.....Done!
```

```
Please change the terminal's baudrate to 9600 bps, press ENTER when ready.
```

14. If you are using a download rate other than 9600 bps, restore the baud rate of the serial port on the terminal to 9600 bps. If the baud rate is 9600 bps, skip this step.

15. Press any key to return to the Boot ROM update menu and enter **0**. On the Boot menu that appears, enter **0** to restart the switch so the updated image can take effect. The following is the Boot ROM update menu:

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu
Enter your choice(0-3):
```

Upgrading system software

To upgrade system software, enter **1** at the Boot menu, and the following menu appears:

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

Enter **3** to set the XMODEM parameters for downloading the software package file.

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

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

NOTE:

- The switch always attempts to boot first with the main file, and if the attempt fails for example, because the main file is not available, the switch tries to boot with the backup file. A file with the **none** attribute is just stored in Flash memory for backup and you must change its attribute to make it usable at reboot.
 - If a file with the same attribute as the file you are loading is already in the Flash memory, the attribute of the old file changes to **none** after the new file becomes valid.
 - The switch automatically updates Boot ROM when loading system software.
-

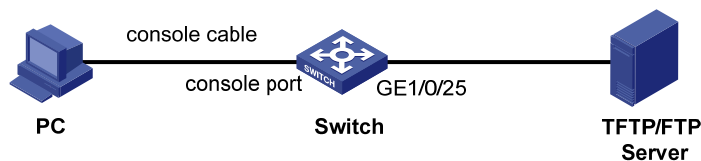
TFTP download through an Ethernet port

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

Upgrading Boot ROM

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

Figure 13 Loading software with TFTP/FTP through Ethernet port



NOTE:

- The PC and the TFTP/FTP server can be co-located.
 - The 5500 HI switches do not come with any TFTP server program, and you must install one yourself.
-

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

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu
```

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

4. Enter **1** to upgrade the entire Boot ROM and access the following protocol parameter setting menu:

```
Bootrom update menu:
```

```
1. Set TFTP protocol parameter
```

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

Enter your choice(0-3):

5. Enter 1 to set the TFTP parameters.

```
Load File Name      :update.bin
Server IP Address   :10.10.10.2
Local IP Address    :10.10.10.3
Gateway IP Address  :
```

Table 14 Description of the TFTP parameters

Item	Description
Load File Name :	Name of the file to be downloaded (for example, update.bin)
Server IP Address :	IP address of the TFTP server (for example, 10.10.10.2)
Local IP Address :	IP address of the switch (for example, 10.10.10.3)
Gateway IP Address :	IP address of the gateway (in this example, no gateway is required because the server and the switch are on the same subnet)

NOTE:

If the switch and the server are on different subnets, you must specify a gateway address for the switch.

6. Enter all required parameters.

```
Loading.....
.....
.....Done!
```

Will you Update Basic BootRom? (Y/N):Y

Enter Y at the prompt to upgrade the basic Boot ROM segment.

```
Updating Basic BootRom.....Done!
```

Updating extended BootRom? (Y/N):Y

Enter Y at the prompt to upgrade the extended Boot ROM segment.

When the upgrade is completed, the following information appears:

```
Updating extended BootRom.....Done!
```

7. Press any key to return to the Boot ROM update menu, enter 0 to return to the Boot menu, and enter 0 to restart the switch from the Boot menu so the upgraded Boot ROM can take effect.

Press enter key when ready

1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu

Enter your choice(0-3):

Upgrading system software

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

1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter

```
0. Return to boot menu
Enter your choice(0-3):3
```

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

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

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

NOTE:

- If a file with the same attribute as the file you are loading is already in the Flash memory, the attribute of the old file changes to **none** after the new file becomes valid.
 - The switch automatically updates Boot ROM when loading system software.
-

FTP download through an Ethernet port

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

Upgrading Boot ROM

NOTE:

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

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

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu
Enter your choice(0-3):
```

4. Enter **1** to upgrade the entire Boot ROM and access the following protocol parameter setting menu:

Bootrom update menu:

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

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

```
Load File Name      :update.bin
Server IP Address   :10.10.10.2
Local IP Address    :10.10.10.3
```

```

Gateway IP Address :0.0.0.0
FTP User Name      :5500
FTP User Password  :123

```

Table 15 Description of the FTP parameters

Item	Description
Load File Name :	Name of the file to be downloaded (for example, update.bin)
Server IP Address :	IP address of the FTP server (for example, 10.10.10.2)
Local IP Address :	IP address of the switch (for example, 10.10.10.3)
Gateway IP Address :	IP address of the gateway (in this example, no gateway is required because the server and the switch are on the same subnet)
FTP User Name	Username for accessing the FTP server, which must be the same as configured on the FTP server.
FTP User Password	Password for accessing the FTP server, which must be the same as configured on the FTP server.

NOTE:

If the switch and the server are on different subnets, you must specify a gateway address for the switch.

6. Enter all required parameters.

```
Will you Update Basic BootRom? (Y/N):Y
```

Enter **Y** at the prompt to upgrade the basic Boot ROM segment.

```
Updating Basic BootRom.....Done!
```

```
Updating extended BootRom? (Y/N):Y
```

Enter **Y** at the prompt to upgrade the extended Boot ROM segment.

When the upgrade is completed, the following information appears:

```
Updating extended BootRom.....Done!
```

7. Press any key to return to the Boot ROM update menu, enter 0 to return to the Boot menu, and enter 0 to restart the switch from the Boot menu so the upgraded Boot ROM can take effect.

```
Press enter key when ready
```

- ```

1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu
Enter your choice(0-3):

```

## Upgrading system software

To upgrade switch software, enter **1** in the Boot menu to access the following menu:

- ```

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

```

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

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

```
Writing flash.....
```

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

NOTE:

- If a file with the same attribute as the file you are loading is already in the Flash memory, the attribute of the old file changes to **none** after the new file becomes valid.
 - The switch automatically updates Boot ROM when loading system software.
-

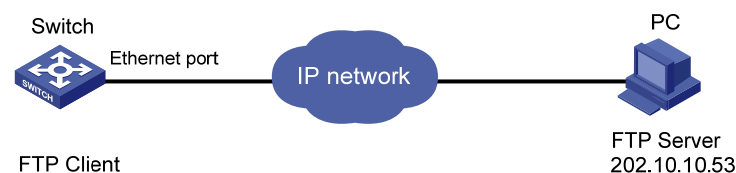
Upgrading at the CLI

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

FTP download from a server

This section uses the topology in [Figure 14](#) as an example. Run FTP server on the management PC at 202.10.10.53, create an FTP username **admin** and password, specify the source file path, telnet to the switch, and get the software package file (for example, **update.bin**) from the server.

Figure 14 FTP download from a server



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

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

2. Upgrade Boot ROM.

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

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

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

```
<HP> display boot-loader
Slot 1
The current boot app is:  flash:/update.bin
The main boot app is:    flash:/update.bin
The backup boot app is:  flash:/update.bin
<HP> reboot
```

NOTE:

- You must reboot the switch with the **reboot** command to complete the upgrade. Before that, save the configurations you have made to avoid data loss.
 - If Flash memory is insufficient, load the Boot ROM image first and delete useless files to free up Flash memory before you load the system software image.
 - Avoid power failure during the loading process.
-

TFTP download from a server

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



Hewlett Packard
Enterprise

HPE 5500HI-CMW520-R5501P36 Release Notes

Software Feature Changes

Contents

R5501P36	1
R5501P35	2
R5501P33	3
New feature: Configuring a collaboration group.....	3
Overview.....	3
Collaboration group configuration task list	4
Setting the recovery timeout time for a collaboration group	4
Adding an interface to a collaboration group	4
Displaying and maintaining collaboration group	4
Collaboration group configuration example	5
Command reference.....	6
display link-group	6
link-group	7
link-group timer	8
New feature: Configuring the action a port takes after it receives an Ethernet OAM event from the remote end.....	9
Configuring the action a port takes after it receives an Ethernet OAM event from the remote end.....	9
Command reference.....	9
oam remote-failure action.....	9
R5501P32	11
R5501P31	12
R5501P30	13
Modified feature: Including default settings in displayed running configuration	13
Feature change description	13
Command changes	13
Modified command: display current-configuration	13
Modified command: display this	13
R5501P28	15
R5501P27	16
New feature: RA guard	16
Configuring RA guard	16
About RA guard	16
Specifying the role of the attached device	16
Configuring an RA guard policy	16
Enabling the RA guard logging feature.....	17
Displaying and maintaining RA guard	18
RA guard configuration example.....	18
Command reference.....	19
display ipv6 nd raguard policy	19
display ipv6 nd raguard statistics	21
if-match acl	21
if-match autoconfig managed-address-flag.....	22
if-match autoconfig other-flag.....	23
if-match hop-limit.....	23

if-match prefix	24
if-match router-preference	25
ipv6 nd raguard apply policy	25
ipv6 nd raguard log enable	26
ipv6 nd raguard policy	27
ipv6 nd raguard role	27
reset ipv6 nd raguard statistics	28
R5501P26	29
R5501P25	30
New feature: Authorization VLAN auto-tagging for MAC authentication	30
Enabling authorization VLAN auto-tagging for MAC authentication	30
Command reference	30
mac-authentication auto-tag	30
R5501P23	32
New feature: Default settings configuration for prefixes advertised in RA messages	32
Configuring the default settings for prefixes advertised in RA messages	32
Command reference	32
ipv6 nd ra prefix default	32
Modified feature: Prefix information configuration in RA messages	33
Feature change description	33
Command changes	33
Modified command: ipv6 nd ra prefix	33
R5501P22	35
R5501P21	36
R5501P20	37
R5501P19	38
New feature: Enabling sending of ICMPv6 redirect messages	38
Enabling sending of ICMPv6 redirect messages	38
Command reference	38
New command: ipv6 redirects enable	38
New feature: Setting the router preference in RA messages	39
Setting the router preference in RA messages	39
Command reference	39
New command: ipv6 nd router-preference	39
New feature: Support for NTP configuration in IPv6 networks	40
Configuring NTP in IPv6 networks	40
Command reference	40
New command: display ntp-service ipv6 sessions	40
New command: ntp-service ipv6 access	42
New command: ntp-service ipv6 dscp	43
New command: ntp-service ipv6 in-interface disable	43
New command: ntp-service ipv6 multicast-client	44
New command: ntp-service ipv6 multicast-server	44
New command: ntp-service ipv6 source-interface	45
New command: ntp-service ipv6 unicast-peer	46
New command: ntp-service ipv6 unicast-server	46

Modified feature: Random number generator standards	47
Feature change description	47
Command changes	47
Modified feature: Enhanced CC authentication feature	47
Feature change description	47
Command changes	47
New command: display public-key local ecdsa public	47
New command: public-key local export ecdsa	48
Modified command: authentication-algorithm	49
Modified command: ciphersuite	49
Modified command: dh	49
Modified command: pfs	50
Modified command: prefer-cipher	50
Modified command: pre-shared-key	50
Modified command: public-key local create	51
Modified command: scp	51
Modified command: sftp	52
Modified command: ssh2	52
Modified feature: Disabling advertising prefix information in RA messages ..	53
Feature change description	53
Command changes	53
Modified command: ipv6 nd ra prefix	53
R5501P17	55
New feature: Disabling reactivation for edge ports shut down by BPDU guard	55
Disabling the device to reactivate edge ports shut down by BPDU guard	55
Command reference	55
New command: stp port shutdown permanent	55
New feature: Data buffer monitoring	56
Configuring data buffer monitoring	56
Command reference	56
New command: buffer usage threshold	56
New command: display buffer usage interface	57
Modified command: display packet-drop	58
New feature: Automatic PI reset	59
Enabling automatic PI reset	59
Command reference	59
poe reset enable	59
New feature: Configuring the default action of the table-miss flow entry	59
Configuring the default action of the table-miss flow entry	59
Command reference	60
New command: default table-miss permit	60
Modified feature: Configuring the OpenFlow instance mode	60
Feature change description	60
Command changes	60
Modified command: classification	60
Modified feature: Creating an OpenFlow table for an OpenFlow instance ...	61
Feature change description	61
Command changes	61
Modified command: flow-table	61

R5501P15	62
Modified feature: Storm control for known unicast packets	62
Feature change description	62
Command changes	62
Modified command: storm-constrain	62
Modified feature: Setting the maximum number of logs that can be stored in the log buffer	62
Feature change description	62
Command changes	63
Modified command: info-center logbuffer	63
Modified feature: VPN instance support for NQA server configuration.....	63
Feature change description	63
Command changes	63
Modified command: nqa server	63
R5501P13	64
New feature: Sending EAP-Success packets to 802.1X users in critical VLAN	64
Configuring the device to send EAP-Success packets to 802.1X users in critical VLAN.....	64
Command reference	65
New command: dot1x critical eapol	65
R5501P12	66
R5501P11	67
New feature: Login delay	67
Enabling the login delay	67
Command reference	67
attack-defense login reauthentication-delay.....	67
Modified feature: IPv6 address with a 127-bit prefix length	68
Feature change description	68
Command changes	68
Modified feature: Specifying log hosts.....	68
Feature change description	68
Command changes	68
Modified command: info-center loghost	68
R5501P10	69
New feature: SNMP notifications for PVST topology changes	69
Enabling SNMP notifications for PVST topology changes	69
Command reference	69
snmp trap enable stp.....	69
R5501P06	71
New feature: Disabling SSL 3.0.....	71
Disabling SSL 3.0	71
Command reference	71
ssl version ssl3.0 disable	71
New feature: 802.1X MAC address binding.....	72
Configuring 802.1X MAC address binding	72

Command reference	72
dot1x binding-mac enable	72
dot1x binding-mac	73
New feature: Web connection idle timeout	74
Setting the Web connection idle timeout	74
Command reference	74
web idle-timeout	74
New feature: Applicable scope of packet filtering on a VLAN interface	75
Configuring the applicable scope of packet filtering on a VLAN interface	75
Command reference	75
packet-filter filter	75
R5501P05	77
Modified feature: Executing interactive commands in interface range view ..	77
Feature change description	77
Command changes	77
Modified feature: Specifying RADIUS security policy servers by IP address	77
Feature change description	77
Command changes	77
Modified command: security-policy-server	77
R5501P03	79
New feature: Per-flow load sharing	79
Configuring per-flow load sharing	79
Command reference	79
ip load-sharing mode	79
New feature: Telnet/SSH user connection control	80
Configuring Telnet/SSH user connection control	80
Configuration prerequisites	80
Configuration procedure	80
Command reference	81
ssh server acl	81
ssh server ipv6 acl ipv6	82
telnet server acl	83
telnet server ipv6 acl ipv6	83
New feature: Packet rate-limiting for the table-miss flow entry	84
Packet rate-limiting for the table-miss flow entry	84
Command reference	84
display openflow flow-table	84
Modified feature: Including time zone information in the timestamp of system information sent to a log host	85
Feature change description	85
Command changes	85
Modified command: info-center timestamp loghost	85
Modified feature: Configuring physical state change suppression on an Ethernet interface	85
Feature change description	85
Command changes	86
Modified command: link-delay	86
Modified feature: Configuring a tag and description for an IPv6 static route	87
Feature change description	87

Command changes	87
Modified command: ipv6 route-static	87
R5501P02	88
New feature: 802.1X voice VLAN	88
Configuring an 802.1X voice VLAN	88
Configuration guidelines	88
Configuration prerequisites	89
Configuration procedure	89
Command reference	89
New command: dot1x voice vlan	89
New feature: Configuring the uplink port to permit multiple isolate-user-VLANs	90
Configuring the uplink port to permit multiple isolate-user-VLANs	90
Overview	90
Configuration procedure	91
Configuration example	92
Command reference	95
port isolate-user-vlan trunk promiscuous	95
New feature: TCP fragment attack protection	98
Enabling TCP fragment attack protection	98
Command reference	98
attack-defense tcp fragment enable	98
New feature: Support for BPDU guard configuration in interface or port group view	99
Configuring BPDU guard for an interface or port group	99
Enabling BPDU guard for an interface or port group when BPDU guard is globally disabled	99
Disabling BPDU guard for an interface or port group when BPDU guard is globally enabled	99
Command reference	100
New command: stp port bpdu-protection	100
New feature: MAC re-authentication timer for users in guest VLAN	101
Configuring MAC re-authentication timer for users in guest VLAN	101
Command reference	102
mac-authentication timer guest-vlan-reauth	102
New feature: Specifying the IPv4/IPv6 VRRP version	103
Specifying the IPv4/IPv6 VRRP version	103
Command reference	103
vrrp version	103
New feature: MAC and port uniqueness check by the DHCP snooping device	104
Enabling MAC and port uniqueness check on the DHCP snooping device	104
Command reference	104
dhcp-snooping check mac-port	104
Modified feature: Auto status transition of dynamic secure MAC addresses	105
Feature change description	105
Command changes	105
Modified feature: The maximum number of gateways supported in MFF automatic mode	105
Feature change description	105

Command changes	105
Modified feature: Username request timeout timer for 802.1X authentication	
.....	106
Feature change description	106
Command changes	106
Modified command: dot1x timer	106
R5501P01	107
New feature: Discarding IPv6 packets that contain extension headers	107
Enabling a device to discard IPv6 packets that contain extension headers	107
Command reference	107
New command: ipv6 option drop enable	107
Modified feature: Configuring IGMP SSM mappings	108
Feature change description	108
Command changes	108
Modified feature: Configuring MLD SSM mappings	108
Feature change description	108
Command changes	109
R5501	110
New feature: OpenFlow	110
Overview	110
Basic concepts	111
OpenFlow instance	113
Protocols and standards	114
OpenFlow configuration task list	114
Configuring OpenFlow instances	115
Creating an OpenFlow instance	115
Associating an OpenFlow instance with VLANs	115
Configuring flow table IDs	115
Setting the connection mode for an OpenFlow instance to establish connections to controllers	116
Configuring the maximum number of flow entries	116
Configuring in-band management VLANs	117
Disabling MAC address learning in the VLANs associated with an OpenFlow instance	117
Configuring the datapath ID for an OpenFlow instance	118
Activating or reactivating an OpenFlow instance	118
Configuring controllers for an OpenFlow switch	118
Configuring controllers and main connections	118
Setting the connection interruption mode	119
Setting OpenFlow timers	119
Configuring OpenFlow to support dynamic MAC addresses	120
Displaying and maintaining OpenFlow	120
OpenFlow configuration example	120
Network requirements	120
Configuration procedure	121
Verifying the configuration	121
OpenFlow commands	122
active instance	122
classification vlan	122
controller address	123
controller connect interval	124
controller echo-request interval	124
controller mode	125
datapath-id	126
description	126
display openflow controller	127

display openflow flow-table	128
display openflow group	132
display openflow instance	134
display openflow meter	135
display openflow summary	137
fail-open mode	138
flow-entry max-limit	139
flow-table	139
in-band management vlan	140
mac-ip dynamic-mac aware	140
mac-learning forbidden	141
openflow instance	141
Modified feature: Setting the device name	142
Feature change description	142
Command changes	142
Modified command: sysname	142
Modified feature: Specifying multiple public keys for an SSH user	142
Feature change description	142
Command changes	143
Modified command: ssh user	143
Modified feature: Disabling an untrusted port from recording clients' IP-to-MAC bindings	144
Feature change description	144
Command changes	144
Modified command: dhcp-snooping trust	144
New command: dhcp-snooping no-user-binding	144
Modified feature: ARP packet rate limit	145
Feature change description	145
Command changes	145
Modified command: arp rate-limit	145
Modified feature: Specifying the username and password to log in to the SCP server	145
Feature change description	145
Command changes	145
Modified command: SCP	145
Modified feature: Customizing DHCP options	146
Feature change description	146
Command changes	146
Modified command: option	146
Modified feature: ACL-based packet filtering on a VLAN interface	147
Feature change description	147
Command changes	147
Modified command: packet-filter	147
R5206	149
New feature: Configuring the ARP detection logging function	149
Configuring the ARP detection logging function	149
Command reference	149
arp detection log enable	149
New feature: 802.1X-based dynamic IPv4 source guard binding entries	150
Overview	150
Configuration procedure	150

Configuration task list	150
Enabling the 802.1X IP freezing function	150
Enabling a port to generate 802.1X-based dynamic IPv4 source guard binding entries	151
Command reference	151
dot1x user-ip freeze	151
ip verify source dot1x	152
New feature: SSL server policy association with the FTP service	152
Configuration procedure	152
Command reference	153
ftp server ssl-server-policy	153
New feature: Enabling MAC authentication multi-VLAN mode	153
Overview	153
Configuration procedure	154
Command reference	154
mac-authentication host-mode multi-vlan	154
Modified feature: Specifying multiple secondary HWTACACS servers	155
Feature change description	155
Command changes	155
Modified command: key (HWTACACS scheme view)	155
Modified command: primary accounting	155
Modified command: primary authentication	156
Modified command: primary authorization	156
Modified command: secondary accounting	157
Modified command: secondary authentication	158
Modified command: secondary authorization	158
Modified feature: Displaying brief interface information	159
Feature change description	159
Command changes	159
Modified command: display interface	159
Modified feature: Displaying brief IP configuration for Layer 3 interfaces ..	160
Feature change description	160
Command changes	160
Modified command: display ip interface brief	160
Modified feature: Configuring static multicast MAC address entries	161
Feature change description	161
Command changes	161
Modified command: mac-address multicast	161
Modified command: display mac-address multicast	161
R5205L01	163
New feature: Multicast ND	163
Configuring multicast ND	163
Command reference	163
New feature: Configuring packet capture	164
Configuring the packet capture function	164
Displaying and maintaining packet capture	165
Packet capture configuration example	165
Packet capture configuration commands	166
display packet capture buffer	166
display packet capture status	167
packet capture	168
packet capture buffer save	170
packet capture schedule	170
packet capture start	171

packet capture stop	172
reset packet capture buffer	173
Modified feature: Configuring system information for the SNMP agent	173
Feature change description	173
Command changes	173
Modified command: snmp-agent sys-info	173
R5203P01	174
R5203	175
Modified feature: Enabling/disabling FIPS mode	175
Feature change description	175
Command changes	175
Modified feature: Setting the maximum number of the IPv4/IPv6 source guard binding entries on a port	175
Feature change description	175
Command changes	176
Modified command: ip verify source max-entries	176
Modified command: ipv6 verify source max-entries	176
Modified feature: Setting the IRF link down report delay	176
Feature change description	176
Command changes	176
Modified command: irf link-delay	176
Modified feature: Setting the minimum password length	177
Feature change description	177
Command changes	177
Modified command: password-control length	177
Modified feature: Switching the user privilege level	177
Feature change description	177
Command changes	177
Modified command: super	177
Modified feature: Upgrading a subordinate member	178
Feature change description	178
Command changes	178
Modified command: issu load	178
Modified feature: Implementing ACL-based IPsec	178
Feature change description	178
IKE-based IPsec tunnel for IPv4 packets configuration example	178
IKE configuration example	180
Command changes	183
Modified feature: Cluster management	183
Deleted feature: Disabling Boot ROM access	183
Feature change description	183
Command changes	184
Modified command: undo startup bootrom-access enable	184
E5201	185
New feature: Configuring a user validity check rule	186
Configuring a user validity check rule	186
Command reference	186

arp detection	186
New feature: Enabling source IP conflict prompt	187
Enabling source IP conflict prompt.....	187
Command reference.....	188
arp ip-conflict prompt.....	188
New feature: Supporting IPv6 routes with a prefix length over 64.....	188
New feature: BGP MDT	188
Configuring BGP MDT	188
Configuration prerequisites.....	189
Configuring BGP MDT peers or peer groups	189
Configuring a BGP MDT route reflector	190
Displaying and maintaining BGP MDT	191
Command reference.....	191
display bgp mdt group	191
display bgp mdt peer.....	193
display bgp mdt routing-table	196
ipv4-family mdt	198
peer enable (BGP-MDT sub-address family view)	198
peer group (BGP-MDT sub-address family view).....	199
peer reflect-client (BGP-MDT sub-address family view)	199
reflect between-clients (BGP-MDT sub-address family view)	200
reflector cluster-id (BGP-MDT sub-address family view)	201
reset bgp mdt	201
New feature: Configuring the maximum number of selected ports allowed for an aggregation group	202
Configuring the maximum number of selected ports allowed for an aggregation group.....	202
Configuration guidelines	202
Configuration procedure	202
Command reference.....	203
link-aggregation selected-port maximum	203
New feature: Enabling MAC address migration log notifying	204
Enabling MAC address migration log notifying.....	204
Command reference.....	204
mac-flapping notification enable	204
New feature: Disabling MAC entry aging timer refresh based on destination MAC address	205
Disabling MAC entry aging timer refresh based on destination MAC address.....	205
Application example	205
Command reference.....	206
mac-address destination-hit disable	206
New feature: PoE power negotiation through Power Via MDI TLV (supported only on PoE-capable switches)	207
Configuring PoE power negotiation through Power Via MDI TLV	207
Command reference.....	207
Modified command: display lldp local-information	207
Modified command: display lldp neighbor-information.....	208
New feature: Specifying a destination server in a VPN for UDP helper.....	209
Specifying a destination server in a VPN for UDP helper	209
Command reference.....	209
Modified command: udp-helper server	209

New feature: Supporting using a self-signed certificate for HTTPS.....	210
New feature: Setting the maximum number of 802.1X authentication attempts for MAC authentication users.....	210
Setting the maximum number of 802.1X authentication attempts for MAC authentication users	210
Command reference.....	210
dot1x attempts max-fail.....	210
New feature: Support of 802.1X for issuing VLAN groups	211
Support of 802.1X for issuing VLAN groups	211
Configuring a VLAN group.....	211
Command reference.....	212
vlan-group	212
vlan-list	212
New feature: Setting the deletion delay time for SAVI.....	213
Setting the deletion delay time for SAVI	213
Command reference.....	213
ipv6 savi down-delay.....	213
New feature: Setting a DSCP value for an ISP domain.....	214
Setting a DSCP value for an ISP domain	214
Command reference.....	215
dscp (ISP domain view)	215
New feature: Advanced packet filtering logging.....	215
Configuring advanced packet filtering logging	216
Command reference.....	216
acl flow logging interval.....	216
acl ipv6 flow logging interval	217
New feature: PoE	217
Overview.....	217
PoE configuration task list.....	218
Configuration guidelines	218
Enabling PoE for a PoE interface	219
Enabling the PSE to detect nonstandard PDs	220
Configuring the maximum PoE interface power	220
Configuring PoE interface power management.....	220
Configuring the PoE monitoring function	221
Configuring PSE power monitoring.....	221
Monitoring PD.....	222
Configuring PoE interface through PoE profile.....	222
Configuring PoE profile.....	222
Applying a PoE profile	222
Upgrading PSE processing software in service.....	223
Displaying and maintaining PoE	223
PoE configuration example	224
Troubleshooting PoE	225
Setting the priority of a PoE interface to critical fails	225
Failure to apply a PoE profile to a PoE interface.....	225
Failure to configure an AC input under-voltage threshold	226
PoE configuration commands	226
apply poe-profile	226
apply poe-profile interface	226
display poe device	227
display poe interface	228
display poe interface power	231
display poe pse.....	232
display poe pse interface	234

display poe pse interface power	235
display poe-profile	236
display poe-profile interface	238
poe enable.....	239
poe legacy enable	239
poe max-power	240
poe pd-description	241
poe pd-policy priority.....	241
poe priority.....	242
poe update.....	243
poe utilization-threshold.....	243
poe-profile	244
New feature: Supporting automatically creating RSA key pairs or SSH	245
Feature change description.....	245
Command changes	245
Modified feature: SCP server name.....	245
Feature change description.....	245
Command changes	245
Modified command: scp.....	245
Modified feature: Configuring portal-free rules to support TCP/UDP port numbers.....	245
Feature change description.....	245
Command changes	246
Modified command: portal free-rule	246
Modified feature: Setting the time to wait for a DAD NS from a DHCPv6 client	246
Feature change description.....	246
Command reference.....	246
Modified command: ipv6 savi dad-preparedelay.....	246
Modified feature: Support of voice VLAN for 128 OUI addresses	247
Feature change description.....	247
Command changes	247
Modified command: voice vlan mac-address	247
Modified feature: Configuring CDP compatibility.....	247
Feature change description.....	247
Command changes	248
Modified command: display lldp neighbor-information.....	248
Modified feature: ping ipv6	249
Feature change description.....	249
Command changes	249
Modified command: ping ipv6.....	249
Modified feature: Configuring the maximum number of operations that an NQA client can simultaneously perform	249
Feature change description.....	249
Command reference.....	250
Modified command: nqa agent max-concurrent.....	250
Modified feature: Configuring parameters for an sFlow collector.....	250
Feature change description.....	250
Command reference.....	250
Modified command: sflow collector.....	250

Modified feature: Configuring load-sharing criteria for a link aggregation group	250
Feature change description	250
Command changes	251
Modified command: link-aggregation load-sharing mode	251
Modified feature: Implementing ACL-based IPsec	252
Feature change description	252
IKE-based IPsec tunnel for IPv4 packets configuration example	252
IKE configuration example	254
Command changes	257
Modified feature: Setting the IRF link down report delay	257
Feature change description	257
Command changes	257
Modified command: irf link-delay	257
Modified feature: Configuring the ABR to advertise a default route to the stub area	257
Feature change description	257
Command changes	257
Modified command: stub	257
R5105	259
New feature: Disabling password recovery capacity	259
Disabling password recovery capacity	259
Command reference	259
password-recovery enable	259
New feature: Configuring a port to forward 802.1X EAPOL packets untagged	260
Configuring a port to forward 802.1X EAPOL packets untagged	260
Command reference	260
dot1x eapol untag	260
New feature: Configuring preferred tunnels in a tunneling policy	261
Configuring preferred tunnels in a tunneling policy	261
Command reference	262
preferred-path	262
Modified feature: Configuring NDP globally and for specific ports	263
Feature change description	263
Command changes	263
Modified command: ndp enable	263
Modified feature: Configuring NTDP globally and for specific ports	263
Feature change description	263
Command changes	263
Modified command: ntdp enable	263
Modified feature: Configuring the cluster function	264
Feature change description	264
Command changes	264
Modified command: cluster enable	264
Modified feature: Default configuration	264
Feature change description	264
Command changes	264

F5103	265
New feature: Delaying the MAC authentication	265
Configuring the MAC authentication delay	266
Command reference	266
mac-authentication timer auth-delay	266
New feature: Specifying the source interface for DNS packets	266
Specifying the source interface for DNS packets	266
Command reference	267
dns source-interface	267
New feature: Configuring DHCPv6 snooping to support Option 18 and Option 37	268
Configuring DHCPv6 snooping to support Option 18 and Option 37	268
Command reference	269
ipv6 dhcp snooping option interface-id enable	269
ipv6 dhcp snooping option interface-id string	269
ipv6 dhcp snooping option remote-id enable	270
ipv6 dhcp snooping option remote-id string	271
New feature: Setting the subnet mask length to be 31	272
Setting the subnet mask length to be 31	272
Command reference	272
Modified command: ip address	272
New feature: Setting the DSCP value for multiple types of protocol packets	272
Setting the DSCP value for BGP protocol packets	272
Setting the DSCP value for DHCPv6 protocol packets	273
Setting the DSCP value for DHCP protocol packets	273
Setting the DSCP value for DNS protocol packets	273
Setting the DSCP value for FTP and TFTP protocol packets	274
Setting the DSCP value for HTTP protocol packets	274
Setting the DSCP value for IGMP protocol packets sent by IGMP snooping	275
Setting the DSCP value for IGMP protocol packets	275
Setting the DSCP value for IPv6 BGP protocol packets	275
Setting the DSCP value for IPv6 DNS protocol packets	275
Setting the DSCP value for IPv6 PIM protocol packets	276
Setting the DSCP value for MLD protocol packets sent by MLD snooping	276
Setting the DSCP value for MLD protocol packets	276
Setting the ToS value for packets sent by the TCP listening service on the NQA server	276
Setting the ToS value for packets sent by the UDP listening service on the NQA server	277
Setting the ToS value for NQA probe packets	277
Setting the DSCP value for NTP protocol packets	277
Setting the DSCP value for OSPF protocol packets	277
Setting the DSCP value for PIM protocol packets	278
Setting the DSCP value for RADIUS protocol packets	278
Setting the DSCP value for RIP protocol packets	278
Setting the DSCP value for SNMP trap packets	279
Setting the DSCP value for SNMP response packets	279
Setting the DSCP value for SSH protocol packets	279
Setting the DSCP value for Telnet protocol packets	280
Setting the DSCP value for VRRP protocol packets	280
Setting the DSCP value for the protocol packets sent to the log host	280
Setting the DSCP value for outgoing LDP packets	281
Setting the DSCP value for outgoing RSVP packets	281
New commands	281
dhcp client dscp	281
dhcp dscp	282

dns dscp	282
dns ipv6 dscp	283
dscp (IGMP view)	283
dscp (IGMP-Snooping view)	284
dscp (IPv6 PIM view)	284
dscp (MLD view)	285
dscp (MLD-Snooping view)	285
dscp (MPLS LDP view)	286
dscp (OSPF view)	286
dscp (PIM view)	287
dscp (RIP view)	288
ftp client dscp	288
ftp client ipv6 dscp	289
ftp server dscp	289
ip http dscp	290
ipv6 dhcp client dscp	290
ipv6 dhcp dscp	291
ipv6 http dscp	291
mpls rsvp-te dscp	292
nqa server tcp-connect tos	292
nqa server udp-echo tos	293
ntp-service dscp	293
peer dscp (BGP/BGP-VPN instance view)	294
peer dscp (IPv6 address family view)	294
radius dscp	295
radius ipv6 dscp	295
sftp client dscp	296
sftp client ipv6 dscp	296
snmp-agent packet response dscp	297
ssh client dscp	297
ssh client ipv6 dscp	298
ssh server dscp	298
ssh server ipv6 dscp	299
telnet client dscp	299
telnet client ipv6 dscp	300
telnet server dscp	300
telnet server ipv6 dscp	301
tftp client dscp	301
tftp client ipv6 dscp	302
tos (DHCP operation type view)	302
vrrp dscp	303
vrrp ipv6 dscp	303
Modified commands	304
Modified command: info-center loghost	304
Modified command: ping ipv6	304
Modified command: snmp-agent target-host	305
Modified command: tracert	305
Modified command: tracert ipv6	305

New feature: Automatic configuration file backup for software downgrading

.....	306
-------	-----

Configuring automatic configuration file backup for software downgrading	306
Command reference	306

New feature: Configuring LLDP to advertise a specific voice VLAN 306

Configuration guidelines	307
Configuration procedure	307
Dynamically advertising server-assigned VLANs through LLDP	307
Command reference	308
lldp voice-vlan	308

New feature: Enabling LLDP to automatically discover IP phones.....	308
Overview.....	308
Configuration procedure	309
Command reference	309
voice vlan track lldp	309
New feature: MVRP	310
Overview.....	310
MRP	310
MVRP registration modes	312
Protocols and standards	313
MVRP configuration task list.....	313
Configuration prerequisites	313
Enabling MVRP	313
Configuration restrictions and guidelines	313
Configuration procedure	314
Configuring the MVRP registration mode	314
Configuring MRP timers	315
Enabling GVRP compatibility	316
Displaying and maintaining MVRP	316
Configuration example for MVRP in normal registration mode	316
Network requirements	316
Configuration procedure	317
Command reference	325
display mvrp running-status	325
display mvrp state	326
display mvrp statistics	328
display mvrp vlan-operation	330
mrp timer join	331
mrp timer leave	331
mrp timer leaveall	332
mrp timer periodic.....	333
mvrp global enable	334
mvrp enable	334
mvrp gvrp-compliance	335
mvrp registration	335
reset mvrp statistics	336
New feature: Portal authentication in IPv6 networks.....	337
Configuring portal authentication for an IPv6 network	337
Specifying an IPv6 portal server for portal authentication	337
Configuring an IPv6 portal-free rule	337
Specifying a source IPv6 subnet for portal authentication.....	337
Specifying an authentication domain for IPv6 portal users	338
Specifying a source IPv6 address for outgoing IPv6 portal packets	338
Logging off an IPv6 portal user.....	338
IPv6 portal authentication commands	339
portal auth-network ipv6.....	339
portal delete-user ipv6	339
portal domain ipv6	340
portal free-rule ipv6.....	340
portal nas-ip ipv6.....	341
portal server ipv6.....	342
New feature: SCP	343
Overview.....	343
Configuring the switch as an SCP server	343
Configuring the switch as the SCP client.....	343
SCP client configuration example	344
SCP server configuration example.....	345
Command reference	346

scp	346
ssh user	347
New feature: FIPS	349
Overview	349
FIPS self-tests	349
Power-up self-test	349
Conditional self-tests	349
Triggering a self-test	349
Configuring FIPS	349
Enabling the FIPS mode	350
Triggering a self-test	350
Displaying and maintaining FIPS	351
FIPS configuration example	351
Command reference	352
fips mode enable	352
display fips status	353
fips self-test	353
New feature: Configuring ACL-based IPsec	354
Configuring ACL-based IPsec	354
ACL-based IPsec configuration task list	354
Configuring ACLs	354
Configuring an IPsec proposal	357
Configuring an IPsec policy	358
Applying an IPsec policy group to an interface	362
Configuring the IPsec session idle timeout	362
Enabling ACL checking of de-encapsulated IPsec packets	363
Configuring the IPsec anti-replay function	363
Configuring packet information pre-extraction	364
Displaying and maintaining IPsec	364
IKE-based IPsec tunnel for IPv4 packets configuration example	365
Command reference	367
Modified command: ah authentication-algorithm	367
New command: connection-name	368
Modified command: display ipsec sa	369
New command: display ipsec session	369
Modified command: esp authentication-algorithm	371
Modified command: esp encryption-algorithm	371
New command: ike-peer (IPsec policy view)	372
New command: ipsec anti-replay check	373
New command: ipsec anti-replay window	373
New command: ipsec decrypt check	374
New command: ipsec policy (interface view)	374
Modified command: ipsec policy (system view)	375
Modified command: ipsec proposal	376
New command: ipsec sa global-duration	376
New command: ipsec session idle-time	377
New command: pfs	377
New command: policy enable	378
Modified command: proposal (IPsec policy view)	379
New command: qos pre-classify	379
Modified command: reset ipsec sa	380
New command: reset ipsec session	381
New command: sa duration	381
Modified command: sa string-key	382
New command: security acl	383
Modified command: transform	384
New command: tunnel local	384
New command: tunnel remote	385

New feature: IKE	386
IKE overview.....	386
IKE security mechanism	386
IKE operation	386
IKE functions.....	387
Relationship between IKE and IPsec	388
Protocols and standards	388
IKE configuration task list.....	388
Configuring a name for the local security gateway.....	389
Configuring an IKE proposal.....	389
Configuring an IKE peer	390
Setting keepalive timers	392
Setting the NAT keepalive timer	392
Configuring a DPD detector.....	392
Disabling next payload field checking	393
Displaying and maintaining IKE.....	393
IKE configuration example	394
Troubleshooting IKE	397
Invalid user ID	397
Proposal mismatch	397
Failing to establish an IPsec tunnel	398
ACL configuration error.....	398
Command reference.....	398
authentication-algorithm.....	398
authentication-method	399
certificate domain	400
dh	400
display ike dpd.....	401
display ike peer.....	402
display ike proposal	403
display ike sa.....	404
dpd.....	407
encryption-algorithm	408
exchange-mode	408
id-type.....	409
ike dpd	410
ike local-name	411
ike next-payload check disabled	411
ike peer (system view).....	412
ike proposal	412
ike sa keepalive-timer interval	413
ike sa keepalive-timer timeout	414
ike sa nat-keepalive-timer interval	414
interval-time	415
local-address.....	415
local-name	416
nat traversal	417
peer.....	417
pre-shared-key	418
proposal (IKE peer view).....	418
remote-address.....	419
remote-name.....	420
reset ike sa	421
sa duration.....	422
time-out.....	422
New feature: Configuring the log file overwrite-protection function	423
Configuring the log file overwrite-protection function	423
Command reference.....	423
info-center logfile overwrite-protection.....	423

New feature: Verifying the correctness and integrity of the file.....	424
Verifying the correctness and integrity of the file	424
Command reference	424
crypto-digest	424
New feature: Displaying per-port queue-based traffic statistics.....	425
Displaying per-port queue-based traffic statistics	425
Command reference	425
display qos queue-statistics	425
Modified feature: Configuring MAC authentication timers	426
Feature change description	426
Command changes	426
Modified command: mac-authentication timer	426
Modified feature: NTP	426
Feature change description	426
Command changes	427
Modified command: ntp-service broadcast-server	427
Modified command: ntp-service multicast-server	427
Modified command: ntp-service unicast-peer	427
Modified command: ntp-service unicast-server	427
Modified feature: Configuring a password for the local user	428
Feature change description	428
Command changes	428
Modified command: password (local user view)	428
Modified feature: 802.1X critical VLAN	428
Feature change description	428
Command changes	429
Modified feature: MAC authentication critical VLAN	429
Feature change description	429
Command changes	429
Modified feature: Modifying CLI configuration commands executed in FIPS mode for CC evaluation	429
Feature change description	429
Modified command: super password	429
Modified feature: Modifying login management commands executed in FIPS mode for CC evaluation	430
Feature change description	430
Command changes	430
Modified command: authentication-mode	430
Modified command: protocol inbound	431
Modified command: set authentication password	432
Modified Feature: Modifying software upgrade commands executed in FIPS mode for CC evaluation	433
Feature change description	433
Command changes	433
Modified Feature: Modifying configuration file management commands executed in FIPS mode for CC evaluation	433
Feature change description	433
Command changes	433

Modified Feature: Modifying security commands executed in FIPS mode for CC evaluation	433
Feature change description	433
Command changes	434
Modified command: key (HWTACACS scheme view)	434
Modified command: key (RADIUS scheme view).....	434
Modified command: password.....	434
Modified command: primary accounting (RADIUS scheme view)	435
Modified command: primary authentication (RADIUS scheme view)	435
Modified command: secondary accounting (RADIUS scheme view)	436
Modified command: secondary authentication (RADIUS scheme view)	436
Modified command: password-control composition	436
Modified command: password-control length.....	437
Modified command: password-control super composition.....	437
Modified command: password-control super length.....	438
Modified command: public-key local create	438
Modified command: scp	438
Modified command: ssh user	439
Modified command: ssh2	440
Modified command: sftp.....	441
Modified command: ciphersuite	442
Modified command: prefer-cipher.....	443
Modified command: certificate request mode.....	444
Modified feature: Modifying SNMP commands executed in FIPS mode for CC evaluation	444
Feature change description	444
Command changes	444
Modified command: display snmp-agent community	444
Modified command: snmp-agent community.....	445
Modified command: snmp-agent group	445
Modified command: snmp-agent usm-user { v1 v2c }.....	445
Modified command: snmp-agent calculate-password	445
Modified command: snmp-agent sys-info.....	446
Modified command: snmp-agent target-host.....	446
Modified command: snmp-agent usm-user v3.....	447
Modified feature: Clearing all users from the password control blacklist ...	447
Feature change description	447
Command changes	448
Modified feature: Setting the interval for saving system information to the log file	448
Feature change description	448
Command changes	448
Modified command: info-center logfile frequency.....	448
F5102	449
Modified feature: Password configuration and display	449
Feature change description	449
Command changes	449
Modified command: area-authentication-mode.....	449
Modified command: bims-server	450
Modified command: certificate request mode.....	450
Modified command: cluster-local-user	451
Modified command: cluster-snmp-agent usm-user v3.....	451
Modified command: cwmp acs password.....	452
Modified command: cwmp cpe password.....	453

Modified command: dldp authentication-mode	453
Modified command: domain-authentication-mode	453
Modified command: ftp-server	454
Modified command: isis authentication-mode	455
Modified command: key (HWTACACS scheme view)	455
Modified command: key (RADIUS scheme view)	456
Modified command: mac-authentication user-name-format	456
Modified command: md5-password	457
Modified command: mpls rsvp-te authentication	457
Modified command: ntp-service authentication-keyid	458
Modified command: ospf authentication-mode	458
Modified command: password (FTP operation type view)	459
Modified command: password (local user view)	459
Modified command: password (RADIUS-server user view)	460
Modified command: peer password (IPv6 address family view)	460
Modified command: peer password (MSDP view)	461
Modified command: portal server	461
Modified command: primary accounting (RADIUS scheme view)	462
Modified command: primary authentication (RADIUS scheme view)	462
Modified command: radius-server client-ip	463
Modified command: rip authentication-mode	464
Modified command: sa authentication-hex	464
Modified command: sa encryption-hex	465
Modified command: sa string-key	465
Modified command: secondary accounting (RADIUS scheme view)	466
Modified command: secondary authentication (RADIUS scheme view)	467
Modified command: set authentication password	467
Modified command: sham-link	468
Modified command: snmp-agent usm-user v3	469
Modified command: super password	470
Modified command: vlink-peer	471
Modified command: vrrp ipv6 vrid authentication-mode	471
Modified command: vrrp vrid authentication-mode	472
Modified feature: Task ID for IPv6 socket display	473
Feature change description	473
Command changes	473
Modified command: display ipv6 socket	473
Removed feature: Local user password display	473
Feature change description	473
Removed commands	473
local-user password-display-mode	473
R5101P01	474
R5101	475
E5101	476

R5501P36

This release has no feature changes.

R5501P35

This release has no feature changes.

R5501P33

This release has the following changes:

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

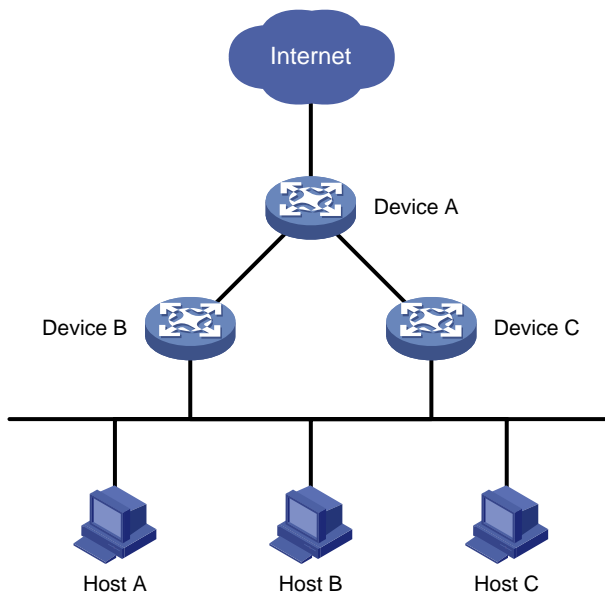
New feature: Configuring a collaboration group

Overview

You can add ports on a device to one group called "collaboration group." All ports in the group have consistent state. They are either able or unable to forward packets at the same time. Collaboration group is mainly used to trigger the downlink port state based on the uplink port state, and implement fast link switchover.

As shown in [Figure 1](#), LAN users Host A, Host B and Host C access the Internet through Device B. When the interface on Device B connecting Device A goes down, the traffic switches from Device B to the standby device Device C because dynamic routing is enabled in the network. However, because the link connecting Device B and the LAN is still up, the time required for dynamic route update is long and the traffic switchover is slow, which greatly affect the LAN users' access to the Internet.

Figure 1 Network diagram



After you assign Device B's ports connecting Device A and the LAN to a collaboration group, the following happens:

- When the physical state of any port in the collaboration group is down, the other ports in the collaboration group are set to the linkgroup-down state, and cannot exchange traffic with the peers. The collaboration group is in down state.
- When the port that was physically down goes up, the system tries to bring up the other ports in the collaboration group. If they go up within the recovery timeout time (10 seconds by default),

the collaboration group goes up; if any port fails to go up within the recovery timeout time, all the other ports are set to the linkgroup-down state. The collaboration group is in down state.

Collaboration group configuration task list

Tasks at a glance
(Optional.) Setting the recovery timeout time for a collaboration group
(Required.) Adding an interface to a collaboration group

Setting the recovery timeout time for a collaboration group

Set the recovery timeout time according to the actual device and networking conditions. A too short recovery timeout time might cause collaboration group flapping because member ports might fail to come up within the timeout time.

To set the recovery timeout time for a collaboration group:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the recovery timeout time for a collaboration group.	link-group <i>link-group-number</i> timer <i>seconds</i>	The default setting is 10 seconds.

Adding an interface to a collaboration group

An interface can belong to only one collaboration group.

When a device is connected to another device through multiple ports, do not assign these ports to the same collaboration group. Otherwise, when one port goes down, its peer port on the remote device may be set to the linkgroup-down state. In that case, all the ports may fail to be brought up.

The state of subinterfaces is associated with the state of the main interface. To ensure collaboration group performance, do not add the main interface and its subinterfaces to the same collaboration group.

To ensure correct collaboration group operation, do not add an aggregate interface and its member ports to the same collaboration group.

To add an interface to a collaboration group:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type interface-number</i>	N/A
3. Add the interface to the specified collaboration group.	link-group <i>link-group-number</i>	By default, an interface does not belong to any collaboration group. Repeat this command to add multiple interfaces to a collaboration group.

Displaying and maintaining collaboration group

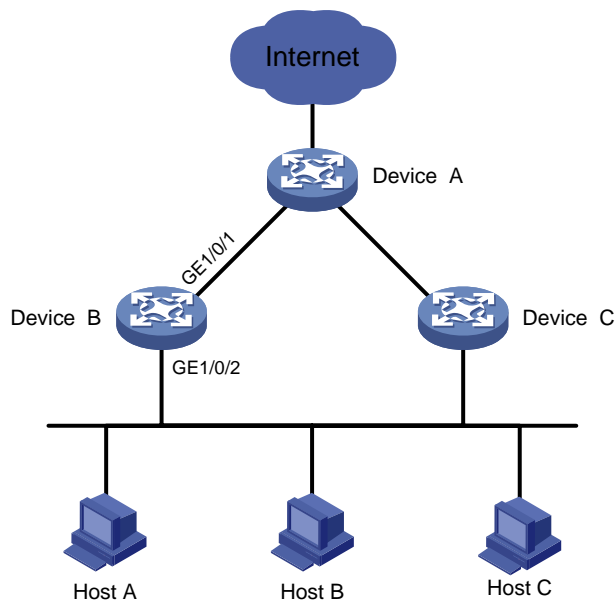
Task	Command	Remarks
Display the collaboration group information	display link-group [number <i>link-group-number</i> brief] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.

Collaboration group configuration example

Network requirements

As shown in Figure 2, LAN users Host A, Host B, and Host C access the Internet through Device B. Device C serves as a backup for Device B. Configure Device B so that when the link connecting Device A and Device B goes down, the traffic rapidly switches from Device B to Device C.

Figure 2 Network diagram



Configuration procedure

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 on Device B to collaboration group 1.

```

[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] link-group 1
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] link-group 1
[DeviceB-GigabitEthernet1/0/2] quit

```

Verifying the configuration

Unplug the cable connecting Device A to GigabitEthernet 1/0/1 on Device B, and check the status of collaboration group 1 and its member ports. The status of GigabitEthernet 1/0/1 is down, and that of GigabitEthernet 1/0/2 is linkgroup-down.

```

[DeviceB] display link-group
Group Number: 1    Group Status: Down
Interface Information:

```

Interface Name	Interface Status
GigabitEthernet1/0/1	Down
GigabitEthernet1/0/2	Linkgroup-down

Command reference

display link-group

Use **display link-group** to display collaboration group information.

Syntax

display link-group [**number** *link-group-number* | **brief**] [| { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

number *link-group-number*: Specifies a collaboration group by its number in the range of 1 to 24. If this option is not specified, the command displays information about all collaboration groups.

brief: Displays brief information about all collaboration groups. If this keyword is not specified, the command displays detailed collaboration group information.

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

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

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

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

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

Examples

Display detailed information about all collaboration groups.

```
<Sysname> display link-group
Group Number: 1    Group Status: Up
Interface Information:
Interface Name      Interface Status
GigabitEthernet1/0/1    Up
GigabitEthernet1/0/2    Up
Group Number: 2    Group Status: Up
Interface Information:
Interface Name      Interface Status
GigabitEthernet1/0/3    Up
GigabitEthernet1/0/4    Up
```

Display detailed information about collaboration group 1.

```
<Sysname> display link-group number 1
Link-Group Information(Supports up to 8 interfaces):
Group Number: 1    Group Status: Up
Interface Information:
```

Interface Name	Interface Status
GigabitEthernet1/0/1	Up
GigabitEthernet1/0/2	Up

Display brief information about all collaboration groups.

```
<Sysname> display link-group brief
```

Group Number	Group Status
1	Up
2	Up

Table 1 Command output

Field	Description
Group Number	Collaboration group number.
Group Status	Collaboration group state: <ul style="list-style-type: none"> • Initial—The collaboration group has no interface. • Up—All interfaces in the collaboration group are up. • Down—At least one interface in the collaboration group is down, and other interfaces are in linkgroup-down state. • Ambiguous—The collaboration group state is unclear and is determined after ten seconds.
Interface Name	Name of interface belonging to this collaboration group.
Interface Status	Interface state: <ul style="list-style-type: none"> • Up—The physical state of the interface is up. • Down—The physical state of an interface is down. • Linkgroup-down—The interface is shut down by the collaboration group and cannot exchange packets with its peer.

link-group

Use **link-group** to add an interface to a collaboration group.

Use **undo link-group** to remove an interface from a collaboration group.

Syntax

link-group *link-group-number*

undo link-group *link-group-number*

Default

An interface does not belong to any collaboration group.

Views

Interface view

Default command level

2: System level

Parameters

link-group-number: Specifies a collaboration group number in the range of 1 to 24.

Usage guidelines

An interface can belong to only one collaboration group.

When a device is connected to another device through multiple ports, do not assign these ports to the same collaboration group. If you assign the ports to the same collaboration group, when one port goes down, its peer port on the remote device might be set to the linkgroup-down state. In that case, all the ports might fail to be brought up.

The state of subinterfaces is associated with the state of the main interface. To ensure collaboration group performance, do not add the main interface and its subinterfaces to the same collaboration group.

To ensure correct collaboration group operation, do not add an aggregate interface and its member ports to the same collaboration group.

Examples

Add GigabitEthernet 1/0/1 to collaboration group 1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] link-group 1
```

link-group timer

Use **link-group timer** to set the recovery timeout time for a collaboration group.

Use **undo link-group timer** to restore the default.

Syntax

link-group *link-group-number* **timer** *seconds*

undo link-group *link-group-number* **timer**

Default

The recovery timeout time for a collaboration group is 10 seconds.

Views

System view

Default command level

2: System level

Parameters

link-group-number: Specifies a collaboration group by its number in the range of 1 to 24.

seconds: Specifies the recovery timeout time in the range of 1 to 20 seconds.

Usage guidelines

Set the recovery timeout time according to the actual device and networking conditions. A too short recovery timeout time might cause collaboration group flapping because member ports might fail to come up within the timeout time.

Examples

Set the recovery timeout time to 5 seconds for collaboration group 1.

```
<Sysname> system-view
[Sysname] link-group 1 timer 5
```

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

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

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

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

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

Command reference

oam remote-failure action

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

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

Syntax

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

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

Default

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

Views

Layer 2 Ethernet port view

Layer 3 Ethernet port view

Default command level

2: System level

Parameters

connection-expired: Specifies a connection timeout fault.

critical-event: Specifies a critical fault.

dying-gasp: Specifies a fatal fault.

link-fault: Specifies a link fault.

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

Examples

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

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] oam remote-failure critical-event action error-link-down
```

R5501P32

This release has no feature changes.

R5501P31

This release has no feature changes.

R5501P30

This release has the following changes:

- **Modified feature: Including default settings in displayed running configuration**

Modified feature: Including default settings in displayed running configuration

Feature change description

This software version added the support for displaying parameters that use the default settings when displaying the running configuration.

Command changes

Modified command: display current-configuration

Old syntax

```
display current-configuration [ [ configuration [ configuration ] | interface [ interface-type [ interface-number ] ] | exclude modules ] [ [ by-linenum ] [ [ { begin | exclude | include } regular-expression ] ] ]
```

New syntax

```
display current-configuration [ [ [ configuration [ configuration ] | interface [ interface-type [ interface-number ] ] ] [ all ] | exclude modules ] [ [ by-linenum ] [ [ { begin | exclude | include } regular-expression ] ] ]
```

Views

Any view

Change description

Before modification: This command cannot display parameters that use the default settings.

After modification: The **all** keyword was added to this command. If you specify this keyword, the command displays settings for all parameters in the running configuration, including parameters that use the default settings.

Modified command: display this

Old syntax

```
display this [ by-linenum ] [ [ { begin | exclude | include } regular-expression ] ]
```

New syntax

```
display this [ all ] [ [ by-linenum ] [ [ { begin | exclude | include } regular-expression ] ] ]
```

Views

Any view

Change description

Before modification: This command cannot display parameters that use the default settings in the current view.

After modification: The **all** keyword was added to this command. If you specify this keyword, the command displays settings for all parameters in the running configuration in the current view, including parameters that use the default settings.

R5501P28

This release has no feature changes.

R5501P27

This release has the following changes:

- **New feature: RA guard**

New feature: RA guard

Configuring RA guard

About RA guard

RA guard allows Layer 2 access devices to analyze and block unwanted and forged RA messages.

Upon receiving an RA message, the device makes the forwarding or dropping decision based on the role of the attached device or the RA guard policy.

1. If the role of the device attached to the port is **router**, the device forwards all RA messages received on the port. If the role is **host**, the device directly drops all RA messages received on the port.
2. If no role is set for the port, the device uses the RA guard policy to match the information found in the RA message.
 - If the RA message content matches every criterion in the policy, the device forwards the message.
 - If the RA message content is not validated, the device drops the message.

Specifying the role of the attached device

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet or aggregate interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Specify the role of the device attached to the port.	ipv6 nd raguard role { host router }	Required. By default, the role of the device attached to the port is not specified. Make sure your setting is consistent with the device type.

Configuring an RA guard policy

Configure an RA guard policy if you do not specify a role for the attached device or if you want to filter the RA messages sent by a router.

To configure an RA guard policy:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create an RA guard policy and enter its view.	ipv6 nd raguard policy	Required.

Step	Command	Remarks
	<i>policy-name</i>	By default, no RA guard policies exist. If the policy does not contain match criteria, the policy will not take effect and the device drops all received RA messages.
3. Specify an ACL match criterion.	if-match acl <i>ipv6-acl-number</i>	Optional. By default, no ACL match criterion exists.
4. Specify a prefix match criterion.	if-match prefix acl <i>ipv6-acl-number</i>	Optional. By default, no prefix match criterion exists.
5. Specify a router preference match criterion.	if-match router-preference maximum { high low medium }	Optional. By default, no router preference match criterion exists.
6. Specify an M flag match criterion.	if-match autoconfig managed-address-flag { off on }	Optional. By default, no M flag match criterion exists.
7. Specify an O flag match criterion.	if-match autoconfig other-flag { off on }	Optional. By default, no O flag match criterion exists.
8. Specify a maximum or minimum hop limit match criterion.	if-match hop-limit { maximum minimum } <i>limit</i>	Optional. By default, no hop limit match criterion exists.
9. Quit RA guard policy view.	quit	N/A
10. Enter VLAN view.	vlan <i>vlan-number</i>	N/A
11. Apply an RA guard policy to the VLAN.	ipv6 nd raguard apply policy [<i>policy-name</i>]	Required. By default, no RA guard policy is applied to the VLAN.

Enabling the RA guard logging feature

This feature allows a device to generate logs when it detects forged RA messages. Each log records the following information:

- Name of the interface that received the forged RA message.
- Source IP address of the forged RA message.
- Number of RA messages dropped on the interface.

The RA guard logging feature sends the log messages to the information center. The information center can then output log messages from different source modules to different destinations. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

To enable the RA guard logging feature:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the RA guard logging feature.	ipv6 nd raguard log enable	Required. By default, the RA guard logging

	feature is disabled.
--	----------------------

Displaying and maintaining RA guard

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display the RA guard policy configuration.	display ipv6 nd raguard policy [<i>policy-name</i>]
Display RA guard statistics.	display ipv6 nd raguard statistics [interface <i>interface-type interface-number</i>]
Clear RA guard statistics.	reset ipv6 nd raguard statistics [interface <i>interface-type interface-number</i>]

RA guard configuration example

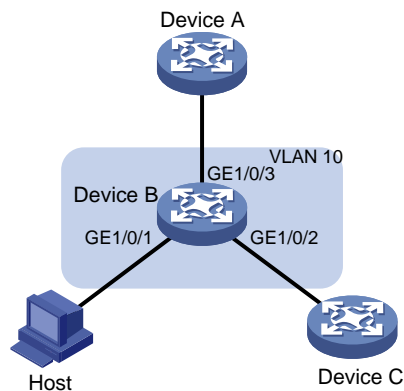
Network requirements

As shown in [Figure 2](#), GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 of Device B are in VLAN 10.

Configure RA guard on Device B to filter forged and unwanted RA messages.

- Configure an RA policy in VLAN 10 for GigabitEthernet 1/0/2 to filter all RA messages received from the unknown device.
- Specify **host** as the role of the host. All RA messages received on GigabitEthernet 1/0/1 are dropped.
- Specify **router** as the role of the Device A. All RA messages received on GigabitEthernet 1/0/3 are forwarded.

Figure 3 Network diagram



Configuration procedure

Create an RA guard policy named **policy1**.

```
<DeviceB> system-view
```

```
[DeviceB] ipv6 nd raguard policy policy1
```

Set the maximum router preference to **high** for the RA guard policy.

```
[DeviceB-raguard-policy-policy1] if-match router-preference maximum high
```

Specify **on** as the M flag match criterion for the RA guard policy.

```
[DeviceB-raguard-policy-policy1] if-match autoconfig managed-address-flag on
```

```

# Specify on as the O flag match criterion for the RA guard policy.
[DeviceB-raguard-policy-policy1] if-match autoconfig other-flag on

# Set the maximum advertised hop limit to 120 for the RA guard policy.
[DeviceB-raguard-policy-policy1] if-match hop-limit maximum 120

# Set the minimum advertised hop limit to 100 for the RA guard policy.
[DeviceB-raguard-policy-policy1] if-match hop-limit minimum 100
[DeviceB-raguard-policy-policy1] quit

# Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to VLAN 10.
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type access
[DeviceB-GigabitEthernet1/0/1] port access vlan 10
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type access
[DeviceB-GigabitEthernet1/0/2] port access vlan 10
[DeviceB-GigabitEthernet1/0/2] quit

# Configure GigabitEthernet 1/0/3 to trunk VLAN 10.
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 10
[DeviceB-GigabitEthernet1/0/3] quit

# Apply the RA guard policy policy1 to VLAN 10.
[DeviceB] vlan 10
[DeviceB-vlan10] ipv6 nd raguard apply policy policy1
[DeviceB-vlan10] quit

# Specify host as the role of the device attached to GigabitEthernet 1/0/1.
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ipv6 nd raguard role host
[DeviceB-GigabitEthernet1/0/1] quit

# Specify router as the role of the device attached to GigabitEthernet 1/0/3.
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] ipv6 nd raguard role router
[DeviceB-GigabitEthernet1/0/3] quit

```

Verifying the configuration

```

# Verify that the device forwards or drops RA messages received on GigabitEthernet 1/0/2 based on
the RA guard policy. (Details not shown.)

# Verify that the device drops RA messages received on GigabitEthernet 1/0/1. (Details not shown.)

# Verify that the device forwards RA messages received on GigabitEthernet 1/0/3 to other ports in
VLAN 10. (Details not shown.)

```

Command reference

display ipv6 nd raguard policy

Syntax

```
display ipv6 nd raguard policy [ policy-name ]
```

Views

Any view

Default command level

1: Monitor level

Parameters

policy-name: Specifies an RA guard policy by its name. The policy name is a case-sensitive string of 1 to 31 characters. If you do not specify a policy, this command displays the configuration of all RA guard policies.

Description

Use **display ipv6 nd raguard policy** to display the RA guard policy configuration.

Related command: **ipv6 nd raguard policy**.

Examples

Display the configuration of all RA guard policies.

```
<Sysname> display ipv6 nd raguard policy
Total number of policies: 2
RA Guard policy: policy1
  if-match ACL 2001
  if-match autoconfig managed-address-flag on
  if-match autoconfig other-flag off
  if-match hop-limit maximum 128
  if-match hop-limit minimum 100
  if-match prefix ACL name aa
  if-match router-preference medium
  applied to VLAN 1-3 7
RA Guard policy: policy2
  if-match ACL name zdd
  if-match prefix ACL 2200
```

Table 2 Command output

Field	Description
RA Guard policy	Name of the RA guard policy.
if-match ACL	Number of the ACL in the ACL match criterion.
if-match ACL name	Name of the ACL in ACL match criterion.
if-match autoconfig managed-address-flag	Match criterion of the advertised M flag: <ul style="list-style-type: none">on—The value of the advertised M flag is 1.off—The value of the advertised M flag is 0.
if-match autoconfig other-flag	Match criterion of the advertised O flag: <ul style="list-style-type: none">on—The value of the advertised O flag is 1.off—The value of the advertised O flag is 0.
if-match hop-limit maximum	The maximum advertised hop limit match criterion.
if-match hop-limit minimum	The minimum advertised hop limit match criterion.
if-match prefix ACL	Number of the ACL used to identify the prefix match criterion.
if-match prefix ACL name	Name of the ACL used to identify the prefix match criterion.
applied to VLAN	ID of the VLAN to which the RA guard policy is applied.

display ipv6 nd raguard statistics

Syntax

display ipv6 nd raguard statistics [**interface** *interface-type interface-number*]

Views

Any view

Default command level

1: Monitor level

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays RA guard statistics for all interfaces.

Description

Use **display ipv6 nd raguard statistics** to display RA guard statistics.

Related command: **reset ipv6 nd raguard statistics**.

Examples

Display RA guard statistics.

```
<Sysname> display ipv6 nd raguard statistics
```

RA messages dropped by RA guard:

Interface	Dropped
-----------	---------

GE1/0/1	78
---------	----

GE1/0/2	0
---------	---

GE1/0/3	32
---------	----

GE1/0/4	0
---------	---

Table 3 Command output

Field	Description
Interface	Interface that received the dropped RA messages.
Dropped	Number of RA messages dropped on the interface.

if-match acl

Syntax

if-match acl *ipv6-acl-number*

undo if-match acl

Views

RA guard policy view

Default command level

2: System level

Parameters

ipv6-acl-number: Specifies an IPv6 basic ACL by its number in the range of 2000 to 2999.

Description

Use **if-match acl** to specify an ACL match criterion.

Use **undo if-match acl** to delete the ACL match criterion.

By default, no ACL match criterion exists.

RA guard uses the ACL match criterion to match the IP address of the RA message sender. If the sender IP address matches a permit rule, the message passes the check.

If the specified ACL does not exist or does not contain a rule, the ACL match criterion does not take effect.

Examples

Use IPv6 basic ACL 2001 as the ACL match criterion for the RA guard policy **policy1**.

```
<Sysname> system-view
[Sysname] ipv6 nd rguard policy policy1
[Sysname-rguard-policy-policy1] if-match acl 2001
```

if-match autoconfig managed-address-flag

Syntax

if-match autoconfig managed-address-flag { off | on }

undo if-match autoconfig managed-address-flag

Views

RA guard policy view

Default command level

2: System level

Parameters

off: Specifies the advertised M flag as 0

on: Specifies the advertised M flag as 1.

Description

Use **if-match autoconfig managed-address-flag** to specify an M flag match criterion.

Use **undo if-match autoconfig managed-address-flag** to delete the M flag match criterion.

By default, no M flag match criterion exists.

The M flag in an RA message determines whether a receiving host uses stateful autoconfiguration to obtain an IPv6 address.

- If the M flag is set to 1, the host uses stateful autoconfiguration, for example, uses a DHCPv6 server.
- If the M flag is set to 0, the host uses stateless autoconfiguration. In stateless autoconfiguration, the host generates an IPv6 address according to its link-layer address and the prefix information in the RA message.

Examples

Specify **on** as the M flag match criterion for the RA guard policy **policy1**.

```
<Sysname> system-view
[Sysname] ipv6 nd rguard policy policy1
[Sysname-rguard-policy-policy1] if-match autoconfig managed-address-flag on
```

if-match autoconfig other-flag

Syntax

```
if-match autoconfig other-flag { off | on }  
undo if-match autoconfig other-flag
```

Views

RA guard policy view

Default command level

2: System level

Parameters

off: Specifies the advertised O flag as 0.

on: Specifies the advertised O flag as 1.

Description

Use **if-match autoconfig other-flag** to specify an O flag match criterion.

Use **undo if-match autoconfig other-flag** to delete the O flag match criterion.

By default, no O flag match criterion exists.

The O flag in an RA message determines whether a receiving host uses stateful autoconfiguration to obtain configuration information other than IPv6 address.

- If the O flag is set to 1, the host uses stateful autoconfiguration, for example, uses a DHCPv6 server.
- If the O flag is set to 0, the host uses stateless autoconfiguration.

Examples

```
# Specify on as the M flag match criterion for the RA guard policy policy1.  
<Sysname> system-view  
[Sysname] ipv6 nd rguard policy policy1  
[Sysname-rguard-policy-policy1] if-match autoconfig other-flag on
```

if-match hop-limit

Syntax

```
if-match hop-limit { maximum | minimum } limit  
undo if-match hop-limit { maximum | minimum }
```

Views

RA guard policy view

Default command level

2: System level

Parameters

maximum: Specifies the maximum advertised hop limit. An RA message passes the check if its current hop limit is not higher than the maximum advertised hop limit.

minimum: Specifies the minimum advertised hop limit. An RA message passes the check if its current hop limit is not less than the minimum advertised hop limit.

limit: Specifies the advertised hop limit in the range of 1 to 255.

Description

Use **if-match hop-limit** to specify a maximum or minimum hop limit match criterion.

Use **undo if-match hop-limit** to delete the maximum or minimum hop limit match criterion.

By default, no maximum or minimum hop limit match criterion exists.

If a hop limit match criterion is set, and the RA message's current hop limit is 0, the message will be dropped.

Examples

Set the maximum hop limit match criterion to 128 for the RA guard policy **policy1**.

```
<Sysname> system-view
[Sysname] ipv6 nd rguard policy policy1
[Sysname-rguard-policy-policy1] if-match hop-limit maximum 128
```

if-match prefix

Syntax

if-match prefix acl *ipv6-acl-number*

undo if-match prefix acl

Views

RA guard policy view

Default command level

2: System level

Parameters

ipv6-acl-number: Specifies an IPv6 basic ACL by its number in the range of 2000 to 2999.

Description

Use **if-match prefix** to specify a prefix match criterion.

Use **undo if-match prefix** to delete the prefix match criterion.

By default, no prefix match criterion exists.

An RA message passes the check if the advertised prefixes in the message match the prefixes set by the ACL.

If the specified ACL does not exist or does not contain a rule, the prefix match criterion does not take effect.

Examples

Use IPv6 basic ACL 2000 as the prefix match criterion for the RA guard policy **policy1**.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2000
[Sysname-acl-ipv6-basic-2000] rule permit source 1001:: 64
[Sysname-acl-ipv6-basic-2000] rule permit source 3124:1123:: 64
[Sysname-acl-ipv6-basic-2000] rule deny source any
[Sysname-acl-ipv6-basic-2000] quit
[Sysname] ipv6 nd rguard policy policy1
[Sysname-rguard-policy-policy1] if-match prefix acl 2000
```

if-match router-preference

Syntax

```
if-match router-preference maximum { high | low | medium }  
undo if-match router-preference maximum
```

Views

RA guard policy view

Default command level

2: System level

Parameters

high: Sets the maximum router preference to **high**. An RA message passes the check if its router preference is not higher than **high**.

low: Sets the maximum router preference to **low**. An RA message passes the check if its router preference is not higher than **low**.

medium: Sets the maximum router preference to **medium**. An RA message passes the check if its router preference is not higher than **medium**.

Description

Use **if-match router-preference maximum** to specify a router preference match criterion.

Use **undo if-match router-preference maximum** to delete the router preference match criterion.

By default, no router preference match criterion exists.

A host selects a router as the default gateway according to the router preference in received RA messages. If router preferences are the same, the host selects the default router from which the first RA message is received.

An RA message will not pass the router preference check if the message does not have a preference value. This RA message will be dropped.

Examples

Specify **medium** as the router preference match criterion for the RA guard policy **policy1**.

```
<Sysname> system-view
```

```
[Sysname] ipv6 nd rguard policy policy1
```

```
[Sysname-rguard-policy-policy1] if-match router-preference maximum medium
```

ipv6 nd rguard apply policy

Syntax

```
ipv6 nd rguard apply policy [ policy-name ]  
undo ipv6 nd rguard apply policy
```

Views

VLAN view

Default command level

2: System level

Parameters

policy-name: Specifies an RA guard policy by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a policy, RA guard blocks RA messages on all ports in the VLAN except ports that are defined to be connected to routers.

Description

Use **ipv6 nd raguard apply policy** to apply an RA guard policy to a VLAN.

Use **undo ipv6 nd raguard apply policy** to remove the RA guard policy from a VLAN.

By default, no RA guard policy is applied to a VLAN.

If an RA message has multiple VLAN tags, RA guard uses the outermost VLAN tag to select the applied RA guard policy.

If the specified RA guard policy does not exist, the command does not take effect.

Related command: **ipv6 nd raguard policy**.

Examples

Apply the RA guard policy **policy1** to VLAN 100.

```
<Sysname> system-view
```

```
[Sysname] vlan 100
```

```
[Sysname-vlan100] ipv6 nd raguard apply policy policy1
```

ipv6 nd raguard log enable

Syntax

ipv6 nd raguard log enable

undo ipv6 nd raguard log enable

Views

System view

Default command level

2: System level

Description

Use **ipv6 nd raguard log enable** to enable the RA guard logging feature.

Use **undo ipv6 nd raguard log enable** to disable the RA guard logging feature.

By default, the RA guard logging feature is disabled.

This command allows a device to generate logs when it detects forged RA messages. Each log records the following information:

- Name of the interface that received the forged RA message.
- Source IP address of the forged RA message.
- Number of RA messages dropped on the interface.

The RA guard logging feature sends the log messages to the information center. The information center can then output log messages from different source modules to different destinations. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

Related commands: **display ipv6 nd raguard statistics** and **reset ipv6 nd raguard statistics**.

Examples

Enable the RA guard logging feature.

```
<Sysname> system-view
[Sysname] ipv6 nd raguard log enable
```

ipv6 nd raguard policy

Syntax

```
ipv6 nd raguard policy policy-name
undo ipv6 nd raguard policy policy-name
```

Views

System view

Default command level

2: System level

Parameters

policy-name: Assigns a name to the RA guard policy. The name is a case-sensitive string of 1 to 31 characters.

Description

Use **ipv6 nd raguard policy** to create an RA guard policy and enter its view, or enter the view of an existing RA guard policy.

Use **undo ipv6 nd raguard policy** to delete an RA guard policy.

By default, no RA guard policies exist.

Related commands: **display ipv6 nd raguard policy** and **ipv6 nd raguard apply policy**.

Examples

Create RA guard policy **policy1** and enter its view.

```
<Sysname> system-view
[Sysname] ipv6 nd raguard policy policy1
[Sysname-raguard-policy-policy1]
```

ipv6 nd raguard role

Syntax

```
ipv6 nd raguard role { host | router }
undo ipv6 nd raguard role
```

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Default command level

2: System level

Parameters

host: Specifies the host role. The port attached to a host drops all received RA messages.

router: Specifies the router role. The port attached to a router forwards all received RA messages.

Description

Use **ipv6 nd raguard role** to specify the role of the device attached to the port.

Use **undo ipv6 nd raguard role** to remove the role of the device attached to the port.

By default, no role is specified for the device attached to the port.

Make sure your setting is consistent with the device type. If you are not aware of the attached device type, do not specify a role for the device.

Examples

Specify **host** as the role for the device attached to GigabitEthernet 1/0/1.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 nd raguard role host
```

reset ipv6 nd raguard statistics

Syntax

reset ipv6 nd raguard statistics [**interface** *interface-type interface-number*]

Views

User view

Default command level

2: System level

Parameters

interface *interface-type interface-number*. Specifies an interface by its type and number. If you do not specify an interface, this command clears RA guard statistics for all interfaces.

Description

Use **reset ipv6 nd raguard statistics** to clear RA guard statistics.

Related command: **display ipv6 nd raguard statistics**.

Examples

Clear RA guard statistics.

```
<Sysname> reset ipv6 nd raguard statistics
```

R5501P26

This release has no feature changes.

R5501P25

This release has the following changes:

- [New feature: Authorization VLAN auto-tagging for MAC authentication](#)

New feature: Authorization VLAN auto-tagging for MAC authentication

Enabling authorization VLAN auto-tagging for MAC authentication

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

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

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

To enable authorization VLAN auto-tagging for MAC authentication:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable authorization VLAN auto-tagging for MAC authentication.	mac-authentication auto-tag [ignore-config]	By default, authorization VLAN auto-tagging for MAC authentication is disabled. If you do not specify the ignore-config keyword, this command does not take effect if the authorization VLAN is specified by the port hybrid vlan command.

Command reference

mac-authentication auto-tag

Syntax

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

undo mac-authentication auto-tag

Views

Ethernet interface view

Default command level

2: System level

Parameters

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

Usage guidelines

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

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

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

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

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

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

Examples

Enable authorization VLAN auto-tagging for MAC authentication.

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

R5501P23

This release has the following changes:

- **New feature:** Default settings configuration for prefixes advertised in RA messages
- **Modified feature:** Prefix information configuration in RA messages

New feature: Default settings configuration for prefixes advertised in RA messages

Configuring the default settings for prefixes advertised in RA messages

This feature allows you to configure the default settings for the prefix specified by using the **ipv6 nd ra prefix** command. If none of the parameters (*valid-lifetime*, *preferred-lifetime*, and **no-advertise**) is configured in the **ipv6 nd ra prefix** command, the prefix uses the default settings.

To configure the default settings for prefixes advertised in RA messages:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the default settings for prefixes advertised in RA messages.	ipv6 nd ra prefix default [<i>valid-lifetime</i> <i>preferred-lifetime</i> [no-autoconfig off-link] * no-advertise]	By default, no default settings are configured for prefixes advertised in RA messages.

Command reference

ipv6 nd ra prefix default

Syntax

```
ipv6 nd ra prefix default [ valid-lifetime preferred-lifetime [ no-autoconfig | off-link ] * | no-advertise ]
```

```
undo ipv6 nd ra prefix default
```

Views

Interface view

Default command level

2: System level

Parameters

valid-lifetime: Specifies the valid lifetime of a prefix, in the range of 0 to 4294967295 seconds. The default value is 2592000 seconds (30 days).

preferred-lifetime: Specifies the preferred lifetime of a prefix used for stateless autoconfiguration, in the range of 0 to 4294967295 seconds. The preferred lifetime cannot be longer than the valid lifetime. The default value is 604800 seconds (7 days).

no-autoconfig: Specifies a prefix not to be used for stateless autoconfiguration. If you do not specify this keyword, the prefix is used for stateless autoconfiguration.

off-link: Indicates that the address with the prefix is not directly reachable on the link. If you do not specify this keyword, the address with the prefix is directly reachable on the link.

no-advertise: Disables the device from advertising the prefix specified in this command. If you do not specify this keyword, the device advertises the prefix specified in this command.

Usage guidelines

Use **ipv6 nd ra prefix default** to configure the default settings for prefixes advertised in RA messages.

Use **undo ipv6 nd ra prefix default** to restore the default.

By default, no default settings are configured for prefixes advertised in RA messages.

This command configures the default settings for the prefix specified by using the **ipv6 nd ra prefix** command. If none of the parameters (*valid-lifetime*, *preferred-lifetime*, and **no-advertise**) is configured in the **ipv6 nd ra prefix** command, the prefix uses the default settings.

Examples

Configure the default settings for prefixes advertised in RA messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra prefix default 100 10
```

Modified feature: Prefix information configuration in RA messages

Feature change description

The *valid-lifetime*, *preferred-lifetime*, and **no-advertise** parameters in the **ipv6 nd ra prefix** command were changed from required to optional.

Command changes

Modified command: ipv6 nd ra prefix

Old syntax

```
ipv6 nd ra prefix { ipv6-prefix prefix-length | ipv6-prefix/prefix-length } { valid-lifetime
preferred-lifetime [ no-autoconfig | off-link ] * | no-advertise }
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: When using the **ipv6 nd ra prefix** command to configure the prefix information, you must configure the parameters for the prefix. The parameters include *valid-lifetime*, *preferred-lifetime*, and **no-autoconfig**.

After modification: If you do not configure a parameter for the prefix, the prefix uses the default settings configured by using the **ipv6 nd ra prefix default** command.

R5501P22

This release has no feature changes.

R5501P21

This release has no feature changes.

R5501P20

This release has no feature changes.

R5501P19

This release has the following changes:

- New feature: Enabling sending of ICMPv6 redirect messages
- New feature: Setting the router preference in RA messages
- New feature: Support for NTP configuration in IPv6 networks
- Modified feature: Random number generator standards
- Modified feature: Enhanced CC authentication feature
- Modified feature: Disabling advertising prefix information in RA messages

New feature: Enabling sending of ICMPv6 redirect messages

Enabling sending of ICMPv6 redirect messages

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

To enable sending of ICMPv6 redirect messages:

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

Command reference

New command: ipv6 redirects enable

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

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

Syntax

ipv6 redirects enable

undo ipv6 redirects

Default

Sending of ICMPv6 redirect packets is disabled.

Views

System view

Default command level

System level

Examples

```
# Enable sending of ICMPv6 redirect packets.  
<Sysname> system-view  
[Sysname] ipv6 redirects enable
```

New feature: Setting the router preference in RA messages

Setting the router preference in RA messages

A host selects a router as the default gateway according to the router preference. If router preferences are the same, the host selects the router from which the first RA message is received.

To set the router preference in RA messages:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the router preference in RA messages.	ipv6 nd router-preference { high low medium }	By default, the router preference is medium.

Command reference

New command: ipv6 nd router-preference

Syntax

```
ipv6 nd router-preference { high | low | medium }  
undo ipv6 nd router-preference
```

View

Interface view

Default level

2: System level

Parameters

high: Sets the router preference to highest.

low: Sets the router preference to lowest.

medium: Sets the router preference to medium.

Description

Use **ipv6 nd router-preference** to set a router preference in RA messages.

Use **undo ipv6 nd router-preference** to restore the default.

By default, the router preference is medium.

Examples

```
# Set the router preference in RA messages to highest on VLAN-interface 100.  
<Sysname> system-view  
[Sysname] interface vlan-interface 100
```

```
[Sysname-Vlan-interface100] ipv6 nd router-preference high
```

New feature: Support for NTP configuration in IPv6 networks

Configuring NTP in IPv6 networks

You can configure NTP in IPv6 networks.

Command reference

New command: display ntp-service ipv6 sessions

Syntax

```
display ntp-service ipv6 sessions [ verbose ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

verbose: Displays detailed information about all IPv6 NTP sessions. If you do not specify this keyword, the command only displays brief information about the IPv6 NTP sessions.

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

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

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

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

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

Description

Use **display ntp-service ipv6 sessions** to display information about all IPv6 NTP sessions.

Examples

```
# Display brief information about all IPv6 NTP sessions.
```

```
<Sysname> display ntp-service ipv6 sessions
```

```
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
```

```
Source: [125]3000::32
```

```
Reference: 127.127.1.0
```

```
Reachabilities: 1
```

```
Last receive time: 6
```

```
Roundtrip delay: 0.0
```

```
Clock stratum: 2
```

```
Poll interval: 64
```

```
Offset: -0.0
```

```
Dispersion: 0.0
```

```
Total sessions: 1
```

Table 4 Command output

Field	Description
[12345]	<ul style="list-style-type: none"> 1—Clock source selected by the system (the current reference source). It has a system clock stratum level less than or equal to 15. 2—The stratum level of the clock source is less than or equal to 15. 3—The clock source has survived the clock selection algorithm. 4—The clock source is a candidate clock source. 5—The clock source was created by a command.
Source	IPv6 address of the NTP server. If this field displays ::, the IPv6 address of the NTP server has not been resolved successfully.
Reference	<p>Reference clock ID of the NTP server:</p> <ul style="list-style-type: none"> If the reference clock is the local clock, the value of this field is related to the value of the Clock stratum field: <ul style="list-style-type: none"> When the value of the Clock stratum field is 0 or 1, this field displays Local. When the Clock stratum field has another value, this field displays the MD5 digest value of the first 32 bits of the IPv6 address. The MD5 digest value is in dotted decimal format. If the reference clock is the clock of another device on the network, this field displays the MD5 digest value of the first 32 bits of the IPv6 address. The MD5 digest value is in dotted decimal format. If this field displays INIT, the local device has not established a connection with the NTP server.
Clock stratum	Stratum level of the NTP server, which determines the clock accuracy. The value is in the range of 1 to 16. A lower stratum level represents higher clock accuracy. A stratum 16 clock is not synchronized and cannot be used as a reference clock.
Reachabilities	Reachability count of the NTP server. 0 indicates that the NTP server is unreachable.
Poll interval	Polling interval in seconds. It is the maximum interval between successive NTP messages.
Last receive time	<p>Length of time from when the last NTP message was received or when the local clock was last updated to the current time.</p> <p>Time is in seconds by default.</p> <ul style="list-style-type: none"> If the time length is greater than 2048 seconds, it is displayed in minutes. If the time length is greater than 300 minutes, it is displayed in hours. If the time length is greater than 96 hours, it is displayed in days. If the time length is greater than 999 days, it is displayed in years. <p>If the time when the most recent NTP message was received or when the local clock was updated most recently is behind the current time, a hyphen (-) is displayed.</p>
Offset	Offset of the system clock relative to the reference clock, in milliseconds.
Roundtrip delay	Roundtrip delay from the local device to the clock source, in milliseconds.
Dispersion	Maximum error of the system clock relative to the reference source.
Total sessions	Total number of associations.

New command: ntp-service ipv6 access

Syntax

ntp-service ipv6 access { **peer** | **query** | **server** | **synchronization** } *acl-number*

undo ntp-service ipv6 access { **peer** | **query** | **server** | **synchronization** }

View

System view

Default level

3: Manage level

Parameters

peer: Permits full access. This level of right permits the peer devices to perform synchronization and control query to the local device and also permits the local device to synchronize its clock to that of a peer device. Control query refers to query of NTP status information, such as alarm information, authentication status, and clock source information.

query: Permits control query. This level of right permits the peer devices to perform control query to the NTP service on the local device but does not permit a peer device to synchronize its clock to that of the local device.

server: Permits server access and query. This level of right permits the peer devices to perform synchronization and control query to the local device but does not permit the local device to synchronize its clock to that of a peer device.

synchronization: Permits server access only. This level of right permits a peer device to synchronize its clock to that of the local device but does not permit the peer devices to perform control query.

acl-number: Specifies a basic ACL number in the range of 2000 to 2999.

Description

Use **ntp-service ipv6 access** to configure the access-control right for the peer devices to access the IPv6 NTP services of the local device.

Use **undo ntp-service ipv6 access** to remove the configured IPv6 NTP service access-control right to the local device.

By default, the access-control right for the peer devices to access the IPv6 NTP services of the local device is set to **peer**.

From the highest NTP service access-control right to the lowest one are **peer**, **server**, **synchronization**, and **query**. When a device receives an NTP request, it matches against the access-control right in this order and uses the first matched right. If no matched right is found, the device drops the NTP request.

The **ntp-service ipv6 access** command provides only a minimum degree of security protection. A more secure method is identity authentication. The related command is **ntp-service authentication enable**.

Before specifying an ACL number in the **ntp-service ipv6 access** command, make sure you have already created and configured this ACL.

Examples

Configure the peer devices on subnet 2001::1 to have full access to the local device.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2001
[Sysname-acl6-basic-2001] rule permit source 2001::1 64
[Sysname-acl6-basic-2001] quit
```

```
[Sysname] ntp-service ipv6 peer acl 2001
```

New command: ntp-service ipv6 dscp

Syntax

```
ntp-service ipv6 dscp dscp-value  
undo ntp-service ipv6 dscp
```

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies the Differentiated Services Code Point (DSCP) value for IPv6 NTP messages, in the range of 0 to 63.

Description

Use the **ntp-service ipv6 dscp** command to set the DSCP value for IPv6 NTP messages.

Use the **undo ntp-service ipv6 dscp** command to restore the default.

By default, the DSCP value for IPv6 NTP messages is 56.

Examples

```
# Set the DSCP value to 30 for IPv6 NTP messages.
```

```
<Sysname> system-view
```

```
[Sysname] ntp-service ipv6 dscp 30
```

New command: ntp-service ipv6 in-interface disable

Syntax

```
ntp-service ipv6 in-interface disable  
undo ntp-service ipv6 in-interface disable
```

View

VLAN interface view

Default level

3: Manage level

Parameters

None

Description

Use **ntp-service ipv6 in-interface disable** to disable an interface from receiving IPv6 NTP messages.

Use **undo ntp-service ipv6 in-interface disable** to restore the default.

By default, all interfaces are enabled to receive IPv6 NTP messages.

Examples

```
# Disable VLAN-interface 1 from receiving IPv6 NTP messages.
```

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service ipv6 in-interface disable
```

New command: ntp-service ipv6 multicast-client

Syntax

```
ntp-service ipv6 multicast-client ipv6-address
undo ntp-service ipv6 multicast-client ipv6-address
```

View

VLAN interface view

Default level

3: Manage level

Parameters

ipv6-address: Specifies an IPv6 multicast IP address. An IPv6 broadcast client and an IPv6 broadcast server must be configured with the same multicast address.

Description

Use **ntp-service ipv6 multicast-client** to configure the device to operate in IPv6 NTP multicast client mode and use the current interface to receive IPv6 NTP multicast packets.

Use **undo ntp-service ipv6 multicast-client** to remove the configuration.

By default, the device does not operate in any NTP operation mode.

Examples

Configure the device to operate in IPv6 multicast client mode and receive IPv6 NTP multicast messages with the destination FF21::1 on VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service ipv6 multicast-client ff21::1
```

New command: ntp-service ipv6 multicast-server

Syntax

```
ntp-service ipv6 multicast-server [ ipv6-address ] [ authentication-keyid keyid | ttl ttl-number ] *
undo ntp-service ipv6 multicast-server [ ipv6-address ]
```

View

VLAN interface view

Default level

3: Manage level

Parameters

ipv6-address: Specifies an IPv6 multicast IP address. An IPv6 multicast client and server must be configured with the same multicast address.

authentication-keyid *keyid*: Specifies the key ID to be used for sending multicast messages to multicast clients, where *keyid* is in the range of 1 to 4294967295. This parameter is not meaningful if authentication is not required.

ttl *ttl-number*: Specifies the TTL of NTP multicast messages. The value range for the *ttl-number* argument is 1 to 255, and the default is 16.

Description

Use **ntp-service ipv6 multicast-server** to configure the device to operate in IPv6 NTP multicast server mode and use the current interface to send IPv6 NTP multicast packets.

Use **undo ntp-service ipv6 multicast-server** to remove the configuration.

By default, the device does not operate in any NTP operation mode.

Examples

```
# Configure the device to operate in IPv6 multicast server mode and send IPv6 NTP multicast
messages on VLAN-interface 1 to the multicast address FF21::1, using key 4 for encryption.
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service ipv6 multicast-server ff21::1 authentication-keyid
4
```

New command: ntp-service ipv6 source-interface

Syntax

ntp-service ipv6 source-interface *interface-type interface-number*

undo ntp-service ipv6 source-interface

View

System view

Default level

3: Manage level

Parameters

interface-type interface-number. Specifies an interface by its type and number.

Description

Use **ntp-service ipv6 source-interface** to specify the source interface for IPv6 NTP messages.

Use **undo ntp-service ipv6 source-interface** to restore the default.

By default, no source interface is specified for IPv6 NTP messages, and the system uses the IP address of the interface determined by the matched route as the source IP address of IPv6 NTP messages.

If you do not want the IP address of a certain interface on the local device to become the destination address of response messages, use this command to specify the source interface for IPv6 NTP messages so that the source IP address in IPv6 NTP messages is the primary IP address of this interface.

If the specified source interface goes down, NTP searches the routing table for the outgoing interface, and uses the primary IP address of the outgoing interface as the source IP address.

Examples

```
# Specify the source interface of IPv6 NTP messages as VLAN-interface 1.
<Sysname> system-view
[Sysname] ntp-service ipv6 source-interface vlan-interface 1
```

New command: ntp-service ipv6 unicast-peer

Syntax

ntp-service ipv6 unicast-peer { *ipv6-address* | *peer-name* } [**authentication-keyid** *keyid* | **priority** | **source-interface** *interface-type interface-number*] *

undo ntp-service ipv6 unicast-peer { *ipv6-address* | *peer-name* }

View

System view

Default level

3: Manage level

Parameters

peer-name: Specifies a host name of the symmetric-passive peer, a string of 1 to 20 characters.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the peer, where *keyid* is in the range of 1 to 4294967295.

priority: Specifies the peer designated by *ip-address* or *peer-name* as the first choice under the same condition.

source-interface *interface-type interface-number*: Specifies the source interface for NTP messages. In an NTP message that the local device sends to its peer, the source IP address is the primary IP address of this interface.

Description

Use **ntp-service ipv6 unicast-peer** to designate an IPv6 symmetric-passive peer for the device.

Use **undo ntp-service ipv6 unicast-peer** to remove the IPv6 symmetric-passive peer designated for the device.

By default, no IPv6 symmetric-passive peer is designated for the device.

Examples

Designate the device with the IPv6 address of 2001::1 as the symmetric-passive peer of the device, and specify the source interface of IPv6 NTP messages as VLAN-interface 1.

```
<Sysname> system-view
```

```
[Sysname] ntp-service ipv6 unicast-peer 2001::1 source-interface vlan-interface 1
```

New command: ntp-service ipv6 unicast-server

Syntax

ntp-service ipv6 unicast-server { *ipv6-address* | *server-name* } [**authentication-keyid** *keyid* | **priority** | **source-interface** *interface-type interface-number*] *

undo ntp-service ipv6 unicast-server { *ipv6-address* | *server-name* }

View

System view

Default level

3: Manage level

Parameters

server-name: Specifies a host name of the NTP server, a string of 1 to 20 characters.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the NTP server, where *keyid* is in the range of 1 to 4294967295.

priority: Specifies this NTP server as the first choice under the same condition.

source-interface *interface-type interface-number*: Specifies the source interface for IPv6 NTP messages. In an IPv6 NTP message that the local device sends to the NTP server, the source IPv6 address is the primary IP address of this interface.

Description

Use **ntp-service ipv6 unicast-server** to designate an IPv6 NTP server for the device.

Use **undo ntp-service ipv6 unicast-server** to remove an IPv6 NTP server designated for the device.

By default, no IPv6 NTP server is designated for the device.

Examples

Designate NTP server 2001::1 for the device.

```
<Sysname> system-view
```

```
[Sysname] ntp-service ipv6 unicast-server 2001::1
```

Modified feature: Random number generator standards

Feature change description

The standards for random number generator were changed to CTR_DRBG.

Command changes

None.

Modified feature: Enhanced CC authentication feature

Feature change description

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

Command changes

New command: display public-key local ecdsa public

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

Syntax

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

Views

Any view

Default command level

1: Monitor level

Parameters

ecdsa: Displays the local ECDSA host public key.

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

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

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

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

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

Examples

Display the local ECDSA host public key.

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

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

Table 5 Command output

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

New command: public-key local export ecdsa

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

Syntax

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

Views

System view

Default command level

2: System level

Parameters

openssh: Uses the format of OpenSSH.

ssh2: Uses the format of SSH2.0.

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

Usage guidelines

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

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

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

Examples

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

```
<Sysname> system-view
```

```
[Sysname] public-key local export ecdsa openssh key.pub
```

Modified command: authentication-algorithm

Old syntax

```
authentication-algorithm sha
```

New syntax

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

Views

IKE proposal view

Change description

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

Modified command: ciphersuite

Old syntax

In FIPS mode:

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

New syntax

In FIPS mode:

```
ciphersuite { rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha } *
```

Views

SSL server policy view

Change description

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

Modified command: dh

Old syntax

```
dh { group2 | group5 | group14 }
```


New syntax

dh group14

Views

IKE proposal view

Change description

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

Modified command: pfs

Old syntax

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

New syntax

pfs dh-group14

Views

IPsec policy view

Change description

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

Modified command: prefer-cipher

Old syntax

In FIPS mode:

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

New syntax

In FIPS mode:

prefer-cipher { rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha }

Views

SSL client policy view

Change description

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

Modified command: pre-shared-key

Old syntax

pre-shared-key [cipher | simple] key

New syntax

pre-shared-key [cipher key]

Views

IKE peer view

Change description

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

Modified command: **public-key local create**

Old syntax

public-key local create { dsa | rsa }

New syntax

In non-FIPS mode:

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

In FIPS mode:

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

Views

System view

Change description

Before modification:

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

After modification:

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

Modified command: **scp**

Old syntax

In non-FIPS mode:

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

In FIPS mode:

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

New syntax

In non-FIPS mode:

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

In FIPS mode:

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

Views

User view

Change description

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

Modified command: sftp

Old syntax

In non-FIPS mode:

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

In FIPS mode:

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

New syntax

In non-FIPS mode:

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

In FIPS mode:

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

Views

User view

Change description

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

Modified command: ssh2

Old syntax

In non-FIPS mode:

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

In FIPS mode:

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

New syntax

In non-FIPS mode:

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

In FIPS mode:

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

Views

User view

Change description

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

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.

R5501P17

This release has the following changes:

- New feature: Disabling reactivation for edge ports shut down by BPDU guard
- New feature: Data buffer monitoring
- New feature: Automatic PI reset
- New feature: Configuring the default action of the table-miss flow entry
- Modified feature: Configuring the OpenFlow instance mode
- Modified feature: Creating an OpenFlow table for an OpenFlow instance

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*.

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

New command: 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

Default command level

2: System level

Description

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: 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 <i>slot-number ratio ratio</i>	By default, the buffer usage threshold is 100.
3. Return to user view.	quit	N/A
4. Display buffer usage statistics for interfaces.	display buffer usage interface [<i>interface-type</i> [<i>interface-number</i>]]	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

The buffer usage threshold is 100.

Views

System view

Default command level

2: System level

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.

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% on 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

Default command level

1: Monitor level

Parameters

interface-type [*interface-number*]: Specifies an interface by its interface 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 GigabitEthernet 1/0/1.

```
<Sysname> display buffer usage interface gigabitethernet 1/0/1
```

Interface	QueueID	Total	Used	Threshold(%)	Violations

GE1/0/1	0	1357056	0	20	0
	1	1357056	0	20	0
	2	1357056	0	20	0
	3	1357056	0	20	0
	4	1357056	0	20	0
	5	1357056	0	20	0

6	1357056	0	20	0
7	1357056	0	20	0

Table 1 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 command output information displayed in [Table 2](#) was changed.

Table 2 Command output changes

Before modification	After modification	Field description
Packets dropped by Full GBP or insufficient bandwidth: 0	Packets dropped due to full GBP or insufficient bandwidth: 0	Number of packets that were dropped because of insufficient memory or bandwidth.
Packets dropped by Fast Filter Processor (FFP): 0	Packets dropped due to Fast Filter Processor (FFP): 0	Number of packets that were dropped because of packet filtering.
Packets dropped by STP non-forwarding state: 0	Packets dropped due to STP non-forwarding state: 0	Number of packets that were dropped because STP is in discarding state.
-	Packets dropped due to insufficient data buffer. Input dropped: 0 Output dropped: 0	Number of inbound packets and number of outbound packets that were dropped because of insufficient data buffer.

Display information about dropped packets on all interfaces.

```
<Sysname> display packet-drop summary
```

All interfaces:

```
Packets dropped due to full GBP or insufficient bandwidth: 301
```

```
Packets dropped due to Fast Filter Processor (FFP): 261
```

```
Packets dropped due to STP non-forwarding state: 321
```

```
Packets dropped due to insufficient data buffer. Input dropped: 0 Output dropped:0
```

New feature: Automatic PI reset

Enabling automatic PI reset

This feature enables PIs to reset automatically after you reboot the device by using the **reboot** command. After the reset, the PIs resume data and power supply services.

To enable automatic PI reset:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable automatic PI reset.	poe reset enable	By default, automatic PI reset is disabled.

Command reference

poe reset enable

Use **poe reset enable** to enable automatic PI reset.

Use **undo poe reset enable** to disable automatic PI reset.

Syntax

poe reset enable

undo poe reset enable

Default

Automatic PI reset is disabled.

Views

System view

Default command level

2: System level

Examples

```
# Enable automatic PI reset.  
<Sysname> system-view  
[Sysname] poe reset enable
```

New feature: Configuring the default action of the table-miss flow entry

Configuring the default action of the table-miss flow entry

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter OpenFlow instance view.	openflow instance <i>instance-id</i>	N/A

Step	Command	Remarks
3. Change the default action of the table-miss flow entry to forward packets to the normal pipeline.	default table-miss permit	By default, the default action of the table-miss flow entry is to drop packets after the OpenFlow instance is activated and before the controller deploys flow entries.

Command reference

New command: default table-miss permit

Use **default table-miss permit** to change the default action of the table-miss flow entry to forward packets to the normal pipeline.

Use **undo default table-miss permit** to restore the default.

Syntax

default table-miss permit

undo default table-miss permit

Default

The default action of the table-miss flow entry is to drop packets after the OpenFlow instance is activated and before the controller deploys flow entries.

Views

OpenFlow instance view

Default command level

2: System level

Examples

Change the default action of the table-miss flow entry to forward packets to the normal pipeline.

```
<Sysname> system-view
```

```
[Sysname] openflow instance 1
```

```
[Sysname-of-inst-1] default table-miss permit
```

Modified feature: Configuring the OpenFlow instance mode

Feature change description

You can configure the global mode.

Command changes

Modified command: classification

Old syntax

classification vlan *vlan-id* [mask *vlan-mask*] [loosen]

New syntax

classification { **global** | **vlan** *vlan-id* [**mask** *vlan-mask*] [**loosen**] }

Views

OpenFlow instance view

Change description

The **global** option was added.

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.

R5501P15

This release has the following changes:

- [Modified feature: Storm control for known unicast packets](#)
- [Modified feature: Setting the maximum number of logs that can be stored in the log buffer](#)
- [Modified feature: VPN instance support for NQA server configuration](#)

Modified feature: Storm control for known unicast packets

Feature change description

The **known-unicast** keyword was added to the **storm-constrain** command. You can use the keyword to configure storm control for known unicast packets.

Command changes

Modified command: storm-constrain

Old syntax

```
storm-constrain { broadcast | multicast | unicast } { pps | kbps | ratio } upperlimit lowerlimit
```

New syntax

```
storm-constrain { broadcast | multicast | unicast | known-unicast } { pps | kbps | ratio } upperlimit lowerlimit
```

Views

Layer 2 Ethernet interface view

Change description

The **known-unicast** keyword was added. You can use the keyword to configure storm control for known unicast packets. The storm control thresholds for known unicast packets can be set only in pps.

Modified feature: Setting the maximum number of logs that can be stored in the log buffer

Feature change description

The maximum value for the *buffersize* argument of the **info-center logbuffer** command was changed from 1024 to 51200. The default setting for the argument was changed from 512 to 51200.

Command changes

Modified command: info-center logbuffer

Syntax

```
info-center logbuffer [ channel { channel-number | channel-name } | size buffersize ] *
```

Views

System view

Change description

Before modification: The value range for the *buffersize* argument is 0 to 1024, and the default is 512.

After modification: The value range for the *buffersize* argument is 0 to 51200, and the default is 51200.

Modified feature: VPN instance support for NQA server configuration

Feature change description

The **vpn-instance** keyword was added to the **nqa server** command. You can use the keyword to enable the NQA server to listen on an IP address in a VPN instance.

Command changes

Modified command: nqa server

Old syntax

```
nqa server { tcp-connect | udp-echo } ip-address port-number
```

New syntax

```
nqa server { tcp-connect | udp-echo } ip-address port-number [ vpn-instance vpn-instance-name ]
```

Views

System view

Change description

The **vpn-instance** keyword was added. You can use the keyword to enable the NQA server to listen on an IP address in a VPN instance.

R5501P13

This release has the following changes:

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

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

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

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

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

To configure the device to send EAP-Success packets to users in the 802.1X critical VLAN:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the 802.1X critical VLAN on the port.	dot1x critical vlan <i>vlan-id</i>	Required. By default, no 802.1X critical VLAN is configured. Different ports can be configured with different critical VLANs, and one port can only be configured with a maximum of one critical VLAN.
4. Configure the port to trigger 802.1X re-authentication on detection of an active authentication server for users in the critical VLAN.	dot1x critical recovery-action reinitialize	Required. By default, when a reachable server is detected, the system removes the port or 802.1X users from the critical VLAN without triggering authentication.
5. Configure the device to send EAP-Success packets to 802.1X users in the critical VLAN on the port.	dot1X critical eapol	Required. By default, the device does not send EAP-Success packets to 802.1X users in the critical VLAN.

Command reference

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 GigabitEthernet 1/0/1 to send EAP-Success packets to 802.1X users in the critical VLAN.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] dot1x critical eapol
```


R5501P12

This release has no feature changes.

R5501P11

This release has the following changes:

- [New feature: Login delay](#)
- [Modified feature: IPv6 address with a 127-bit prefix length](#)
- [Modified feature: Specifying log hosts](#)

New feature: Login delay

Enabling the login delay

The login delay feature delays the device to accept a login request from a user after the user fails a login attempt. This feature can slow down login dictionary attacks.

To enable the login delay:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the login delay feature.	attack-defense login reauthentication-delay <i>seconds</i>	By default, the login delay feature is disabled.

Command reference

attack-defense login reauthentication-delay

Syntax

attack-defense login reauthentication-delay *seconds*

undo attack-defense login reauthentication-delay

Views

System view

Default command level

2: System level

Parameters

seconds: Sets the delay period in seconds, in the range of 4 to 60.

Description

Use **attack-defense login reauthentication-delay** to enable the login delay feature.

Use **undo attack-defense login reauthentication-delay** to restore the default.

By default, the login delay feature is disabled. The device does not delay accepting a login request from a user who has failed a login attempt.

Examples

Enable the login delay feature and set the delay period to 5 seconds.

```
<Sysname> system-view
```

[Sysname] attack-defense login reauthentication-delay 5

Modified feature: IPv6 address with a 127-bit prefix length

Feature change description

Before modification, you cannot execute the **ipv6 address** command to configure an IPv6 global unicast address in the form of **XXX::2/127**. The system identifies IPv6 address in this form as an anycast address.

After modification:

- You can use the **ipv6 address** command to configure an IPv6 global unicast address in the form of **XXX::2/127**.
- The system does not support any IPv6 anycast address with the 127-bit prefix length.

Command changes

None.

Modified feature: Specifying log hosts

Feature change description

The maximum number of log hosts that can be configured by using the **info-center loghost** command 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.

R5501P10

This release has the following changes:

- **New feature:** [SNMP notifications for PVST topology changes](#)

New feature: SNMP notifications for PVST topology changes

Enabling SNMP notifications for PVST topology changes

This feature enables the device to generate logs and report PVST topology change events to an NMS when the device detects or receives a TC BPDU. For the SNMP notifications to be sent correctly, you must also configure SNMP as described in *Network Management and Monitoring Configuration Guide*.

To enable SNMP notifications for PVST topology changes:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable SNMP notifications for PVST topology changes.	snmp-agent trap enable stp [tc]	By default, SNMP notifications are disabled for PVST topology changes on all VLANs.

Command reference

snmp trap enable stp

Use **snmp-agent trap enable stp** to enable SNMP notifications for PVST topology changes.

Use **undo snmp-agent trap enable stp** to disable SNMP notifications for PVST topology changes.

Syntax

snmp-agent trap enable stp [**tc**]

undo snmp-agent trap enable stp [**tc**]

Default

SNMP notifications are disabled for PVST topology changes on all VLANs.

Views

System view

Predefined user roles

3: Manage level

Parameters

tc: Specifies SNMP notifications for PVST topology changes.

Usage guidelines

This command configures SNMP notifications only for PVST topology changes whether you specify the **tc** keyword or not.

Examples

Enable SNMP notifications for PVST topology changes.

```
<Sysname> system-view
```

```
[Sysname] snmp-agent trap enable stp tc
```

R5501P06

This release has the following changes:

- New feature: Disabling SSL 3.0
- New feature: 802.1X MAC address binding
- New feature: Web connection idle timeout
- New feature: Applicable scope of packet filtering on a VLAN interface

New feature: Disabling SSL 3.0

Disabling SSL 3.0

This feature allows you to disable SSL 3.0 on a device to enhance system security.

- An SSL server supports only TLS 1.0 after SSL 3.0 is disabled.
- An SSL client always uses SSL 3.0 if SSL 3.0 is specified for the client policy, whether you disable SSL 3.0 or not.

To ensure successful establishment of an SSL connection, do not disable SSL 3.0 on a device when the peer device only supports SSL 3.0. HP recommends upgrading the peer device to support TLS 1.0 to improve security.

To disable SSL 3.0 on a device:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Disable SSL 3.0 on the device.	ssl version ssl3.0 disable	By default, the device supports SSL 3.0.

Command reference

ssl version ssl3.0 disable

Syntax

ssl version ssl3.0 disable

undo ssl version ssl3.0 disable

Views

System view

Parameters

None

Description

Use **ssl version ssl3.0 disable** to disable SSL 3.0 on the device. Use **undo ssl version ssl3.0 disable** restore the default.

By default, the device supports SSL 3.0.

Examples

```
# Disable SSL 3.0 on the device.
<Sysname> system-view
[Sysname] ssl version ssl3.0 disable
```

New feature: 802.1X MAC address binding

Configuring 802.1X MAC address binding

This feature can automatically bind MAC addresses of authenticated 802.1X users to the users' access port and generate 802.1X MAC address binding entries. You can also use the **dot1x binding-mac mac-address** command to manually configure 802.1X MAC address binding entries.

802.1X MAC address binding entries never age out. They can survive a user logoff or a device reboot. To delete an entry, you must use the **undo dot1x binding-mac mac-address** command.

After the number of 802.1X MAC address binding entries reaches the upper limit of concurrent 802.1X users, the following restrictions exist:

- Users not in the binding entries will fail authentication even after users in the binding entries go offline.
- New 802.1X MAC address binding entries are not allowed.

When you configure the 802.1X MAC address binding feature on a port, follow these restrictions and guidelines:

- The 802.1X MAC address binding feature takes effect only when the port performs MAC-based access control.
- Manually configured MAC address binding entries take effect only when the 802.1X MAC address binding feature takes effect.
- An 802.1X MAC address binding entry cannot be deleted when the user in the entry is online.

To configure the 802.1X MAC address binding feature on a port:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view.	interface <i>interface-type interface-number</i>	N/A
3. Enable the 802.1X MAC address binding feature.	dot1x binding-mac enable	By default, the feature is disabled.
4. (Optional.) Manually configure 802.1X MAC address binding entries.	dot1x binding-mac <i>mac-address</i>	By default, no 802.1X MAC address binding entries are configured on the port.

Command reference

dot1x binding-mac enable

Use **dot1x binding-mac enable** to enable the 802.1X MAC address binding feature.

Use **undo dot1x binding-mac enable** to restore the default.

Syntax

dot1x binding-mac enable

undo dot1x binding-mac enable

Default

The 802.1X MAC address binding feature is disabled.

Views

Layer 2 Ethernet interface view

Default command level

2: System level

Usage guidelines

This command takes effect on a port only when the port performs MAC-based access control.

The 802.1X MAC address binding feature automatically binds MAC addresses of authenticated 802.1X users to the users' access port and generates 802.1X MAC address binding entries.

802.1X MAC address binding entries, both automatically generated and manually configured, never age out. They can survive a user logoff or a device reboot. To delete an entry, you must use the **undo dot1x binding-mac mac-address** command. An 802.1X MAC address binding entry cannot be deleted when the user in the entry is online.

After the number of 802.1X MAC address binding entries reaches the upper limit of concurrent 802.1X users (set by using the **dot1x max-user** command), the following restrictions exist:

- Users not in the binding entries will fail authentication even after users in the binding entries go offline.
- New 802.1X MAC address binding entries are not allowed.

Examples

Enable 802.1X MAC address binding on GigabitEthernet 1/0/1.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] dot1x binding-mac enable
```

dot1x binding-mac

Use **dot1x binding-mac** to configure an 802.1X MAC address binding entry.

Use **undo dot1x binding-mac** to delete an 802.1X MAC address binding entry.

Syntax

dot1x binding-mac mac-address

undo dot1x binding-mac mac-address

Default

No 802.1X MAC address binding entries are configured on a port.

Views

Layer 2 Ethernet interface view

Default command level

2: System level

Parameters

mac-address: Specifies a MAC address, in the format of H-H-H, excluding broadcast, multicast, and all-zero MAC addresses.

Usage guidelines

This command takes effect only the 802.1X MAC address binding feature takes effect.

802.1X MAC address binding entries, both manually configured and automatically generated, never age out. They can survive a user logoff or a device reboot. To delete an entry, you must use the **undo dot1x binding-mac mac-address** command. An 802.1X MAC address binding entry cannot be deleted when the user in the entry is online.

After the number of 802.1X MAC address binding entries reaches the upper limit of concurrent 802.1X users (set by using the **dot1x max-user** command), the following restrictions exist:

- Users not in the binding entries will fail authentication even after users in the binding entries go offline.
- New 802.1X MAC address binding entries are not allowed.

Examples

Configure an 802.1X MAC address binding entry on GigabitEthernet 1/0/1.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] dot1x binding-mac 000a-eb29-75f1
```

New feature: Web connection idle timeout

Setting the Web connection idle timeout

The system automatically terminates a Web connection if no mouse or keyboard operation occurs within the idle timeout interval.

To set the Web connection idle timeout:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the Web connection idle timeout.	web idle-timeout <i>idle-time</i>	By default, the Web connection idle timeout is 10 minutes.

Command reference

web idle-timeout

Syntax

web idle-timeout *idle-time*

undo web idle-timeout

Default

The Web connection idle timeout is 10 minutes.

Views

System view

Default command level

2: System level

Parameters

idle-time: Specifies the idle timeout in minutes. The value range is 1 to 999.

Description

The system automatically terminates a user connection if no mouse or keyboard operation occurs within the idle timeout interval.

This command takes effect immediately for current Web connections.

Examples

Set the Web connection idle timeout to 100 minutes.

```
<Sysname> system-view
```

```
[Sysname] web idle-timeout 100
```

New feature: Applicable scope of packet filtering on a VLAN interface

Configuring the applicable scope of packet filtering on a VLAN interface

You can configure the packet filtering on a VLAN interface to filter the following packets:

- Packets forwarded at Layer 3 by the VLAN interface.
- All packets, including packets forwarded at Layer 3 by the VLAN interface and packets forwarded at Layer 2 by the physical ports associated with the VLAN interface.

To configure the applicable scope of packet filtering on a VLAN interface:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a VLAN interface and enter its view.	interface vlan-interface <i>vlan-interface-id</i>	If the VLAN interface already exists, you directly enter its view. By default, no VLAN interface exists.
3. Specify the applicable scope of packet filtering on the VLAN interface.	packet-filter filter { route all }	By default, the packet filtering filters all packets.

Command reference

packet-filter filter

Use **packet-filter filter** to specify the applicable scope of packet filtering on a VLAN interface.

Use **undo packet-filter filter** to restore the default.

Syntax

packet-filter filter { **route** | **all** }

undo packet-filter filter

Default

The packet filtering filters all packets.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

route: Filters packets forwarded at Layer 3 by the VLAN interface.

all: Filters all packets, including packets forwarded at Layer 3 by the VLAN interface and packets forwarded at Layer 2 by the physical ports associated with the VLAN interface.

Examples

Configure the packet filtering on VLAN-interface 2 to filter packets forwarded at Layer 3.

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 2
```

```
[Sysname-Vlan-interface2] packet-filter filter route
```

R5501P05

This release has the following changes:

- [Modified feature: Executing interactive commands in interface range view](#)
- [Modified feature: Specifying RADIUS security policy servers by IP address](#)

Modified feature: Executing interactive commands in interface range view

Feature change description

Before modification: When executing an interactive command such as **default** in interface range view, you need to confirm the command execution on the member interfaces one by one.

After modification: When executing an interactive command such as **default** in interface range view, you do not need to confirm the command execution on the member interfaces one by one. The system automatically confirms the command execution on every member interface.

Command changes

None.

Modified feature: Specifying RADIUS security policy servers by IP address

Feature change description

Support for IPv6 RADIUS security policy servers was added.

Command changes

Modified command: security-policy-server

Old syntax

```
security-policy-server ip-address  
undo security-policy-server { ip-address | all }
```

New syntax

```
security-policy-server { ipv4-address | ipv6 ipv6-address }  
undo security-policy-server { ipv4-address | all | ipv6 ipv6-address }
```

Views

RADIUS scheme view

Change description

Before modification: The *ip-address* argument specifies an IPv4 address.

After modification: The *ip-address* argument was changed to *ipv4-address*, which specifies an IPv4 address. The **ipv6** *ipv6-address* option was added, which specifies an IPv6 address.

R5501P03

This release has the following changes:

- New feature: Per-flow load sharing
- New feature: Telnet/SSH user connection control
- New feature: Packet rate-limiting for the table-miss flow entry
- Modified feature: Including time zone information in the timestamp of system information sent to a log host
- Modified feature: Configuring physical state change suppression on an Ethernet interface
- Modified feature: Configuring a tag and description for an IPv6 static route

New feature: Per-flow load sharing

Configuring per-flow load sharing

Per-flow load sharing allows the device to forward flows over equal-cost routes. Packets of one flow travel along the same routes. You can configure the device to identify a flow based on the source IP address, destination IP address, source port number, destination port number, IP protocol number, and ingress port.

In a complex network, when these criteria cannot distinguish flows, you can use the `algorithm` keyword to specify an algorithm to identify flows for load sharing.

To configure per-flow load sharing:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure per-flow load sharing.	ip load-sharing mode { all slot <i>slot-number</i> } per-flow [algorithm <i>algorithm-number</i>] [dest-ip dest-port ingress-port ip-pro src-ip src-port] *]	By default, the device performs per-flow load sharing based on the source IP address and destination IP address.

Command reference

ip load-sharing mode

Use **ip load-sharing mode** to configure per-flow load sharing.

Use **undo ip load-sharing mode** to restore the default.

Syntax

ip load-sharing mode { **all** | **slot** *slot-number* } **per-flow** [**algorithm** *algorithm-number*] [**dest-ip** | **dest-port** | **ingress-port** | **ip-pro** | **src-ip** | **src-port**] *]

undo ip load-sharing mode { **all** | **slot** *slot-number* }

Default

The device performs per-flow load sharing based on the source IP address and destination IP address.

Views

System view

Default command level

2: System level

Parameters

per-flow: Implements per-flow load sharing.

algorithm *algorithm-number*: Specifies an algorithm for per-flow load sharing. The value range for the *algorithm-number* argument is 0 to 1, and the default value is 0.

dest-ip: Identifies flows by destination IP address.

dest-port: Identifies flows by destination port.

ingress-port: Identifies flows by ingress port.

ip-pro: Identifies flows by protocol number.

src-ip: Identifies flows by source IP address.

src-port: Identifies flows by source port.

all: Specifies all member devices.

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

Examples

Configure per-flow load sharing on IRF member device 2.

```
<Sysname> system-view
```

```
[Sysname] ip load-sharing mode slot 2 per-flow
```

New feature: Telnet/SSH user connection control

Configuring Telnet/SSH user connection control

This feature allows you to control Telnet/SSH user connections to the device based on the referenced ACL. Only the Telnet/SSH users that the referenced ACL permits can initiate Telnet/SSH connections to the device.

All Telnet/SSH users can initiate Telnet/SSH connections to the device when any one of the following conditions exists:

- You do not specify any ACLs.
- The specified ACL does not exist.
- The specified ACL does not have any rules.

Configuration prerequisites

Before you configure Telnet/SSH user connection control, configure the ACL as required.

Configuration procedure

To configure Telnet user connection control:

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Configure Telnet user connection control.	<ul style="list-style-type: none"> Configure IPv4 Telnet user connection control: telnet server acl <i>acl-number</i> Configure IPv6 Telnet user connection control: telnet server ipv6 acl ipv6 <i>acl-number</i> 	By default, all Telnet users can initiate Telnet connections to the device.

To configure SSH user connection control:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure SSH user connection control.	<ul style="list-style-type: none"> Configure IPv4 SSH user connection control: ssh server acl <i>acl-number</i> Configure IPv6 SSH user connection control: ssh server ipv6 acl ipv6 <i>acl-number</i> 	By default, all SSH users can initiate SSH connections to the device.

Command reference

ssh server acl

Use **ssh server acl** to specify an ACL to control IPv4 SSH user connections.

Use **undo ssh server acl** to restore the default.

Syntax

ssh server acl *acl-number*

undo ssh server acl

Default

No ACLs are specified and all IPv4 SSH users can initiate SSH connections to the device.

Views

System view

Default command level

3: Manage level

Parameters

acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999.

Usage guidelines

The specified ACL filters IPv4 SSH users' connection requests. Only the IPv4 SSH users that the ACL permits can initiate SSH connections to the device.

All IPv4 SSH users can initiate SSH connections to the device when any one of the following conditions exists:

- You do not specify any ACLs.
- The specified ACL does not exist.
- The specified ACL does not have any rules.

The ACL takes effect only on SSH connections that are initiated after the ACL configuration.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure ACL 2001 and permit only the users at 1.1.1.1 to initiate SSH connections to the device.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 1.1.1.1 0
[Sysname-acl-basic-2001] quit
[Sysname] ssh server acl 2001
```

ssh server ipv6 acl ipv6

Use **ssh server ipv6 acl ipv6** to specify an ACL to control IPv6 SSH user connections.

Use **undo ssh server ipv6 acl** to restore the default.

Syntax

ssh server ipv6 acl ipv6 *acl-number*

undo ssh server ipv6 acl

Default

No ACLs are specified and all IPv6 SSH users can initiate SSH connections to the device.

Views

System view

Default command level

3: Manage level

Parameters

acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999.

Usage guidelines

The specified ACL filters IPv6 SSH users' connection requests. Only the IPv6 SSH users that the ACL permits can initiate SSH connections to the device.

All IPv6 SSH users can initiate SSH connections to the device when any one of the following conditions exists:

- You do not specify any ACLs.
- The specified ACL does not exist.
- The specified ACL does not have any rules.

The ACL takes effect only on SSH connections that are initiated after the ACL configuration.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure ACL 2001 and permit only the users on the subnet 1::1/64 to initiate SSH connections to the device.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2001
[Sysname-acl6-basic-2001] rule permit source 1::1 64
[Sysname-acl6-basic-2001] quit
[Sysname] ssh server ipv6 acl ipv6 2001
```

telnet server acl

Use **telnet server acl** to specify an ACL to control IPv4 Telnet user connections.

Use **undo telnet server acl** to restore the default.

Syntax

telnet server acl *acl-number*

undo telnet server acl

Default

No ACLs are specified and all IPv4 Telnet users can initiate Telnet connections to the device.

Views

System view

Default command level

3: Manage level

Parameters

acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999.

Usage guidelines

This command is not supported in FIPS mode.

The specified ACL filters IPv4 Telnet users' connection requests. Only the IPv4 Telnet users that the ACL permits can initiate Telnet connections to the device.

All IPv4 Telnet users can initiate Telnet connections to the device when any one of the following conditions exists:

- You do not specify any ACLs.
- The specified ACL does not exist.
- The specified ACL does not have any rules.

The ACL takes effect only on Telnet connections that are initiated after the ACL configuration.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure ACL 2001 and permit only the users at 1.1.1.1 to initiate Telnet connections to the device.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 1.1.1.1 0
[Sysname-acl-basic-2001] quit
[Sysname] telnet server acl 2001
```

telnet server ipv6 acl ipv6

Use **telnet server ipv6 acl ipv6** to specify an ACL to control IPv6 Telnet user connections.

Use **undo telnet server ipv6 acl** to restore the default.

Syntax

telnet server ipv6 acl ipv6 *acl-number*

undo telnet server ipv6 acl

Default

No ACLs are specified and all IPv6 Telnet users can initiate Telnet connections to the device.

Views

System view

Default command level

3: Manage level

Parameters

acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999.

Usage guidelines

This command is not supported in FIPS mode.

The specified ACL filters IPv6 Telnet users' connection requests. Only the IPv6 Telnet users that the ACL permits can initiate Telnet connections to the device.

All IPv6 Telnet users can initiate Telnet connections to the device when any one of the following conditions exists:

- You do not specify any ACLs.
- The specified ACL does not exist.
- The specified ACL does not have any rules.

The ACL takes effect only on Telnet connections that are initiated after the ACL configuration.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure ACL 2001 and permit only the users at 2000::1 to initiate Telnet connections to the device.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2001
[Sysname-acl6-basic-2001] rule permit source 2000::1 128
[Sysname-acl6-basic-2001] quit
[Sysname] telnet server ipv6 acl ipv6 2001
```

New feature: Packet rate-limiting for the table-miss flow entry

Packet rate-limiting for the table-miss flow entry

You can specify a meter entry for the table-miss flow entry for rate-limiting on the controller and deploy the table-miss flow entry to devices. Packets that match the table-miss flow entry are directed to the meter entry for rate-limiting before they are sent to the controller.

Command reference

display openflow flow-table

Use **display openflow flow-table** to display flow table information for an OpenFlow instance.

Syntax

display openflow instance *instance-id* **flow-table** [*table-id*]

Views

Any view

Change description

Before modification: The output from the **display openflow flow-table** command does not include information about the meter entry used by the table-miss flow entry.

After modification: The output from the **display openflow flow-table** command includes information about the meter entry used by the table-miss flow entry.

Modified feature: Including time zone information in the timestamp of system information sent to a log host

Feature change description

Added support for including time zone information in the timestamp of system information sent to a log host.

Command changes

Modified command: info-center timestamp loghost

Old syntax

```
info-center timestamp loghost { date | iso | no-year-date | none }
```

New syntax

```
info-center timestamp loghost { date | iso [ with-timezone ] | no-year-date | none }
```

Views

System view

Change description

The following parameter was added:

with-timezone: Includes time zone information in the timestamp of system information sent to a log host.

Modified feature: Configuring physical state change suppression on an Ethernet interface

Feature change description

Before modification:

- The system can suppress only link-down or only link-up events. For example, if you configure the **link-delay delay-time [mode up]** command and then configure the **link-delay delay-time** command, the system suppresses only link-down events.
- When you disable physical state change suppression on an interface, suppression for both link-up and link-down events are disabled.

After modification, you can perform the following operations:

- Enable the physical state change suppression time to be accurate to milliseconds by specifying the **msec** keyword.
- Enable the system to suppress both link-down and link-up events by specifying the **updown** keyword.
- Configure different suppression intervals for link-up and link-down events. For example, if you configure the **link-delay [msec] delay-time [mode up]** command and then configure the **link-delay [msec] delay-time** command, both commands take effect.
- Disable suppression for only link-up events, only link-down events, or both. For example, when both link-up and link-down events are suppressed on an interface and you configure the **undo link-delay delay-time mode up** command, only suppression for link-up events is disabled.

Command changes

Modified command: link-delay

Old syntax

```
link-delay delay-time [ mode up ]
undo link-delay
```

New syntax

```
link-delay [ msec ] delay-time [ mode { up | updown } ]
undo link-delay [ [ msec delay-time ] [ mode { up | updown } ] ]
```

Views

Ethernet interface view

Change description

Before modification:

- The value range for the *delay-time* argument is 2 to 10 seconds.
- When you configure the **undo link-delay** command on an interface, suppression for both link-up and link-down events are disabled.

After modification:

- The **msec** and **updown** keywords were added to the **link-delay delay-time [mode up]** command.
 - If you specify the **msec** keyword, the value range for the *delay-time* argument is 500 to 10000 milliseconds, and the value must be an integer multiple of 100. If you do not specify the **msec** keyword, the value range for the *delay-time* argument is 2 to 10 seconds.
 - If you specify the **updown** keyword, the link-down or link-up event is not reported to the CPU unless the interface is still down or up when the suppression interval (*delay-time*) expires.
- The **undo link-delay** command was changed to **undo link-delay [[msec delay-time] [mode { up | updown }]]**.

You can disable suppression for only link-up events, only link-down events, or both. For example, when both link-up and link-down events are suppressed on an interface and you configure the **undo link-delay delay-time mode up** command, only suppression for link-up events is disabled.

Modified feature: Configuring a tag and description for an IPv6 static route

Feature change description

The **tag** *tag-value* and **description** *description-text* options were added to the **ipv6 route-static** command. The **tag** *tag-value* option configures a tag for an IPv6 static route, and the **description** *description-text* option configures a description for an IPv6 static route.

Command changes

Modified command: ipv6 route-static

Old syntax

```
ipv6 route-static ipv6-address prefix-length { interface-type interface-number [ next-hop-address ] | next-hop-address } [ vpn-instance d-vpn-instance-name next-hop-address ] [ preference preference-value ]
```

```
ipv6 route-static vpn-instance s-vpn-instance-name<1-6> ipv6-address prefix-length { interface-type interface-number [ next-hop-address ] | next-hop-address [ public ] } [ vpn-instance d-vpn-instance-name next-hop-address ] [ preference preference-value ]
```

New syntax

```
ipv6 route-static ipv6-address prefix-length { interface-type interface-number [ next-hop-address ] | next-hop-address } [ vpn-instance d-vpn-instance-name next-hop-address ] [ preference preference-value ] [ tag tag-value ] [ description description-text ]
```

```
ipv6 route-static vpn-instance s-vpn-instance-name<1-6> ipv6-address prefix-length { interface-type interface-number [ next-hop-address ] | next-hop-address [ public ] } [ vpn-instance d-vpn-instance-name next-hop-address ] [ preference preference-value ] [ tag tag-value ] [ description description-text ]
```

Views

System view

Change description

The **tag** *tag-value* and **description** *description-text* options were added.

- **tag** *tag-value*: Configures a tag for an IPv6 static route, in the range of 1 to 4294967295. The default is 0. Tags of routes are used for route control in routing policies.
- **description** *description-text*: Configures a description for an IPv6 static route. The description is a string of 1 to 60 characters, including special characters such as the space, but excluding the question mark (?).

R5501P02

This release has the following changes:

- New feature: 802.1X voice VLAN
- New feature: Configuring the uplink port to permit multiple isolate-user-VLANs
- New feature: TCP fragment attack protection
- New feature: Support for BPDU guard configuration in interface or port group view
- New feature: MAC re-authentication timer for users in guest VLAN
- New feature: Specifying the IPv4/IPv6 VRRP version
- New feature: MAC and port uniqueness check by the DHCP snooping device
- Modified feature: Auto status transition of dynamic secure MAC addresses
- Modified feature: The maximum number of gateways supported in MFF automatic mode
- Modified feature: Username request timeout timer for 802.1X authentication

New feature: 802.1X voice VLAN

Configuring an 802.1X voice VLAN

You can configure an 802.1X voice VLAN on an 802.1X-enabled port that connects to a voice terminal. The 802.1X voice VLAN feature is effective only on voice terminals that support VLAN-tagged packets.

The 802.1X voice VLAN feature works with a remote authentication server. The device uses the following process to implement this feature:

1. Identifies a voice terminal from the packet sent by the authentication server when the terminal passes 802.1X authentication. The authentication server identifies the terminal type by information such as its OUI and user account, and then sends the terminal type information to the device.
2. Assigns the port to the configured voice VLAN as a tagged member and sends the voice VLAN information through an LLDP or CDP packet to the terminal.

A voice terminal is not associated with a specific voice VLAN. The voice VLAN assigned to the voice terminal depends on the voice VLAN configuration on the access port.

Configuration guidelines

When you configure an 802.1X voice VLAN, follow these guidelines:

- You can configure only one 802.1X voice VLAN on a port. The 802.1X voice VLANs on different ports can be different.
- To ensure a correct exchange of 802.1X EAPOL packets, you must configure the **dot1x eapol untag** command. For information about how to configure this command, see *HP 5500 HI Switch Series Security Configuration Guide-Release 52xx*.
- A server-assigned authorization VLAN for a voice terminal takes precedence over the 802.1X voice VLAN. The port will be assigned to the authorization VLAN if both VLANs coexist. For information about 802.1 X VLAN manipulations, see *HP 5500 HI Switch Series Security Configuration Guide-Release 52xx*.
- This feature cannot work with the RADIUS server provided by IMC.

Configuration prerequisites

Before you configure this feature, complete the following tasks:

- Enable 802.1X on the port.
- Set the port type to hybrid or trunk, because the port is assigned to the 802.1X voice VLAN as a tagged member. For information about port types, see *HP 5500 HI Switch Series Layer 2—LAN Switching Configuration Guide-Release 52xx*.
- Configure LLDP or CDP compatibility on the device. For information about the LLDP and CDP compatibility features, see *HP 5500 HI Switch Series Layer 2—LAN Switching Configuration Guide-Release 52xx*.

Configuration procedure

To configure an 802.1X voice VLAN on a port:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure an 802.1X voice VLAN on the port.	dot1x voice vlan <i>vlan-id</i>	By default, no 802.1X voice VLAN is configured on a port.

Command reference

New command: dot1x voice vlan

Use **dot1x voice vlan** to configure an 802.1X voice VLAN on a port.

Use **undo dot1x voice vlan** to remove the 802.1X voice VLAN on a port.

Syntax

dot1x voice vlan *vlan-id*

undo dot1x voice vlan

Default

No 802.1X voice VLAN is configured on a port.

Views

Ethernet interface view

Default command level

2: System level

Parameters

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

Usage guidelines

This command must function with a remote authentication server (for example, FreeRADIUS). It cannot work with the RADIUS server provided by IMC.

To ensure a correct exchange of 802.1X EAPOL packets, you must configure the **dot1x eapol untag** command. For information about how to configure this command, see *HP 5500 HI Switch Series Security Configuration Guide-Release 52xx*.

The server-assigned authorization VLAN takes precedence over the 802.1X voice VLAN on a port. The port will be assigned to the authorization VLAN if both VLANs coexist. For information about 802.1 X VLAN manipulations, see *HP 5500 HI Switch Series Security Configuration Guide-Release 52xx*.

Before you configure an 802.1X voice VLAN on a port, perform the following tasks:

- Enable 802.1X on the port.
- Set the port type to hybrid or trunk, because the port is assigned to the 802.1X voice VLAN as a tagged member. For information about port types, see *HP 5500 HI Switch Series Layer 2—LAN Switching Configuration Guide-Release 52xx*.
- Configure LLDP or CDP compatibility on the device. For information about the LLDP and CDP compatibility features, see *HP 5500 HI Switch Series Layer 2—LAN Switching Configuration Guide-Release 52xx*.

Examples

Configure VLAN 20 as the 802.1X voice VLAN on GigabitEthernet 1/0/1.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] dot1x voice vlan 20
```

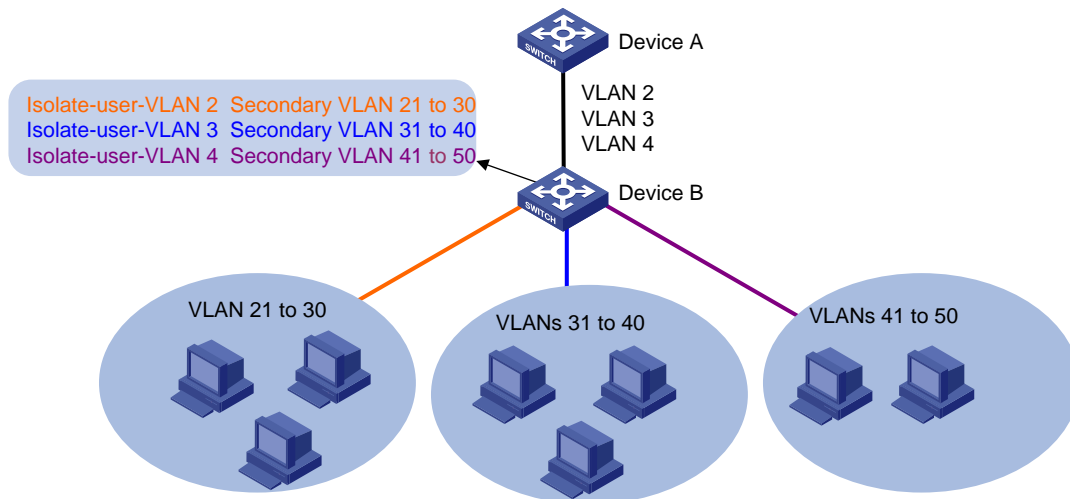
New feature: Configuring the uplink port to permit multiple isolate-user-VLANs

Configuring the uplink port to permit multiple isolate-user-VLANs

Overview

This feature configures the uplink port of a switch to permit packets from multiple isolate-user-VLANs to pass through tagged. As shown in [Figure 2](#), VLANs 2, 3, and 4 are configured as isolate-user-VLANs on Device B. Secondary VLANs 21 through 30 are associated with isolate-user-VLAN 2, secondary VLANs 31 through 40 are associated with isolate-user-VLAN 3, and secondary VLANs 41 through 50 are associated with isolate-user-VLAN 4. Packets from isolate-user-VLANs 2, 3, and 4 pass through the uplink port (the port connecting Device B to Device A in [Figure 2](#)) tagged. Device A identifies only VLANs 2, 3, and 4.

Figure 4 Application scenario



Configuration procedure

To configure the uplink port to permit packets from multiple isolate-user-VLANs to pass through tagged:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a VLAN and enter VLAN view.	vlan <i>vlan-id</i>	N/A
3. Configure the VLAN as an isolate-user-VLAN.	isolate-user-vlan enable	By default, no isolate-user-VLAN exists.
4. Return to system view.	quit	N/A
5. Configure multiple VLANs in batch.	vlan { <i>vlan-id1</i> [to <i>vlan-id2</i>] all }	N/A
6. Isolate ports in the same secondary VLAN at Layer 2.	isolated-vlan enable	Optional. By default, ports in the same secondary VLAN can communicate with each other at Layer 2. This configuration takes effect only after the ports in the secondary VLAN are configured to operate in host mode and the secondary VLAN is associated with an isolate-user-VLAN.
7. Return to system view.	quit	N/A

Step	Command	Remarks
8. Configure the uplink port.	<ol style="list-style-type: none"> Enter Layer-2 Ethernet interface view or Layer-2 aggregate interface view: interface <i>interface-type</i> <i>interface-number</i> Configure the port to operate in promiscuous mode in the specified VLANs: port isolate-user-vlan <i>vlan-list</i> trunk promiscuous 	By default, a port does not operate in promiscuous mode.
9. Configure the downlink port.	<ol style="list-style-type: none"> Enter Layer-2 Ethernet interface view or Layer-2 aggregate interface view: interface <i>interface-type</i> <i>interface-number</i> (Optional.) Configure the link type of the port: port link-type { access hybrid trunk } Assign the downlink port to the specified secondary VLANs (use one of the commands depending on the link type): port access vlan <i>vlan-id</i> Or port trunk permit vlan { <i>vlan-list</i> all } Or port hybrid vlan <i>vlan-list</i> { tagged untagged } Configure the downlink port to operate in host mode: port isolate-user-vlan host 	By default, a port does not operate in host mode.
10. Return to system view.	quit	N/A
11. Associate the specified secondary VLANs with an isolate-user-VLAN.	isolate-user-vlan <i>isolate-user-vlan-id</i> secondary <i>secondary-vlan-id</i> [to <i>secondary-vlan-id</i>]	By default, no isolate-user-VLAN is associated with a secondary VLAN.

CAUTION:

The **port isolate-user-vlan** *vlan-list* **trunk promiscuous** command and the **port isolate-user-vlan** *vlan-id* **promiscuous** command are mutually exclusive. The two commands are different as follows:

- The former configures a port to permit packets from multiple isolate-user-VLANs to pass through tagged.
- The latter configures a port to permit packets from only one isolate-user-VLAN to pass through untagged.

NOTE:

For more information about the isolate-user-VLAN configuration, see *Layer 2—LAN Switching Configuration Guide*.

Configuration example

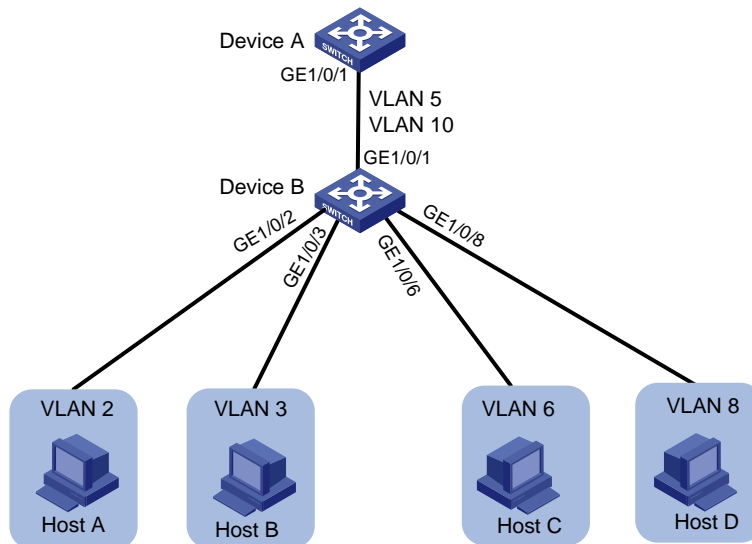
Network requirements

As shown in [Figure 3](#), Device B is attached to Device A.

Configure the isolate-user-VLAN feature, so that:

- VLAN 5 and VLAN 10 are isolate-user-VLANs on Device B. The uplink port GigabitEthernet 1/0/1 permits packets from VLANs 5 and 10 to pass through tagged.
- On Device B, the downlink port GigabitEthernet 1/0/2 permits secondary VLAN 2 and the downlink port GigabitEthernet 1/0/3 permits VLAN 3. Secondary VLANs 2 and 3 are associated with isolate-user-VLAN 5.
- On Device B, the downlink port GigabitEthernet 1/0/6 permits secondary VLAN 6 and the downlink port GigabitEthernet 1/0/8 permits VLAN 8. Secondary VLANs 6 and 8 are associated with isolate-user-VLAN 10.
- Device A identifies only VLANs 5 and 10 on Device B.

Figure 5 Network diagram



Configuration procedure

1. Configure Device B:

Configure VLAN 5 and VLAN 10 as isolate-user-VLANs.

```
<DeviceB> system-view
[DeviceB] vlan 5
[DeviceB-vlan5] isolate-user-vlan enable
[DeviceB-vlan5] quit
[DeviceB] vlan 10
[DeviceB-vlan10] isolate-user-vlan enable
[DeviceB-vlan10] quit
```

Create VLANs 2, 3, 6, and 8.

```
[DeviceB] vlan 2 to 3
[DeviceB] vlan 6
[DeviceB-vlan6] quit
[DeviceB] vlan 8
[DeviceB-vlan8] quit
```

Configure the uplink port GigabitEthernet 1/0/1 to operate in promiscuous mode in VLANs 5 and 10.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port isolate-user-vlan 5 10 trunk promiscuous
[DeviceB-GigabitEthernet1/0/1] quit
```

Assign the downlink port GigabitEthernet 1/0/2 to VLAN 2, and configure the port to operate in host mode in VLAN 2. Assign the downlink port GigabitEthernet 1/0/3 to VLAN 3, and configure the port to operate in host mode in VLAN 3.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port access vlan 2
[DeviceB-GigabitEthernet1/0/2] port isolate-user-vlan host
[DeviceB-GigabitEthernet1/0/2] quit
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port access vlan 3
[DeviceB-GigabitEthernet1/0/3] port isolate-user-vlan host
[DeviceB-GigabitEthernet1/0/3] quit
```

Associate secondary VLANs 2 and 3 with isolate-user-VLAN 5.

```
[DeviceB] isolate-user-vlan 5 secondary 2 to 3
```

Assign the downlink port GigabitEthernet 1/0/6 to VLAN 6, and configure the port to operate in host mode in VLAN 6. Assign the downlink port GigabitEthernet 1/0/8 to VLAN 8, and configure the port to operate in host mode in VLAN 8.

```
[DeviceB] interface gigabitethernet 1/0/6
[DeviceB-GigabitEthernet1/0/6] port access vlan 6
[DeviceB-GigabitEthernet1/0/6] port isolate-user-vlan host
[DeviceB-GigabitEthernet1/0/6] quit
[DeviceB] interface gigabitethernet 1/0/8
[DeviceB-GigabitEthernet1/0/8] port access vlan 8
[DeviceB-GigabitEthernet1/0/8] port isolate-user-vlan host
[DeviceB-GigabitEthernet1/0/8] quit
```

Associate secondary VLANs 6 and 8 with isolate-user-VLAN 10.

```
[DeviceB] isolate-user-vlan 10 secondary 6 8
```

2. Configure Device A:

Create VLAN 5 and VLAN 10.

```
[DeviceA] vlan 5
[DeviceA-vlan5] quit
[DeviceA] vlan 10
[DeviceA-vlan10] quit
```

Configure GigabitEthernet 1/0/1 as a hybrid port, and configure the port to permit the packets from VLAN 5 and VLAN 10 to pass through tagged.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type hybrid
[DeviceA-GigabitEthernet1/0/1] port hybrid vlan 5 10 tagged
[DeviceA-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Display the configuration of isolate-user-VLAN 5. (The output for isolate-user-VLAN 10 is similar.)

```
[DeviceB] display isolate-user-vlan 5
Isolate-user-VLAN VLAN ID : 5
Secondary VLAN ID : 2-3
```

```
VLAN ID: 5
VLAN Type: static
Isolate-user-VLAN type : isolate-user-VLAN
```

```

Route Interface: not configured
Description: VLAN 0005
Name: VLAN 0005
Tagged   Ports:
    GigabitEthernet1/0/1
Untagged Ports:
    GigabitEthernet1/0/2          GigabitEthernet1/0/3

VLAN ID: 2
VLAN Type: static
Isolate-user-VLAN type : secondary
Route Interface: not configured
Description: VLAN 0002
Name: VLAN 0002
Tagged   Ports:
    GigabitEthernet1/0/1
Untagged Ports:
    GigabitEthernet1/0/2

VLAN ID: 3
VLAN Type: static
Isolate-user-VLAN type : secondary
Route Interface: not configured
Description: VLAN 0003
Name: VLAN 0003
Tagged   Ports:
    GigabitEthernet1/0/1
Untagged Ports:
    GigabitEthernet1/0/3

```

Command reference

port isolate-user-vlan trunk promiscuous

Use **port isolate-user-vlan *vlan-list* trunk promiscuous** to configure a port to operate in promiscuous mode in the specified VLANs and assign the port to the specified VLANs as a tagged member. If the specified VLANs are isolate-user-VLANs associated with existing secondary VLANs, this command automatically assigns the port to the associated secondary VLANs as a tagged member. You can configure the specified VLANs as isolate-user-VLANs before or after you execute this command.

Use **undo port isolate-user-vlan *vlan-list* trunk promiscuous** to remove the port from the specified VLANs and disable the promiscuous mode for the port in the specified VLANs. However, this command does not remove the port from the associated secondary VLANs or change the link type and PVID of the port. When the promiscuous mode is disabled for the port in all isolate-user-VLANs, the port does not operate in promiscuous mode in any VLAN.

Syntax

port isolate-user-vlan *vlan-list* trunk promiscuous

undo port isolate-user-vlan *vlan-list* trunk promiscuous

Default

A port does not operate in promiscuous mode in any VLAN.

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default command level

2: System level

Parameters

vlan-list: Specifies multiple isolate-user-VLANs in the format of *vlan-list* = { *vlan-id1* [**to** *vlan-id2*] }&<1-10>, where *vlan-id1* and *vlan-id2* each range from 1 to 4094, *vlan-id1* cannot be greater than *vlan-id2*, and &<1-10> indicates that you can specify up to ten *vlan-id1* [**to** *vlan-id2*] parameters.

Usage guidelines

When you execute the **port isolate-user-vlan *vlan-list* trunk promiscuous** command, follow these guidelines:

- If the port is an access port, this command configures the link type as hybrid, and keeps the PVID configuration; if the port is a trunk or hybrid port, this command does not change the link type and PVID configuration of the port.
- If the link type of the port has been hybrid or is changed from access to hybrid by this command, this command automatically assigns the port to the specified VLANs and the associated secondary VLANs as a tagged member (if the port has been assigned to some of the specified VLANs and the associated secondary VLANs as an untagged member, this command does not change untagged membership).

The **port isolate-user-vlan *vlan-list* trunk promiscuous** command is mutually exclusive with the **port isolate-user-vlan *vlan-id* promiscuous** command and the **port isolate-user-vlan host** command.

Examples

Configure the access port GigabitEthernet 1/0/1 to operate in promiscuous mode in isolate-user-VLANs 2 and 3, which are associated with VLANs 20 and 30, respectively. Then, disable the promiscuous mode for GigabitEthernet 1/0/1 in isolate-user-VLANs 2 and 3.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
#
return
[Sysname-GigabitEthernet1/0/1] port isolate-user-vlan 2 3 trunk promiscuous
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port isolate-user-vlan 2 3 trunk promiscuous
 port link-type hybrid
 port hybrid vlan 2 3 20 30 tagged
 port hybrid vlan 1 untagged
#
```

```

return
[Sysname-GigabitEthernet1/0/1] undo port isolate-user-vlan 2 3 trunk promiscuous
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
    port link-mode bridge
    port link-type hybrid
    port hybrid vlan 20 30 tagged
    port hybrid vlan 1 untagged
#
return
# VLAN 10 is not an isolate-user-VLAN. Configure the access port GigabitEthernet 1/0/1 to
operate in promiscuous mode in VLAN 10. Then, disable the promiscuous mode configuration
for GigabitEthernet 1/0/1 in VLAN 10.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
    port link-mode bridge
#
return
[Sysname-GigabitEthernet1/0/1] port isolate-user-vlan 10 trunk promiscuous
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
    port link-mode bridge
    port isolate-user-vlan 10 trunk promiscuous
    port link-type hybrid
    port hybrid vlan 10 tagged
    port hybrid vlan 1 untagged
#
return
[Sysname-GigabitEthernet1/0/1] undo port isolate-user-vlan 10 trunk promiscuous
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
    port link-mode bridge
    port link-type hybrid
    port hybrid vlan 1 untagged
#
Return

```


New feature: TCP fragment attack protection

Enabling TCP fragment attack protection

The TCP fragment attack protection function enables the device to drop attack TCP fragments to prevent TCP fragment attacks. As defined in RFC 1858, attack TCP fragments refer to the following TCP fragments:

- First fragments in which the TCP header is smaller than 20 bytes.
- Non-first fragments with a fragment offset of 8 bytes (FO=1).

Traditional packet filter on the device detects the source and destination IP addresses, source and destination ports, and transport layer protocol of the first fragment of a TCP packet. If the first fragment passes the detection, all subsequent fragments of the TCP packet are allowed to pass through. An attacker can launch TCP fragment attacks through either of the following ways:

- Make the first fragment small enough to force some TCP header fields into the second fragment and set TCP flags illegally in the second fragment.
- Fabricate a non-first fragment in which the fragment offset is set to 8 bytes and the TCP flags are set differently and illegally from those in the first fragment. When the receiving host reassembles the fragments, the illegal TCP flags in the non-first fragment overwrite the legal TCP flags in the first fragment.

Because the first fragment does not hit any match in the packet filter, the subsequent fragments can all pass through. After the receiving host reassembles the fragments, a TCP fragment attack occurs.

To enable TCP fragment attack protection:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable TCP fragment attack protection.	attack-defense tcp fragment enable	By default, TCP fragment attack protection is enabled.

Command reference

attack-defense tcp fragment enable

Use **attack-defense tcp fragment enable** to enable TCP fragment attack protection.

Use **undo attack-defense tcp fragment enable** to disable TCP fragment attack protection.

Syntax

attack-defense tcp fragment enable

undo attack-defense tcp fragment enable

Default

TCP fragment attack protection is enabled.

Views

System view

Default command level

2: System level

Usage guidelines

This command enables the device to drop attack TCP fragments to prevent TCP fragment attacks.

Examples

```
# Enable TCP fragment attack protection.  
<Sysname> System-view  
[Sysname] attack-defense tcp fragment enable
```

New feature: Support for BPDU guard configuration in interface or port group view

Configuring BPDU guard for an interface or port group

Before this feature was introduced, the device supported only global BPDU guard configuration (**stp bpduguard**). Global BPDU guard configuration takes effect on all edge ports. Edge ports are configured by using the **stp edged-port enable** command.

This feature allows you to perform the following tasks:

- Enable BPDU guard for an interface or port group when BPDU guard is globally disabled.
- Disable BPDU guard for an interface or port group when BPDU guard is globally enabled.

You must enable BPDU guard on a port that directly connects to a user terminal rather than another device or shared LAN segment.

Enabling BPDU guard for an interface or port group when BPDU guard is globally disabled

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view or port group view.	<ul style="list-style-type: none">• Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: interface <i>interface-type interface-number</i>• Enter port group view: port-group manual <i>port-group-name</i>	Use one of the commands.
3. Enable BPDU guard.	stp port bpduguard enable	BPDU guard is disabled on all interfaces if it is globally disabled. By default, BPDU guard is globally disabled.

Disabling BPDU guard for an interface or port group when BPDU guard is globally enabled

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Disable BPDU guard globally.	stp bpduguard	By default, BPDU guard is globally disabled.

Step	Command	Remarks
3. Enter interface view or port group view.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: interface <i>interface-type</i> <i>interface-number</i> Enter port group view: port-group manual <i>port-group-name</i> 	Use one of the commands.
4. Disable BPDU guard.	stp port bpdu-protection disable	By default, BPDU guard is enabled on all edge ports if it is globally enabled.

Command reference

New command: stp port bpdu-protection

Use **stp port bpdu-protection** to configure BPDU guard on an interface.

Use **undo stp port bpdu-protection** to restore the default.

Syntax

stp port bpdu-protection { enable | disable }

undo stp port bpdu-protection

Default

BPDU guard is not configured on an interface. For an edge port, BPDU guard is enabled on the port if the function is globally enabled. BPDU guard is disabled on the port if the function is disabled globally.

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default command level

2: System level

Parameters

enable: Enables BPDU guard on the interface.

disable: Disables BPDU guard on the interface.

Usage guidelines

When the setting is configured in Layer 2 Ethernet interface view, it takes effect on only that interface.

When the setting is configured in Layer 2 aggregate interface view, it takes effect on only the aggregate interface.

When the setting is configured in port group view, it takes effect on all ports in the port group.

When the setting is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Enable BPDU guard on GigabitEthernet 1/0/1.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] stp port bpdu-protection enable
```

Related commands

- **stp bpdu-protection**
- **stp edged-port**

For more information about these commands, see spanning tree commands in *Layer 2—LAN Switching Command Reference*.

New feature: MAC re-authentication timer for users in guest VLAN

Configuring MAC re-authentication timer for users in guest VLAN

The MAC re-authentication timer sets the interval that the device must wait before it can re-authenticate a user in the MAC authentication guest VLAN.

The device handles VLANs for users in the MAC authentication guest VLAN based on the following rules:

Authentication status	VLAN manipulation
A user fails MAC re-authentication because of unreachable servers.	<ul style="list-style-type: none">• If a MAC authentication critical VLAN is available, the device assigns the user to the critical VLAN.• If no MAC authentication critical VLAN is configured, the user is still in the MAC authentication guest VLAN. The MAC re-authentication timer restarts for the user.
A user fails MAC re-authentication for any other reasons except for unreachable servers.	The user is still in the MAC authentication guest VLAN. The MAC re-authentication timer restarts for the user.
A user passes MAC re-authentication.	<ul style="list-style-type: none">• The device removes the user from the MAC authentication guest VLAN and assigns the user to the authorization VLAN.• If the authentication server does not authorize a VLAN, the user is assigned to the initial VLAN. The initial VLAN refers to the VLAN to which the user belongs before it was assigned to the MAC authentication guest VLAN.

To configure the MAC re-authentication timer for users in the MAC authentication guest VLAN:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the MAC authentication guest VLAN on the port.	mac-authentication guest-vlan <i>vlan-id</i>	By default, no guest VLAN is configured on the port.
4. Return to system view.	quit	N/A
5. Configure the MAC re-authentication timer for users in the guest VLAN.	mac-authentication timer guest-vlan-reauth <i>interval</i>	The default timer is 30 seconds.

Command reference

mac-authentication timer guest-vlan-reauth

Use **mac-authentication timer guest-vlan-reauth** to set the MAC re-authentication timer for users in the MAC authentication guest VLAN.

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

Syntax

mac-authentication timer guest-vlan-reauth *interval*

undo mac-authentication timer guest-vlan-reauth

Default

The MAC re-authentication timer is 30 seconds for users in the MAC authentication guest VLAN.

Views

System view

Default command level

2: System view

Parameters

interval: Set the MAC re-authentication timer for users in the MAC authentication guest VLAN. The value range for this argument is 1 to 3600, in seconds.

Usage guidelines

When the MAC re-authentication timer expires, the device re-authenticates the users in the MAC authentication guest VLAN.

The device handles VLANs for users in the MAC authentication guest VLAN based on the following rules:

Authentication status	VLAN manipulation
A user fails MAC re-authentication because of unreachable servers.	<ul style="list-style-type: none">If a MAC authentication critical VLAN is available, the device assigns the user to the critical VLAN.If no MAC authentication critical VLAN is configured, the user is still in the MAC authentication guest VLAN. The MAC re-authentication timer restarts for the user.
A user fails MAC re-authentication for any other reasons except for unreachable servers.	The user is still in the MAC authentication guest VLAN. The MAC re-authentication timer restarts for the user.
A user passes MAC re-authentication.	<ul style="list-style-type: none">The device removes the user from the MAC authentication guest VLAN and assigns the user to the authorization VLAN.If the authentication server does not authorize a VLAN, the user is assigned to the initial VLAN. The initial VLAN refers to the VLAN to which the user belongs before it was assigned to the MAC authentication guest VLAN.

Examples

Set the MAC re-authentication timer to 60 seconds for users in the MAC authentication guest VLAN.

```
<Sysname> system-view
```

```
[Sysname] mac-authentication timer guest-vlan-reauth 60
```

New feature: Specifying the IPv4/IPv6 VRRP version

Specifying the IPv4/IPv6 VRRP version

The VRRP version on all routers in a VRRP group must be the same.

If you specify VRRPv3 as the version for an interface, the authentication configuration on the VRRP group does not take effect.

VRRPv3 supports a maximum advertisement interval of 4095 centiseconds. If you configure an advertisement interval that is greater than 4095 centiseconds, the advertisement interval of 4095 centiseconds applies.

To specify the version of IPv4/IPv6 VRRP:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Specify the version of VRRP.	vrrp version <i>version-number</i>	By default, VRRPv2 is used.

Command reference

vrrp version

Use **vrrp version** to specify the version of VRRP on an interface.

Use **undo vrrp version** to restore the default.

Syntax

vrrp version *version-number*

undo vrrp version

Default

VRRPv2 is used.

Views

Interface view

Default command level

2: System level

Parameters

version-number: Specifies a VRRP version. The version number is 2 or 3. For more information, see the following table:

Value	VRRP version	RFC	Value of the version field in VRRP packets
2	IPv4 VRRPv2	RFC 2338	<ul style="list-style-type: none">2 in standard protocol mode.8 in load balancing mode.
	IPv6 VRRPv2	RFC 3768	<ul style="list-style-type: none">3 in standard protocol mode.9 in load balancing mode.

Value	VRRP version	RFC	Value of the version field in VRRP packets
3	IPv4/IPv6 VRRPv3	RFC 5798	3 in standard protocol mode or load balancing mode.

NOTE:

The IPv6 VRRP packet format is not defined in RFC 3768. HP implemented IPv6 VRRPv2 based on RFC 3768.

Usage guidelines

The version of VRRP on all routers in a VRRP group must be the same.

If you specify VRRPv3 as the version for an interface, the authentication configuration on the VRRP group does not take effect.

For VRRPv3, if you configure an advertisement interval that is greater than 4095 centiseconds, the advertisement interval of 4095 centiseconds applies.

Examples

Specify VRRPv3 to run on VLAN-interface 2.

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 2
```

```
[Sysname-Vlan-interface2] vrrp version 3
```

New feature: MAC and port uniqueness check by the DHCP snooping device

Enabling MAC and port uniqueness check on the DHCP snooping device

This function allows the DHCP snooping device to maintain only one DHCP snooping entry for the same client's MAC address in one VLAN.

When receiving a DHCP REQUEST, the DHCP snooping device checks for a DHCP snooping entry that matches the client's MAC address (the **chaddr** field in the request). If an entry exists with the same MAC address and VLAN but different receiving port, the device updates the entry. When DHCP snooping entries are used by security modules, such as IP source guard, this function prevents clients from using the same MAC address to apply for multiple IP addresses.

To enable MAC and port uniqueness check on the DHCP snooping device:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable MAC and port uniqueness check on the DHCP snooping device.	dhcp-snooping check mac-port	By default, MAC and port uniqueness check is disabled on the DHCP snooping device.

Command reference

dhcp-snooping check mac-port

Use **dhcp-snooping check mac-port** to enable MAC and port uniqueness check on the DHCP snooping device.

Use **undo dhcp-snooping check mac-port** to disable MAC and port uniqueness check on the DHCP snooping device.

Syntax

dhcp-snooping check mac-port

undo dhcp-snooping check mac-port

Default

MAC and port uniqueness check is disabled on the DHCP snooping device.

Views

System view

Default command level

2: System level

Examples

Enable MAC and port uniqueness check on the DHCP snooping device.

```
<Sysname> system-view
```

```
[Sysname] dhcp-snooping check mac-port
```

Modified feature: Auto status transition of dynamic secure MAC addresses

Feature change description

Before modification: A dynamic secure MAC address entry will not be deleted if the port for the entry goes down.

After modification: The status of dynamic secure MAC address entries transits automatically based on the port status. The device deletes a dynamic secure MAC address entry if the port for the entry goes down. This MAC address is reported as an unknown source MAC address if it is detected on another port.

Command changes

None.

Modified feature: The maximum number of gateways supported in MFF automatic mode

Feature change description

In MFF automatic mode, the maximum number of gateways that can be learned in a VLAN was changed from 20 to 64. No more gateways can be learned when the limit is reached.

Command changes

None.

Modified feature: Username request timeout timer for 802.1X authentication

Feature change description

The minimum value for the 802.1X username request timeout timer was changed from 10 seconds to 1 second. This modification allows the device to send EAP-Request/Identity packets to initiate 802.1X authentication at a shorter interval.

Command changes

Modified command: dot1x timer

Syntax

dot1x timer tx-period *tx-period-value*

Views

System view

Change description

Before modification: The value range for the *tx-period-value* argument is 10 to 120 seconds.

After modification: The value range for the *tx-period-value* argument is 1 to 120 seconds.

R5501P01

This release has the following changes:

- [New feature: Discarding IPv6 packets that contain extension headers](#)
- [Modified feature: Configuring IGMP SSM mappings](#)
- [Modified feature: Configuring MLD SSM mappings](#)

New feature: Discarding IPv6 packets that contain extension headers

Enabling a device to discard IPv6 packets that contain extension headers

This feature enables a device to discard a received IPv6 packet in either of the following situations:

- The packet contains a Hop-by-Hop Options header.
- The packet contains two or more extension headers.

To enable a device to discard IPv6 packets that contain extension headers:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the device to discard IPv6 packets that contain extension headers.	ipv6 option drop enable	By default, the device does not discard IPv6 packets that contain extension headers.

Command reference

New command: ipv6 option drop enable

Use **ipv6 option drop enable** to enable the device to discard IPv6 packets that contain extension headers.

Use **undo ipv6 option drop** to disable the device from discarding IPv6 packets that contain extension headers.

Syntax

ipv6 option drop enable

undo ipv6 option drop

Default

A device does not discard IPv6 packets that contain extension headers.

Views

System view

Default command level

2: System level

Usage guidelines

This feature enables a device to discard a received IPv6 packet in either of the following situations:

- The packet contains a Hop-by-Hop Options header.
- The packet contains two or more extension headers.

Examples

```
# Enable the device to discard IPv6 packets that contain extension headers.
```

```
<Sysname> system-view
```

```
[Sysname] ipv6 option drop enable
```

Modified feature: Configuring IGMP SSM mappings

Feature change description

Before modification: The IGMP SSM mapping feature processes only IGMPv1 and IGMPv2 reports but not IGMPv3 reports. When an IGMPv1 or IGMPv2 report arrives at a device that is configured with IGMP SSM mappings, the device examines the multicast address G in the report:

- If G is not in the configured SSM group range, the device provides the ASM service.
- If G is in the configured SSM group range but does not match any IGMP SSM mappings, the device discards the report.
- If G is in the configured SSM group range and matches an IGMP SSM mapping, the device provides the SSM service. The (*, G) information in the report is translated into (G, INCLUDE, (S1, S2, ...)) information for the SSM service.

After modification: The IGMP SSM mapping feature can process IGMPv1 reports and IGMPv2 reports. In addition, it can also process IGMPv3 reports that contain an empty EXCLUDE source address list. The device processes these IGMPv3 reports in the same way IGMPv1 and IGMPv2 reports are processed.

Command changes

None.

Modified feature: Configuring MLD SSM mappings

Feature change description

Before modification: The MLD SSM mapping feature processes only MLDv1 reports but not MLDv2 reports. When an MLDv1 report arrives at a device that is configured with MLD SSM mappings, the device examines the IPv6 multicast address G in the report:

- If G is not in the configured SSM group range, the device provides the ASM service.
- If G is in the configured SSM group range but does not match any MLD SSM mappings, the device discards the report.
- If G is in the configured SSM group range and matches an MLD SSM mapping, the device provides the SSM service. The (*, G) information in the report is translated into (G, INCLUDE, (S1, S2, ...)) information for the SSM service.

After modification: The MLD SSM mapping feature can process MLDv1 reports. In addition, it can also process MLDv2 reports that contain an empty EXCLUDE source address list. The device processes these MLDv2 reports in the same way MLDv1 reports are processed.

Command changes

None.

R5501

This release has the following changes:

- New feature: OpenFlow
- Modified feature: Setting the device name
- Modified feature: Specifying multiple public keys for an SSH user
- Modified feature: Disabling an untrusted port from recording clients' IP-to-MAC bindings
- Modified feature: ARP packet rate limit
- Modified feature: Specifying the username and password to log in to the SCP server
- Modified feature: Customizing DHCP options
- Modified feature: ACL-based packet filtering on a VLAN interface

New feature: OpenFlow

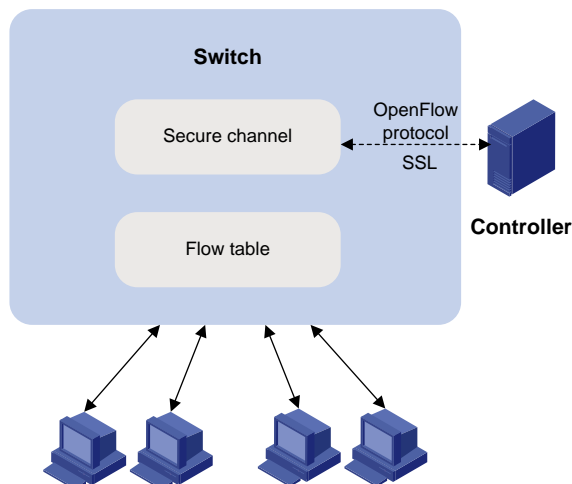
Software-Defined Networking (SDN) was developed to meet the growing requirements of virtualization technologies and data networks. SDN uses software to separate controlling functions from data forwarding, and provides simple, flexible device operations and high extensibility.

OpenFlow is the communication interface between a controller and network devices to implement SDN. With OpenFlow, you can perform centralized data forwarding management for physical and virtual devices.

Overview

OpenFlow separates the data forwarding and routing decision functions. It keeps the flow-based forwarding function and employs a separate controller to make routing decisions. A switch communicates with the controller through a secure channel.

Figure 6 OpenFlow network diagram



Basic concepts

OpenFlow switch

OpenFlow switches are classified into the following types:

- **OpenFlow-only**—Supports only OpenFlow operation.
- **OpenFlow-hybrid**—Supports both OpenFlow operation and traditional Ethernet switching operations. Switches of this series are OpenFlow-hybrid switches.

OpenFlow port

❗ IMPORTANT:

The switch does not support tunnel interfaces and loopback interfaces.

OpenFlow supports the following types of ports:

- **Physical port**—Corresponds to a hardware interface of a switch, such as an Ethernet interface. A physical port can be either an ingress port or an output port.
- **Logical port**—Does not correspond to a hardware interface of a switch and might be defined by non-OpenFlow methods. A logical port can be either an ingress port or an output port.
- **Reserved port**—Defined by OpenFlow to specify forwarding actions. Reserved ports include the following types:
 - **All**—All OpenFlow ports that can be used to forward a packet.
 - **Controller**—OpenFlow controller.
 - **Table**—Flow table.
 - **In_Port**—Packet ingress port.
 - **Any**—Generic port description. The port cannot be used as an ingress port or output port.
 - **Local**—Local CPU.
 - **Normal**—Normal forwarding process.
 - **Flood**—Flooding.

Except the **Any** type, all reserved ports can be used only as output ports.

OpenFlow flow table

An OpenFlow switch matches packets against one or more user-defined flow tables. A flow table consists of flow entries, and packets are matched based on the matching precedence of flow entries.

Figure 7 Components of a flow entry

Match Fields	Priority	Counters	Instructions	Timeouts	Cookie
--------------	----------	----------	--------------	----------	--------

A flow entry contains the following fields:

- **Match fields**—Matching rules of the flow entry. These consist of the ingress port, packet headers, and metadata specified by the previous table.
- **Priority**—Matching precedence of the flow entry. A packet is matched against the table and only the highest priority flow entry that matches the packet is selected.
- **Counters**—Counts of the packets that match the flow entry.
- **Instructions**—To modify the action set or pipeline processing. These include the following types:
 - **Meter**—Directs the packets to the specified meter to limit the rate of the packets.
 - **Apply-Actions**—Applies the specified actions in the action list immediately.
 - **Clear-Actions**—Clears all the actions in the action set immediately.

- **Write-Actions**—Modifies all the actions in the action set immediately.
- **Write-Metadata**—Modifies packets between two flow tables if there are multiple flow tables.
- **Goto-Table**—Indicates the next flow table in the processing line.

Actions are executed in one of the following ways:

- **Action Set**—When the instruction set of a flow entry does not contain a **Goto-Table** instruction, pipeline processing stops and the actions in the action set are executed. An action set contains a maximum of one action of each type.
- **Action List**—The actions in the action list are executed immediately in the order specified by the action list. The effect of those actions is cumulative.
- **Timeouts**—Maximum amount of idle time or hard time for the flow entry.
 - **Idle Time**—The flow entry is removed when it has matched no packets during the idle time.
 - **Hard Time**—The flow entry is removed when the hard time timeout is exceeded, regardless of whether or not it has matched packets.
- **Cookie**—Flow entry identifier specified by the controller.

Every flow table must support a table-miss flow entry to process table misses. The table-miss flow entry specifies how to process packets unmatched by other flow entries in the flow table. The table-miss flow entry wildcards all match fields (all fields omitted) and has the lowest priority 0. The table-miss flow entry behaves in most ways like any other flow entry.

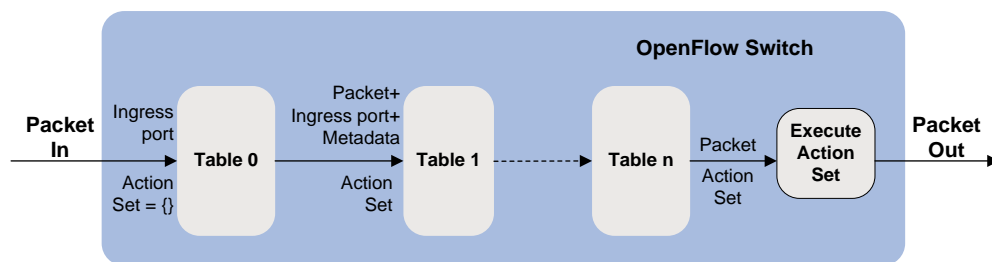
OpenFlow pipeline

The OpenFlow pipeline processing defines how packets interact with flow tables contained by a switch.

The flow tables of an OpenFlow switch are sequentially numbered, starting at 0. The packet is first matched against flow entries of first flow table: flow table 0. A flow entry can only direct a packet to a flow table number which is greater than its own flow table number.

When a packet matches a flow entry, the OpenFlow switch updates the action set for the packet and passes the packet to the next flow table. In the last flow table, the OpenFlow switch executes all actions to modify packet contents and specify the output port for packet forwarding. If the instruction set of one of the flow tables contains an action list, the OpenFlow switch executes the actions to modify a copy of the packet immediately in this table.

Figure 8 OpenFlow forwarding workflow



OpenFlow flow tables include the following types:

- **MAC-IP**—Combines the MAC address table and FIB table.
A MAC-IP flow table provides the following match fields:
 - Destination MAC address
 - VLAN
 - Destination IP address
 A MAC-IP flow table provides the following actions:
 - Modifying the destination MAC address
 - Modifying the source MAC address

- Modifying the VLAN
- Specifying the output port
- **Extensibility**—Provides more matching fields and actions than a MAC-IP flow table does.

Group table

The ability for a flow entry to point to a group enables OpenFlow to represent additional methods of forwarding. A group table consists of group entries.

Figure 9 Components of a group entry

Group Identifier	Group Type	Counters	Action Buckets
------------------	------------	----------	----------------

A group entry contains the following fields:

- **Group Identifier**—A 32 bit unsigned integer uniquely identifying the group.
- **Group Type**—Type of the group.
- **Counters**—Updated when packets are processed by a group.
- **Action Buckets**—An ordered list of action buckets, where each action bucket contains a set of actions to execute and associated parameters.

Meter table

Meters enable OpenFlow to implement various simple QoS operations, such as rate-limiting. A meter table consists of meter entries.

Figure 10 Components of a meter entry

Meter Identifier	Meter Bands	Counters
------------------	-------------	----------

A meter entry contains the following fields:

- **Meter Identifier**—A 32 bit unsigned integer uniquely identifying the meter.
- **Meter Bands**—Each meter can have one or more meter bands. Each band specifies the rate at which the band applies and the way packets should be processed. If the current rate of packets exceeds the rate of multiple bands, the band with the highest configured rate is used.
- **Counters**—Updated when packets are processed by a meter.

Figure 11 Components of a meter band

Band Type	Rate	Counters	Type Specific arguments
-----------	------	----------	-------------------------

A meter band contains:

- **Band Type**—Defines how packets are processed. Packets that exceed the band rate are dropped.
- **Rate**—Used by the meter to select the meter band, defines the lowest rate at which the band can apply.
- **Counters**—Updated when packets are processed by a band.

Type Specific Arguments—Some band types have optional arguments.

OpenFlow instance

You can configure one or more OpenFlow instances on the same device. A controller considers each OpenFlow instance as a separate OpenFlow switch and deploys forwarding instructions to it.

In this chapter, an OpenFlow switch is the same as an OpenFlow instance, unless otherwise specified.

Associated VLAN

When an OpenFlow instance is associated with VLANs, the flow tables take effect on packets only within these VLANs.

Activation and reactivation

The controller can deploy flow entries only to OpenFlow instances that are activated.

An activated OpenFlow instance need be reactivated when any of the following parameters are changed:

- Associated VLANs
- Flow tables
- Maximum number of supported flow entries

After reactivation, the OpenFlow instance is disconnected from all controllers and reconnects to them.

OpenFlow instance port

An OpenFlow switch sends information about the following ports to the controller:

- Physical ports
- Logical ports
- Reserved ports of the local type

These ports belong to the VLANs that are associated with the OpenFlow instance only when all associated VLANs are within the list of the VLANs to which the ports are assigned. However, if the **loosen** mode is used, a port belongs to the OpenFlow instance when VLANs that are associated with the OpenFlow instance overlap with the VLANs to which the port is assigned.

Protocols and standards

OpenFlow Switch Specification Version 1.3.1

OpenFlow configuration task list

Task		Remarks
Configuring OpenFlow instances	Creating an OpenFlow instance	Required.
	Associating an OpenFlow instance with VLANs	
	Configuring flow table IDs	Optional.
	Setting the connection mode for an OpenFlow instance to establish connections to controllers	
	Configuring the maximum number of flow entries	
	Configuring in-band management VLANs	
	Disabling MAC address learning in the VLANs associated with an OpenFlow instance	

Task		Remarks
	Configuring the datapath ID for an OpenFlow instance	
	Activating or reactivating an OpenFlow instance	Required.
Configuring controllers for an OpenFlow switch	Configuring controllers and main connections	Required.
	Setting the connection interruption mode	Optional.
Setting OpenFlow timers		Optional.
Configuring OpenFlow to support dynamic MAC addresses		Optional.

Configuring OpenFlow instances

Creating an OpenFlow instance

Step	Command	Remarks
3. Enter system view.	system-view	N/A
4. Create an OpenFlow instance and enter OpenFlow instance view.	openflow instance <i>instance-id</i>	By default, no OpenFlow instance exists.
5. (Optional.) Specify a description for the OpenFlow instance.	description <i>text</i>	By default, an OpenFlow instance does not have a description.

Associating an OpenFlow instance with VLANs

When you associate an OpenFlow instance with VLANs, follow these guidelines:

- Do not associate multiple OpenFlow instances to the same VLAN. Otherwise, VLAN traffic cannot be correctly processed.
- When you activate an OpenFlow instance that is associated with non-existent VLANs, the system automatically creates the VLANs. Do not delete any of these VLANs after the OpenFlow instance is activated.
- VLANs that are associated with an OpenFlow instance cannot contain loopback interfaces.

To associate an OpenFlow instance with VLANs:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter OpenFlow instance view.	openflow instance <i>instance-id</i>	N/A
3. Associate the OpenFlow instance with VLANs.	classification vlan <i>vlan-id</i> [mask <i>vlan-mask</i>] [loosen]	By default, an OpenFlow instance is not associated with any VLAN.

Configuring flow table IDs

You can configure one MAC-IP flow table and one extensibility flow table for an OpenFlow instance, and the MAC-IP flow table ID must be smaller than the extensibility flow table ID.

To configure flow table IDs for an OpenFlow instance:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter OpenFlow instance view.	openflow instance <i>instance-id</i>	N/A
3. Configure the flow table ID.	flow-table { <i>extensibility</i> <i>table-id</i> <i>mac-ip</i> <i>table-id</i> } *	By default, OpenFlow supports only one flow table with an ID of 0, which is the extensibility type.

Setting the connection mode for an OpenFlow instance to establish connections to controllers

The following connection modes are available for an OpenFlow instance to establish connections to controllers:

- **single**—When the connection mode is **single**, an OpenFlow establishes a connection to only one controller at a time, and the other controllers back up the controller. When the current connection is broken, the OpenFlow instance attempts to connect to the next controller until it successfully establishes a connection.
- **multiple**—When the connection mode is **multiple**, an OpenFlow can establish connections to multiple controllers at a time. When the OpenFlow instance fails to connect to a controller or the connection to a controller is broken, the OpenFlow instance attempts to reconnect to the controller after the reconnection interval expires until it successfully establishes a connection to the controller.

To set the connection mode for an OpenFlow instance to establish connections to controllers:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter OpenFlow instance view.	openflow instance <i>instance-id</i>	N/A
3. Set the connection mode for the OpenFlow instance to establish connections to controllers.	controller mode { multiple single }	By default, the connection mode is multiple .

Configuring the maximum number of flow entries

To improve OpenFlow availability, extensibility flow table can have a maximum number of flow entries. When entries in a table reaches the maximum number, the OpenFlow instance does not accept new flow entries for that table and sends a deployment failure notification to the controller.

To configure the maximum number of flow entries that each extensibility flow table supports:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter OpenFlow instance view.	openflow instance <i>instance-id</i>	N/A

Step	Command	Remarks
3. Configure the maximum number of extensibility flow entries.	flow-entry max-limit <i>limit-value</i>	By default: <ul style="list-style-type: none"> An extensibility flow table can include at most 1024 flow entries on the S5500-28SC-HI and S5500-52SC-HI switches. An extensibility flow table can include at most 3072 flow entries on the other switches.

Configuring in-band management VLANs

In-band management VLANs of an OpenFlow instance are part of the VLANs associated with the OpenFlow instance. In-band management VLANs are used to establish connections between the OpenFlow instance and controllers in an OpenFlow instance.

When the in-band management VLANs are configured, the data packets within the in-band management VLANs are not forwarded through OpenFlow, and the ports that are assigned to only in-band management VLANs are not OpenFlow ports. Before configuring in-band management VLANs, you must plan the network.

To configure in-band management VLANs:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter OpenFlow instance view.	openflow instance <i>instance-id</i>	N/A
3. Configure in-band management VLANs.	in-band management vlan <i>vlan-list</i>	By default, no in-band management VLAN is configured. The in-band management VLANs of an OpenFlow instance must be within the list of the VLANs that are associated with the OpenFlow instance.

Disabling MAC address learning in the VLANs associated with an OpenFlow instance

This configuration does not take effect on in-band management VLANs.

To disable MAC address learning in the VLANs associated with an OpenFlow instance:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter OpenFlow instance view.	openflow instance <i>instance-id</i>	N/A
3. Disable MAC address learning in the VLANs associated with an OpenFlow instance.	mac-learning forbidden	By default, MAC address learning is enabled in the VLANs associated with an OpenFlow instance.

Configuring the datapath ID for an OpenFlow instance

In an OpenFlow network, each OpenFlow instance is uniquely identified by a datapath ID. By default, the datapath ID of an OpenFlow instance consists of the instance ID and the bridge MAC address. The datapath ID is configurable.

To configure the datapath ID for an OpenFlow instance:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter OpenFlow instance view.	openflow instance <i>instance-id</i>	N/A
3. Configure the datapath ID for the OpenFlow instance.	datapath-id <i>datapath-id</i>	By default, the datapath ID of an OpenFlow instance consists of the instance ID and the bridge MAC address. The upper 16 bits are the instance ID and the lower 48 bits are the bridge MAC address.

Activating or reactivating an OpenFlow instance



CAUTION:

Reactivating an OpenFlow instance refreshes the configuration data and interrupts communication with the controllers.

To activate or reactivate an OpenFlow instance:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter OpenFlow instance view.	openflow instance <i>instance-id</i>	N/A
3. Activate or reactivate the OpenFlow instance.	active instance	By default, an OpenFlow instance is not activated.

Configuring controllers for an OpenFlow switch

Configuring controllers and main connections

An OpenFlow switch supports up to 64 controllers. However, the OpenFlow channel between the OpenFlow switch and each controller can have only one main connection, which uses TCP or SSL. The main connection must be reliable and processes control messages to complete tasks such as deploying entries, obtaining data, and sending information.

To specify a controller for an OpenFlow switch and configure the main connection to the controller:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter OpenFlow instance view.	openflow instance <i>instance-id</i>	N/A

Step	Command	Remarks
3. Specify a controller and configure the main connection to the controller.	controller <i>id</i> address { ip <i>ip-address</i> ipv6 <i>ipv6-address</i> } [port <i>port-number</i>] [ssl <i>ssl-policy-name</i>]	By default, an OpenFlow instance is not configured with any main connection.

Setting the connection interruption mode

An OpenFlow switch is set to either of the following modes when it is disconnected from all controllers:

- **Secure**—In this mode, the OpenFlow switch forwards traffic based on flow tables and does not delete unexpired flow entries.
- **Standalone**—The OpenFlow switch uses the normal forwarding process.

To set the connection interruption mode for an OpenFlow switch:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter OpenFlow instance view.	openflow instance <i>instance-id</i>	N/A
3. Set the connection interruption mode.	fail-open mode { secure standalone }	By default, the secure mode is used.

Setting OpenFlow timers

An OpenFlow switch supports the following timers:

- **Connection detection interval**—Interval at which the OpenFlow switch sends two consecutive Echo Request messages to a controller. The OpenFlow switch can send up to three Echo Request messages. If none of the requests received a reply, the OpenFlow switch is disconnected from the controller.
- **Reconnection interval**—Interval for the OpenFlow switch to wait before it attempts to reconnect to a controller.

To set OpenFlow timers for an OpenFlow switch:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter OpenFlow instance view.	openflow instance <i>instance-id</i>	N/A
3. Set the interval at which the OpenFlow switch sends two consecutive Echo Request messages to a controller.	controller echo-request interval <i>interval-value</i>	The default setting is 5 seconds. To reduce the CPU load, HP recommends that you set the interval for the OpenFlow switch to send two consecutive Echo Request messages to a large value.
4. Set the reconnection interval.	controller connect interval <i>interval-value</i>	The default setting is 60 seconds.

Configuring OpenFlow to support dynamic MAC addresses

On an OpenFlow switch that supports MAC-IP flow tables, you can configure OpenFlow to support query and deletion of dynamic MAC addresses in the flow tables.

To configure OpenFlow to support dynamic MAC addresses:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter OpenFlow instance view.	openflow instance <i>instance-id</i>	N/A
3. Configure OpenFlow to support dynamic MAC addresses.	mac-ip dynamic-mac aware	By default, OpenFlow prohibits controllers from querying and deleting dynamic MAC addresses.

Displaying and maintaining OpenFlow

Task	Command	Remarks
Display the detailed information for an OpenFlow instance.	display openflow instance [<i>instance-id</i>]	Available in any view
Display flow table entries for an OpenFlow instance.	display openflow instance <i>instance-id</i> flow-table [<i>table-id</i>]	Available in any view
Display controller information for an OpenFlow instance.	display openflow instance <i>instance-id</i> controller	Available in any view
Display group table information for an OpenFlow instance.	display openflow instance <i>instance-id</i> group [<i>group-id</i>]	Available in any view
Display meter information for an OpenFlow instance.	display openflow instance <i>instance-id</i> meter [<i>meter-id</i>]	Available in any view
Display summary OpenFlow instance information.	display openflow summary	Available in any view

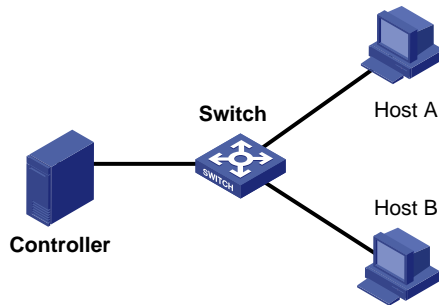
OpenFlow configuration example

Network requirements

As shown in [Figure 10](#), perform the following configuration on the switch to enable OpenFlow communication with the controller in specific VLANs:

- Create OpenFlow instance 1, associate VLANs 4092 and 4094 with the OpenFlow instance, and activate the OpenFlow instance.
- Configure the controller's IP address to have the controller manage the OpenFlow switch.

Figure 12 Network diagram



Configuration procedure

Create VLANs 4092 and 4094.

```
<Switch> system-view
[Switch] vlan 4092
[Switch-vlan4092] quit
[Switch] vlan 4094
[Switch-vlan4092] quit
```

Create OpenFlow instance 1 and associate VLANs with it.

```
[Switch] openflow instance 1
[Switch-of-inst-1] classification vlan 4092 mask 4093
```

Specify a controller for the OpenFlow instance and activate the instance.

```
[Switch-of-inst-1] controller 1 address ip 192.168.49.49
[Switch-of-inst-1] active instance
```

Verifying the configuration

Display the detailed information for OpenFlow instance 1.

```
[Switch-of-inst-1] display openflow summary
Instance 1 information:
```

Configuration information:

Description : --

Active status : active

Inactive configuration:

none

Active configuration:

Classification VLAN, total VLANs(2)

4092, 4094

In-band management VLAN, total VLANs(0)

empty VLAN

Connect mode: multiple

Mac address learning: Enabled

Flow table:

Table ID(type): 0(Extensibility), count: 0

Flow-entry max-limit: 3072

Datapath ID: 0x00010cda415e232e


```
Port information:
  none
Active channel information:
  Failopen mode: secure
```

OpenFlow commands

active instance

Syntax

active instance

View

OpenFlow instance view

Default command level

2: System level

Description

Use **active instance** to activate or reactivate an OpenFlow instance.

By default, an OpenFlow instance is not activated.

An OpenFlow instance takes effect only after it is activated.

Reactivating an OpenFlow instance refreshes the configuration data and interrupts communication with the controllers.

Examples

```
# Activate OpenFlow instance 1.
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] active instance
```

classification vlan

Syntax

classification vlan *vlan-id* [**mask** *vlan-mask*] [**loosen**]
undo classification

View

OpenFlow instance view

Default command level

2: System level

Parameters

vlan-id: Specifies the VLAN ID in the range of 1 to 4094.

vlan-mask: Specifies a VLAN mask in the range of 0 to 4095. The default value is 4095.

loosen: Specifies the loosen mode for the OpenFlow instance-VLAN association.

Description

Use **classification vlan** to associate VLANs with an OpenFlow instance.

Use **undo classification** to cancel the association.

By default, an OpenFlow instance is not associated with any VLAN.

The system calculates the VLANs to be associated according to the specified VLAN ID and mask. To view the associated VLANs, use the **display openflow instance** command.

If you execute this command multiple times, the most recent configuration takes effect.

When the **loosen** keyword is specified, a port is an OpenFlow port only when the VLANs associated with the OpenFlow instance overlap with the VLANs permitted on the port.

When the **loosen** keyword is not specified, a port is an OpenFlow port only when the VLANs associated with the OpenFlow instance are a subset of the VLANs permitted on the port.

Examples

```
# Associate an OpenFlow instance with a list of VLANs determined by VLAN ID 255 and VLAN mask 7.

<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] classification vlan 255 mask 7
```

Related commands

```
display openflow instance
```

controller address

Syntax

```
controller controller-id address { ip ip-address | ipv6 ipv6-address } [ port port-number ] [ ssl ssl-policy-name ]
undo controller controller-id address
```

View

OpenFlow instance view

Default command level

2: System level

Parameters

Controller-id: Specifies a controller ID in the range of 0 to 63.

ip ip-address: Specifies the IPv4 address of the controller.

ipv6 ipv6-address: Specifies the IPv6 address of the controller.

port port-number: Sets the port number used to establish TCP connections to the controller. The value range of the port number is 0 to 65535. The default value is 6633.

ssl ssl-policy-name: Specifies the SSL client policy that the controller uses to authenticate the OpenFlow switch. The policy name is a case-insensitive string of 1 to 16 characters.

Description

Use **controller address** to specify a controller for an OpenFlow switch and configure the main connection to the controller.

Use **undo controller address** to remove the configuration.

By default, the main connection is not configured for an OpenFlow instance.

You can specify multiple controllers for an OpenFlow switch. The OpenFlow channel between the OpenFlow switch and each controller can have only one main connection.

The OpenFlow switch exchanges control messages with a controller through the main connection to:

- Receive flow table entries or data.
- Report information to the controller.

Examples

Specify controller 10 for OpenFlow instance 1. The controller's IP address is 1.1.1.1 and the port number is 6666.

```
<Sysname> system-view
```

```
[Sysname] openflow instance 1
```

```
[Sysname-of-inst-1] controller 10 address ip 1.1.1.1 port 6666
```

controller connect interval

Syntax

controller connect interval *interval-value*

undo controller connect interval

View

OpenFlow instance view

Default command level

2: System level

Parameters

interval-value: Sets a reconnection interval in seconds, in the range of 10 to 120.

Description

Use **controller connect interval** to set a reconnection interval for an OpenFlow switch.

Use **undo controller connect interval** to restore the default.

By default, the reconnection interval is 60 seconds.

The OpenFlow switch waits a reconnection interval before it attempts to reconnect to a controller.

Examples

Set the reconnection interval to 10 seconds for OpenFlow instance 1.

```
<Sysname> system-view
```

```
[Sysname] openflow instance 1
```

```
[Sysname-of-inst-1] controller connect interval 10
```

controller echo-request interval

Syntax

controller echo-request interval *interval-value*

undo controller echo-request interval

View

OpenFlow instance view

Default command level

2: System level

Parameters

interval-value: Sets a interval at which the OpenFlow switch sends two consecutive Echo Request messages to a controller in seconds. The value range is 1 to 10.

Description

Use **controller echo-request interval** to set an interval at which the OpenFlow switch sends two consecutive Echo Request messages to a controller.

Use **undo controller echo-request interval** to restore the default.

By default, the interval at which the OpenFlow switch sends two consecutive Echo Request messages to a controller is 5 seconds.

To reduce the CPU load, HP recommends that you set the interval for the OpenFlow switch to send two consecutive Echo Request messages to a large value.

Examples

Set the interval for OpenFlow instance 1 to send two consecutive Echo Request messages to 10 seconds.

```
<Sysname> system-view
```

```
[Sysname] openflow instance 1
```

```
[Sysname-of-inst-1] controller echo-request interval 10
```

controller mode

Syntax

controller mode { multiple | single }

undo controller mode

View

OpenFlow instance view

Default command level

2: System level

Parameters

multiple: Configures the connection mode as **multiple** for the OpenFlow instance to establish connections to controllers.

single: Configures the connection mode as **single** for the OpenFlow instance to establish connections to controllers.

Description

Use **controller mode** to configure the connection mode for an OpenFlow instance to establish connections to controllers.

Use **undo controller mode** to restore the default.

By default, the connection mode is **multiple**.

When the connection mode is **single**, an OpenFlow establishes a connection to only one controller at a time, and the other controllers back up the controller. When the connection is broken, the OpenFlow instance attempts to connect to the next controller until it successfully establishes a connection.

When the connection mode is **multiple**, an OpenFlow instance can establish connections to all controllers at a time. When one or more controllers fail or one or more controller connections are broken, the OpenFlow switch can operate correctly.

Examples

```
# Configure the connection mode as single for OpenFlow instance 1.
```

```
<Sysname> system-view
```

```
[Sysname] openflow instance 1
```

```
[Sysname-of-inst-1] controller mode single
```

datapath-id

Syntax

```
datapath-id datapath-id
```

```
undo datapath-id
```

View

OpenFlow instance view

Default command level

2: System level

Parameters

datapath-id: Specifies the datapath ID for an OpenFlow instance. The argument is a hexadecimal number and the value range is 1 to 0xFFFFFFFFFFFFFFFF.

Description

Use **datapath-id** to configure the datapath ID for an OpenFlow instance.

Use **undo datapath-id** to restore the default.

By default, the datapath ID of an OpenFlow instance comprises the instance ID and the bridge MAC address. The upper 16 bits are the instance ID and the lower 48 bits are the bridge MAC address.

Examples

```
# Set the datapath ID to 0x123456 for OpenFlow instance 1.
```

```
<Sysname> system-view
```

```
[Sysname] openflow instance 1
```

```
[Sysname-of-inst-1] datapath-id 123456
```

description

Syntax

```
description text
```

```
undo description
```

View

OpenFlow instance view

Default command level

2: System level

Parameters

text: Specifies description for the OpenFlow instance, which is a case-insensitive string of 1 to 255 characters and must start with an English letter.

Description

Use **description** to configure a description for an OpenFlow instance.

Use **undo description** to restore the default.

By default, an OpenFlow instance does not have a description.

Examples

Configure a description for OpenFlow instance 1 as **test-desc**.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] description test-desc
```

display openflow controller

Syntax

display openflow instance *instance-id* **controller** [*controller-id*]

View

Any view

Default command level

1: Monitor level

Parameters

instance-id: Specifies an OpenFlow instance ID in the range of 1 to 64.

controller-id: Specifies a controller by its ID in the range of 0 to 63. If no controller ID is specified, this command displays information about all controllers for an OpenFlow instance.

Description

Use **display openflow controller** to display controller information for an OpenFlow instance.

The controller information includes connection information and packet statistics.

Examples

Display controller information for OpenFlow instance 10.

```
<Sysname> display openflow instance 10 controller
Instance 10 controller information:
Reconnect interval: 60 (s)
Echo interval      : 5 (s)

Controller ID       : 1
Controller IP address : 192.168.49.49
Controller port     : 6633
Controller role      : Equal
Connect type        : TCP
Connect state       : Established
Packets sent        : 9
Packets received    : 9
SSL policy           : --
```

Table 6 Command output

Field	Description
Reconnect interval	Reconnection interval (in seconds) for an OpenFlow instance to re-connect to all controllers.

Field	Description
Echo interval	Interval (in seconds) at which an OpenFlow instance sends an Echo Request message to all controller.
Controller role	Role of the controller: <ul style="list-style-type: none"> • Equal—The controller has the same mode as other controllers that are specified for the OpenFlow instance. • Master—The controller is the master controller for the OpenFlow instance. • Slave—The controller is a slave controller for the OpenFlow instance. If the controller is not configured with any role, this field displays two hyphens (--).
Connect type	Type of the connection between the OpenFlow instance and the controller: TCP or SSL .
Connect state	State of the connection between the OpenFlow instance and the controller: Idle or Established .
Packets sent	Number of packets that have been sent to the controller.
Packets received	Number of packets that have been received from the controller.
SSL policy	Name of the SSL client policy used for SSL connections. If no SSL client policy controller is configured, this field displays two hyphens (--).

display openflow flow-table

Syntax

display openflow instance *instance-id* **flow-table** [*table-id*]

View

Any view

Default command level

1: Monitor level

Parameters

instance-id: Specifies an OpenFlow instance ID in the range of 1 to 64.

table-id: Specifies a flow table ID in the range of 0 to 254.

Description

Use **display openflow flow-table** to display flow table information for an OpenFlow instance.

If you do not specify the flow table ID, the command displays information about all flow tables for the specified OpenFlow instance.

Examples

Display information about all flow tables for OpenFlow instance 10.

```
<Sysname> display openflow instance 10 flow-table
```

Instance 10 flow table information:

Table 0 information:

Table Type: MAC-IP, flow entry count: 1, total flow entry count: 2

MissRule (default) Flow entry information:

```

cookie: 0x0, priority: 0, hard time: 0, idle time: 0, flags: reset_counts
|no_pkt_counts|no_byte_counts, byte count: --, packet count: --
Match information: any
Instruction information:
Write actions:
Drop

```

```

Flow entry 1 information:
cookie: 0x0, priority: 1, hard time: 0, idle time: 0, flags: none,
byte count: --, packet count: --
Match information:
Ethernet destination MAC address: 0000-0000-0001
Ethernet destination MAC address mask: ffff-ffff-ffff
VLAN ID: 100, mask: 0xfff
Instruction information:
Write actions:
Output interface: GE1/0/4
Write metadata/mask: 0x0000000000000001/0xffffffffffffffff
Goto table: 1

```

```

Table 1 information:
Table Type: Extensibility, flow entry count: 2, total flow entry count: 2

```

```

MissRule (default)Flow entry information:
cookie: 0x0, priority: 0, hard time: 0, idle time: 0, flags: none,
byte count: --, packet count: 60
Match information: any
Instruction information:
Write actions:
Drop

```

```

Flow entry 1 information:
cookie: 0x0, priority: 0, hard time: 0, idle time: 0, flags: flow_send_rem
|check_overlap, byte count: --, packet count: 1
Match information:
Input interface: GE1/0/3
Ethernet source MAC address: 0000-0000-0001
Ethernet source MAC address mask: ffff-ffff-ffff
Instruction information:
Set meter: 100
Apply actions:
Output interface: GE1/0/4
Write actions:
Output interface: Controller, send length: 128 bytes

```

Table 7 Command output

Field	Description
Table Type	Type of the flow table: MAC-IP or Extensibility .

Field	Description
flow entry count	Number of flow entries deployed by controllers.
total flow entry count	Total number of flow entries in the table.
cookie	Cookie ID of the flow entry.
priority	Priority of the flow entry. The larger the value, the higher the priority.
hard time	Hard timeout of the flow entry, in seconds. The flow entry is aged out immediately after the hard timeout expires. If the flow entry has no hard timeout, the field displays 0 .
idle time	Idle timeout of the flow entry, in seconds. The flow entry is aged out if no packet matches the entry within the idle timeout. If the flow entry has no idle timeout, the field displays 0 .
flags	Flags that the flow entry includes: <ul style="list-style-type: none"> • flow_send_rem—Sends a flow removed message when the flow entry is removed or expires. • check_overlap—Checks for overlapping flow entries. • reset_counts—Resets flow table counters. • no_pkt_counts—Does not count packets. • no_byte_counts—Does not count bytes. If the flow entry does not include any flags, this field displays none .
byte count	Number of bytes that have matched the flow entry.
packet count	Number of packets that have matched the flow entry.
Match information	Contents in the Match field of the flow entry (see Table 7).
Instruction information	Contents in the Instruction field of the flow entry: <ul style="list-style-type: none"> • Set meter—Sends the matched packet to a specified meter. • Write metadata/mask—Writes the metadata value and mask into the metadata fields of the matched packet. • Goto table—Sends the matched packet to the next flow table for processing. • Clear actions—Clears all actions in the action set of the matched packet. • Apply actions—Applies specified actions in the action set of the matched packet. • Write actions—Writes specified actions into the action set of the matched packet. For more information about actions, see Table 8 .

Table 8 Match information

Match field	Match field mask	Description
Input interface	N/A	Ingress port (see Table 9).
Physical input interface	N/A	Ingress physical port.

Match field	Match field mask	Description
Metadata	N/A	<p>Meta data that is transmitted between flow tables.</p> <ul style="list-style-type: none"> • 1—Matches the destination MAC address in the metadata. • 2—Matches the source MAC address in the metadata. • 4—Matches the destination IP address in the metadata.
Ethernet destination MAC address	Mask	Ethernet destination MAC address and mask.
Ethernet source MAC address	Mask	Ethernet source MAC address and mask.
Ethernet type	N/A	Ethernet type of the OpenFlow packet payload.
VLAN ID	Mask	VLAN ID and mask.
VLAN PCP	N/A	VLAN priority.
IP DSCP	N/A	Differentiated Services Code Point (DSCP) value.
IP ECN	N/A	Explicit Congestion Notification (ECN) value in the IP header.
IP protocol	N/A	IPv4 or IPv6 protocol number.
IPv4 source address	Mask	IPv4 source address and mask.
IPv4 destination address	Mask	IPv4 destination address and mask.
TCP source port	Mask	TCP source port and mask.
TCP destination port	Mask	TCP destination port and mask.
UDP source port	Mask	UDP source port and mask.
UDP destination port	Mask	UDP destination port and mask.
ICMPv4 type	N/A	ICMPv4 type.
ICMPv4 code	N/A	ICMPv4 code.
ARP source IPv4 address	Mask	Sender IPv4 address and mask in the ARP payload.
ARP source MAC address	Mask	Sender MAC address and mask in the ARP payload.
IPv6 source address	Mask	Source IPv6 address and mask.
IPv6 destination address	Mask	Destination IPv6 address and mask.
IPv6 flow label	Mask	IPv6 flow label and mask.
ICMPv6 type	N/A	ICMPv6 type.
ICMPv6 code	N/A	ICMPv6 code.
IPv6 ND source MAC address	N/A	Source link-layer address in an IPv6 Neighbor Discovery message.
IPv6 ND target MAC address	N/A	Target link-layer address in an IPv6 Neighbor Discovery message.

Table 9 Actions

Field	Description
Drop	Drops the matched packet.
Output interface	Sends the packet through a specified port. For more information about ports, see Table 9 .
send length	Specifies the length of bytes to be taken from the packet and be sent to the controller.
Group	Specifies a group to process the packet.
Set queue	Maps the flow entry to a queue specified by ID.
Set field	Modifies a specific field of the packet.

Table 10 Ports

Port name	Ingress port	Output port	Description
In_Port	Not supported.	Supported.	Ingress port of the packet.
Table	Not supported.	Supported.	Start flow table in the OpenFlow workflow.
Normal	Not supported.	Supported.	Normal forwarding workflow of the switch.
Flood	Not supported.	Supported.	Flooding workflow.
All	Not supported.	Supported.	All ports.
Controller	Supported.	Supported.	Channel connected to the controller.
Local	Supported.	Supported.	Local CPU.
Any	Not supported.	Not supported.	No port is specified. It cannot be ingress port or output port.
GE1/0/3 (port name)	Supported.	Supported.	Name of a physical or logical port, such as an aggregate interface.

display openflow group

Syntax

display openflow instance *instance-id* **group** [*group-id*]

View

Any view

Default command level

1: Monitor level

Parameters

instance-id: Specifies an OpenFlow instance by its ID in the range of 1 to 64.

group-id: Specifies a group entry by its ID in the range of 0 to 4294967040. If this argument is not specified, the command displays information about all group entries of the OpenFlow instance.

Description

Use **display openflow group** to display the group table information for an OpenFlow instance.

The group entries are referenced by flow entries to make the OpenFlow device support more packet forwarding functions, for example, multicast and broadcast. Each group table contains multiple

action buckets. The actions in the buckets of a group entry are performed for packets matching the group entry.

You cannot configure group entries on the OpenFlow devices. Instead, you can configure group entries on the controller and issue the group entries to the OpenFlow device.

Examples

Display the group table information for OpenFlow instance 10.

```
<Sysname> display openflow instance 10 group
```

Instance 10 group table information:

Group count: 1

Group entry 4294967040:

Type: All, byte count: 0, packet count: 0

Bucket 1 information:

Action count 1, watch port: GE1/0/1, watch group: 0

Byte count 0, packet count 0

Output interface: GE1/0/2

Referenced information:

Count: 1

Flow table: 254

Flow entry: 2

Table 11 Output description

Field	Description
Group count	Number of group entries contained in the OpenFlow instance.
Type	Group table type: All —Execute all buckets in the group. This group is used for multicast or broadcast forwarding.
bucket	Action buckets contained in the group table.
Action count	Number of actions in the action bucket.
Byte count	Number of bytes processed by the action bucket. Two hyphens (--) are displayed when the field is not supported.
packet count	Number of packets processed by the action bucket. Two hyphens (--) are displayed when the field is not supported.
watch port	Ports that affect the action bucket status.
watch group	Group table IDs of the ports that affect the action bucket status.
Output interface	Output interface in the group table.
Referenced information	Information about the flow entries referencing group entries.
Count	Number of flow entries that reference group entries.
Flow table	ID of the flow table to which the flow entries referencing the group entries belong.
Flow entry	IDs of flow entries referencing group entries.

display openflow instance

Syntax

display openflow instance [*instance-id*]

View

Any view

Default command level

1: Monitor level

Parameters

instance-id: Specifies an OpenFlow instance by its ID in the range of 1 to 64.

description

Use **display openflow instance** to display the detailed information for an OpenFlow instance.

Examples

Display the detailed information of OpenFlow instances.

```
<Sysname> display openflow instance
```

Instance 10 information:

Configuration information:

Description : test-desc

Active status : active

Inactive configuration:

Classification VLAN, total VLANs(1)

3

Flow table:

Table ID(type): 0(MAC-IP)

Table ID(type): 1(Extensibility)

Active configuration:

Classification VLAN, loosen mode, total VLANs(1)

2

In-band management VLAN, total VLANs(0)

empty VLAN

Connect mode: multiple

Mac address learning: Enabled

Flow table:

Table ID(type): 0(MAC-IP), count: 0

Flow-entry max-limit: 3072

Datapath ID: 0x0000001234567891

Port information:

GigabitEthernet1/0/3

Active channel information:

Controller 1 IP address: 192.168.49.49 port: 6633

Controller 2 IP address: 192.168.43.49 port: 6633

Table 12 Command output

Field	Description
Description	Description of the OpenFlow instance.
Active status	Activation status of the OpenFlow instance.
Inactive configuration	Inactive OpenFlow instance configuration.
Active configuration	Active OpenFlow instance configuration.
Classification VLAN, loosen mode, total VLANs	VLANs associated with the OpenFlow instance, the total number of VLANs, and the loosen mode.
In-band management VLAN, total VLANs	In-band management VLANs and the total number of in-band management VLANs. empty VLAN is displayed when no in-band management VLAN is configured.
Connect mode	Connection mode for the OpenFlow instance to establish connections to controllers: <ul style="list-style-type: none"> multiple—The connection mode is multiple for the OpenFlow instance to establish connections to controllers. single—The connection mode is single for the OpenFlow instance to establish connections to controllers.
Mac-address learning	Whether MAC address learning is enabled in the VLANs associated with the OpenFlow instance: <ul style="list-style-type: none"> Enabled—MAC address learning is enabled in the VLANs associated with the OpenFlow instance. Disabled—MAC address learning is disabled in the VLANs associated with the OpenFlow instance.
Flow-entry max-limit	Maximum number of flow entries allowed in the extensibility flow table.
Datapath ID	Datapath ID of the OpenFlow instance.
Port information	Ports added to the OpenFlow instance.
Flow table	Flow table information of the OpenFlow instance.
Table ID(type)	Flow table ID (flow table type). The flow table type can be MAC-IP or Extensibility .
count	Total number of flow entries in the flow table.
Active channel information	Information about active control channels.
Controller id IP address: port:	Brief information of controllers which have established connections to the OpenFlow instance. This field is displayed only when the OpenFlow instance has established connections to controllers.
Failopen mode	Connection interruption mode when the OpenFlow instance is disconnected from all controllers (this field is displayed only when the OpenFlow instance is disconnected from all controllers): <ul style="list-style-type: none"> secure—The OpenFlow switch uses flow tables for traffic forwarding after it is disconnected from all controllers. standalone—The OpenFlow switch uses the normal forwarding process after it is disconnected from all controllers.

display openflow meter

Syntax

display openflow instance *instance-id* **meter** [*meter-id*]

View

Any view

Default command level

1: Monitor level

Parameters

instance-id: Specifies an OpenFlow instance by its ID in the range of 1 to 64.

meter-id: Specifies a meter by its ID in the range of 0 to 4294901760. If no meter ID is specified, this command displays information about all meter entries for an OpenFlow instance.

Description

Use **display openflow meter** to display meter entry information for an OpenFlow instance.

Examples

Display meter entry information for OpenFlow instance 10.

```
<Sysname> display openflow instance 10 meter
```

```
Meter flags: KBPS -- Rate value in kb/s, PKTPS -- Rate value in packet/sec
             BURST -- Do burst size,          STATS -- Collect statistics
```

```
Instance 10 meter table information:
```

```
meter entry count: 2
```

```
Meter entry 100 information:
```

```
Meter flags: KBPS
```

```
Band 1 information
```

```
Type: drop, rate: 64kbps, burst size: 256kbps
```

```
Byte count: --, packet count: 0
```

```
Referenced information:
```

```
Count: 3
```

```
Flow table: 0
```

```
Flow entry: 1, 2, 3
```

```
Meter entry 200 information:
```

```
Meter flags: KBPS
```

```
Band 1 information
```

```
Type: drop, rate: 64kbps, burst size: 128kbps
```

```
Byte count: --, packet count: 0
```

```
Referenced information:
```

```
Count: 0
```

Table 13 Command output

Field	Description
Group entry count	Total number of meter entries included in the OpenFlow instance.
Meter flags	Flags configured for the meter: <ul style="list-style-type: none">• KBPS—The rate value is in kbps.• PKTPS—The rate value is in pps.• BURST—The burst size field in the band is used and the length of the packet or byte burst is determined by the burst size.• STATS—Meter statistics are collected.

Field	Description
Band	Bands included in the meter.
Type	Type of the band: <ul style="list-style-type: none"> drop—Discard the packet. dscp remark—Modify the drop precedence of the DSCP field in the IP header of the packet.
Rate	Rate value above which the corresponding band may apply to packets.
Burst size	Length of the packet or byte burst to consider for applying the meter.
Byte count	Number of bytes processed by a band. If this field is not supported, the field displays two hyphens (--).
packet count	Number of packets processed by a band. If this field is not supported, the field displays two hyphens (--).
Referenced information	Information about the meter entry referenced by flow entries.
Count	Total number of flow entries that reference the meter entry.
Flow table	Flow table to which the flow entries that reference the meter entry belong.
Flow entry	Flow entries that reference the meter entry.

display openflow summary

Syntax

display openflow instance summary

View

Any view

Default command level

1: Monitor level

Description

Use **display openflow summary** to display summary OpenFlow instance information, including OpenFlow instance ID, activation status, and datapath ID.

Examples

Display summary information about OpenFlow instances.

```
<Sysname> display openflow summary
```

Fail-open mode: Se - Secure mode, Sa - Standalone mode

ID	Status	Datapath-ID	Channel	Table-num	Port-num	Reactivate
1	Active	11000a0b0c0d0	Connected	2	8	Y
2	Active	21000a0b0c0d0	Connected	2	6	N

Table 14 Command output

Field	Description
ID	OpenFlow instance ID.
Status	Activation status of the OpenFlow instance: <ul style="list-style-type: none"> Active—The OpenFlow instance is active. Inactive—The OpenFlow instance is inactive.

Field	Description
Datapath-ID	Datapath ID of the OpenFlow instance. A hyphen (-) is displayed when the OpenFlow instance is inactive.
Channel	<p>Status of the secure channel between the OpenFlow instance and the controller:</p> <ul style="list-style-type: none"> • Connected—The secure channel between the OpenFlow instance and the controller has been established. • Failed(Se)—The secure channel between the OpenFlow instance and the controller has been disconnected, and the OpenFlow instance is operating in secure mode. • Failed(Sa)—The channel between the OpenFlow instance and the controller has been disconnected, and the OpenFlow instance is operating in standalone mode. <p>A hyphen (-) is displayed when the OpenFlow instance is inactive.</p>
Table-num	Number of flow tables in the OpenFlow instance. A hyphen (-) is displayed when the OpenFlow instance is inactive.
Port-num	Number of ports belonging to the OpenFlow instance. A hyphen (-) is displayed when the OpenFlow instance is inactive.
Reactivate	<p>Indicates whether the OpenFlow instance needs to be reactivated:</p> <ul style="list-style-type: none"> • Y—The OpenFlow instance needs to be reactivated. • N—The OpenFlow instance does not need to be reactivated. <p>A hyphen (-) is displayed when the OpenFlow instance is inactive.</p>

fail-open mode

Syntax

fail-open mode { secure | standalone }

undo fail-open mode

View

OpenFlow instance view

Default command level

2: System level

Parameters

secure: Configures the OpenFlow switch to use flow tables for traffic forwarding after it is disconnected from all controllers.

standalone: Configures the OpenFlow switch to use the normal forwarding process after it is disconnected from all controllers.

Description

Use **fail-open mode** to set the connection interruption mode for an OpenFlow switch.

Use **undo fail-open mode** to restore the default.

By default, the connection interruption mode is **secure**, and the controller deploys the table-miss flow entry (the action is **Drop**) to the OpenFlow instance.

Examples

Configure the connection interruption mode to **standalone** for OpenFlow instance 1.

```
<Sysname> system-view
```

```
[Sysname] openflow instance 1
```

[Sysname-of-inst-1] fail-open mode standalone

flow-entry max-limit

Syntax

flow-entry max-limit *limit-value*

undo flow-entry max-limit

View

OpenFlow instance view

Default command level

2: System level

Parameters

limit-value: Specifies the maximum number of flow entries:

- On the S5500-28SC-HI and S5500-52SC-HI switches, the value is in the range of 1 to 1024.
- On the other switches, the value is in the range of 1 to 3072.

Description

Use **flow-entry max-limit** to configure the maximum number of entries that every extensibility flow table can include.

Use **undo flow-entry max-limit** to restore the default.

By default:

- An extensibility flow table can include at most 1024 flow entries on the S5500-28SC-HI and S5500-52SC-HI switches.
- An extensibility flow table can include at most 3072 flow entries on the other switches.

Examples

Configure OpenFlow instance 1 to include at most 256 entries in each extensibility flow table.

```
<Sysname> system-view
```

```
[Sysname] openflow instance 1
```

```
[Sysname-of-inst-1] flow-entry max-limit 256
```

flow-table

Syntax

flow-table { **extensibility** *extensibility-table-id* | **mac-ip** *mac-ip-table-id* }*

undo flow-table

View

OpenFlow instance view

Default command level

2: System level

Parameters

extensibility *extensibility-table-id*: Specifies an extensibility flow table ID in the range of 0 to 254.

mac-ip *mac-ip-table-id*: Specifies a MAC-IP flow table ID in the range of 0 to 254.

Description

Use **flow-table** to configure a flow table for an OpenFlow instance.

Use **undo flow-table** to restore the default.

By default, an OpenFlow instance has an extensibility flow table whose ID is 0.

You can specify only one MAC-IP flow table and one extensibility flow table for an OpenFlow instance, and the MAC-IP flow table ID must be smaller than the extensibility flow table ID.

Configure flow tables before you activate an OpenFlow instance.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure a MAC-IP flow table with ID 0 and an extensibility flow table with ID 1 for OpenFlow instance 1.

```
<Sysname> system-view
```

```
[Sysname] openflow instance 1
```

```
[Sysname-of-inst-1] flow-table mac-ip 0 extensibility 1
```

in-band management vlan

Syntax

in-band management vlan *vlan-list*

undo in-band management vlan

View

OpenFlow instance view

Default command level

2: System level

Parameters

vlan-list: Specifies a list of VLANs in the format of *vlan-list* = { *vlan-id1* [**to** *vlan-id2*] } &<1-10>, where *vlan-id1* and *vlan-id2* are both in the range of 1 to 4094, *vlan-id2* cannot be smaller than *vlan-id1*, and &<1-10> indicates that you can specify up to 10 *vlan-id1* [**to** *vlan-id2*] parameters.

Description

Use **in-band management vlan** to configure in-band management VLANs.

Use **undo in-band management vlan** to restore the default.

By default, no in-band management VLAN is configured.

The in-band management VLANs must be a subset of the VLANs associated with the OpenFlow instance.

Examples

Configure VLAN 10 as an in-band management VLAN in OpenFlow instance 1.

```
<Sysname> system-view
```

```
[Sysname] openflow instance 1
```

```
[Sysname-of-inst-1] in-band management vlan 10
```

mac-ip dynamic-mac aware

Syntax

mac-ip dynamic-mac aware

undo mac-ip dynamic-mac aware

View

OpenFlow instance view

Default command level

2: System level

Description

Use **mac-ip dynamic-mac aware** to configure OpenFlow to support dynamic MAC addresses.

Use **undo mac-ip dynamic-mac aware** to restore the default.

By default, an OpenFlow instance ignores dynamic MAC address messages sent from controllers.

When a MAC-IP flow table is configured for an OpenFlow switch, you can configure OpenFlow to support query and deletion of dynamic MAC addresses in the table.

When this command is configured, the OpenFlow switch does not send change events for the dynamic MAC addresses to controllers.

Examples

Configure OpenFlow instance 1 to support dynamic MAC addresses.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] mac-ip dynamic-mac aware
```

mac-learning forbidden

Syntax

mac-learning forbidden

undo mac-learning forbidden

View

OpenFlow instance view

Default command level

2: System level

Description

Use **mac-learning forbidden** to disable MAC address learning for the VLANs associated with the OpenFlow instance.

Use **undo mac-learning forbidden** to restore the default.

By default, MAC address learning is enabled in the VLANs associated with an OpenFlow instance.

Examples

Disable MAC address learning in the VLANs associated with OpenFlow instance 1.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] mac-learning forbidden
```

openflow instance

Syntax

openflow instance *instance-id*

undo openflow instance *instance-id*

View

System view

Default command level

2: System level

Parameters

instance-id: Specifies an OpenFlow instance ID in the range of 1 to 64.

Description

Use **openflow instance** to create an OpenFlow instance and enter OpenFlow instance view.

Use **undo openflow instance** to remove an OpenFlow instance.

By default, no OpenFlow instance exists.

Examples

Create OpenFlow instance 1, and enter the OpenFlow instance view.

```
<Sysname> system-view
```

```
[Sysname] openflow instance 1
```

```
[Sysname-of-inst-1]
```

Modified feature: Setting the device name

Feature change description

The allowed maximum device name length has changed.

Command changes

Modified command: sysname

Syntax

sysname *sysname*

Views

System view

Change description

Before modification: The device name can have 1 to 30 characters.

After modification: The device name can have 1 to 64 characters.

Modified feature: Specifying multiple public keys for an SSH user

Feature change description

When the SSH server uses the digital signature to authentication an SSH user, up to six public keys can be assigned to the user. The SSH server authenticates the user through the first matching public key.

Command changes

Modified command: ssh user

Old syntax

In non-FIPS mode:

```
ssh user username service-type stelnet authentication-type { password | { any | password-publickey | publickey } assign publickey keyname }
```

```
ssh user username service-type { all | scp | sftp } authentication-type { password | { any | password-publickey | publickey } assign publickey keyname work-directory directory-name }
```

```
undo ssh user username
```

In FIPS mode:

```
ssh user username service-type stelnet authentication-type { password | password-publickey assign publickey keyname }
```

```
ssh user username service-type { all | scp | sftp } authentication-type { password | password-publickey assign publickey keyname work-directory directory-name }
```

```
undo ssh user username
```

New syntax

In non-FIPS mode:

```
ssh user username service-type stelnet authentication-type { password | { any | password-publickey | publickey } assign publickey keyname&<1-6> }
```

```
ssh user username service-type { all | scp | sftp } authentication-type { password | { any | password-publickey | publickey } assign publickey keyname&<1-6> work-directory directory-name }
```

```
undo ssh user username
```

In FIPS mode:

```
ssh user username service-type stelnet authentication-type { password | password-publickey assign publickey keyname&<1-6> }
```

```
ssh user username service-type { all | scp | sftp } authentication-type { password | password-publickey assign publickey keyname&<1-6> work-directory directory-name }
```

```
undo ssh user username
```

Views

System view

Change description

Before modification: You can assign only one public key to an SSH user. The **assign publickey *keyname*** option is used to specify this public key.

After modification: You can assign multiple public keys to an SSH user. The **assign publickey *keyname*&<1-6>** option is used to specify these public keys, and &<1-6> indicates that up to six public keys can be specified. When multiple public keys are used, the SSH server authenticates the user through the first matching public key.

Modified feature: Disabling an untrusted port from recording clients' IP-to-MAC bindings

Feature change description

In previous releases, you can disable only trusted ports from recording clients' IP-to-MAC bindings. In this release, both trusted and untrusted ports can be disabled from recording clients' IP-to-MAC bindings.

Command changes

Modified command: dhcp-snooping trust

Old syntax

```
dhcp-snooping trust [ no-user-binding ]  
undo dhcp-snooping trust
```

New syntax

```
dhcp-snooping trust  
undo dhcp-snooping trust
```

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Change description

Before modification: You can use the **dhcp-snooping trust** command to configure a port as a trusted port, and specify the **no-user-binding** keyword to disable the trusted port from recording clients' IP-to-MAC bindings. Untrusted ports on the DHCP snooping device always record clients' IP-to-MAC bindings, and this function cannot be disabled.

After modification: The **no-user-binding** keyword is removed from the **dhcp-snooping trust** command. You can use the new command **dhcp-snooping no-user-binding** to disable a port from recording clients' IP-to-MAC bindings. The port can be either a trusted port or an untrusted port.

New command: dhcp-snooping no-user-binding

Use **dhcp-snooping no-user-binding** to disable a port (either trusted or untrusted) from recording clients' IP-to-MAC bindings.

Use **undo dhcp-snooping no-user-binding** to restore the default.

Syntax

```
dhcp-snooping no-user-binding  
undo dhcp-snooping no-user-binding
```

Default

With DHCP snooping enabled, all ports record clients' IP-to-MAC bindings.

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default command level

2: System level

Examples

```
# Disable GigabitEthernet 1/0/1 from recording clients' IP-to-MAC bindings.
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping no-user-binding
```

Modified feature: ARP packet rate limit

Feature change description

Changed the value range of the *pps* argument.

Command changes

Modified command: `arp rate-limit`

Syntax

```
arp rate-limit { disable | rate pps drop }
```

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Change description

Before modification: The value range for the *pps* argument is 5 to 256.

After modification: The value range for the *pps* argument is 5 to 500.

Modified feature: Specifying the username and password to log in to the SCP server

Feature change description

Before you transfer files through SCP, you can log in to the SCP server by using one of the following methods for **password**, **password-publickey**, or **any** authentication:

- Entering the username and password as prompted
- Specifying the username and password in the **scp** command

Command changes

Modified command: `SCP`

Old syntax

In non-FIPS mode:

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

In FIPS mode:


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

New syntax

In non-FIPS mode:

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

In FIPS mode:

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

Views

User view

Change description

Before modification: The **username username password password** option is not supported. You can enter the username and password only as prompted.

After modification: The **username username password password** option is supported. In addition to entering the username and password as prompted, you can also specify the username and password in the **scp** command.

The *username* argument specifies the username. It is a case-sensitive string of 1 to 80 characters.

The *password* argument specifies the password in plain text. It is a string of 1 to 63 characters.

Modified feature: Customizing DHCP options

Feature change description

Changed the value range for the *code* argument.

Command changes

Modified command: option

Syntax

```
option code { ascii ascii-string | hex hex-string<1-16> | ip-address ip-address<1-8> }
undo option code
```

Views

DHCP address pool view

Change description

Before modification: The value range for the *code* argument is 2 to 254, excluding 12, 50 through 55, 57 through 61, and 82.

After modification: The value range for the *code* argument is 2 to 254, excluding 50 through 54, 58, 59, 61, and 82.

Modified feature: ACL-based packet filtering on a VLAN interface

Feature change description

In versions prior to Release 5501, the ACL applied to a VLAN interface filters packets forwarded at Layer 3. In Release 5501 and later versions, the ACL applied to a VLAN interface filters packets forwarded at Layer 3 and packets forwarded at Layer 2.

Command changes

Modified command: packet-filter

Syntax

packet-filter { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

Views

Interface view

Change description

Before modification, the ACL applied to a VLAN interface filters packets forwarded at Layer 3.

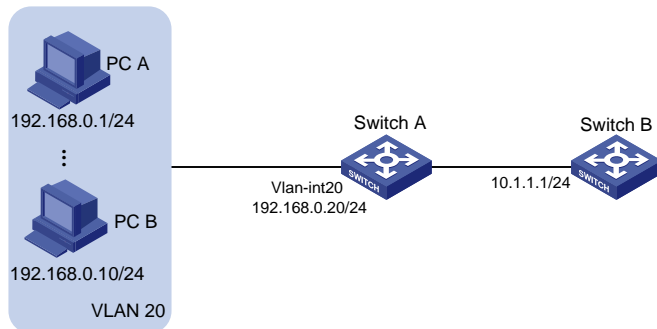
After modification, the ACL applied to a VLAN interface filters packets forwarded at Layer 3 and packets forwarded at Layer 2.

Examples

As shown in [Figure 1](#), configure packet filtering on Switch A to meet the following requirements:

- Allow only packets from PC A to Switch B to pass through.
- Allow PC A and PC B to communicate at Layer 2.

Figure 1 Network diagram



- In versions before Release 5501, the configuration on Switch A is as follows:

```
<SwitchA>system-view
System View: return to User View with Ctrl+Z.
[SwitchA]acl number 3000
[SwitchA-acl-adv-3000]rule permit ip source 192.168.0.1 0 destination 10.1.1.1 0.0.0.255
[SwitchA-acl-adv-3000]rule deny ip
[SwitchA-acl-adv-3000]quit
[SwitchA]interface Vlan-interface 20
```

```
[SwitchA-Vlan-interface20]packet-filter 3000 inbound
```

Because the ACL does not take effect on packets forwarded at Layer 2, you just need to configure two rules in the following order:

- a.** A permit rule that permits packets from PC A to Switch B.
 - b.** A deny rule that denies all packets.
- In Release 5501 and later versions, the configuration on Switch A is as follows:

```
<SwitchA>system-view
```

```
System View: return to User View with Ctrl+Z.
```

```
[SwitchA]acl number 3000
```

```
[SwitchA-acl-adv-3000]rule permit ip source 192.168.0.1 0 destination 10.1.1.1 0.0.0.255
```

```
[SwitchA-acl-adv-3000]rule permit ip source 192.168.0.1 0.0.0.255 destination 192.168.0.10 0.0.0.255
```

```
[SwitchA-acl-adv-3000]rule deny ip
```

```
[SwitchA-acl-adv-3000]quit
```

```
[SwitchA]interface Vlan-interface 20
```

```
[SwitchA-Vlan-interface20]packet-filter 3000 inbound
```

Because the ACL takes effect on packets forwarded at Layer 3 and packets forwarded at Layer 2, you need to configure one more permit rule to permit packets from PC A to PC B. Configure the rules in the following order:

- a.** A permit rule that permits packets from PC A to Switch B.
 - c.** A permit rule that permits packets from PC A to PC B.
 - d.** A deny rule that denies all packets.

R5206

This release has the following changes:

- New feature: Configuring the ARP detection logging function
- New feature: 802.1X-based dynamic IPv4 source guard binding entries
- New feature: SSL server policy association with the FTP service
- New feature: Enabling MAC authentication multi-VLAN mode
- Modified feature: Specifying multiple secondary HWTACACS servers
- Modified feature: Displaying brief interface information
- Modified feature: Displaying brief IP configuration for Layer 3 interfaces
- Modified feature: Configuring static multicast MAC address entries

New feature: Configuring the ARP detection logging function

Configuring the ARP detection logging function

The ARP detection logging function enables a device to generate ARP detection log messages when ARP packet attacks are detected. An ARP detection log message can include the following information:

- Receiving interface of the ARP packets.
- Sender IP address.
- Total number of ARP packets dropped.

The following is an example of an ARP detection log message:

Detected an inspection occurred on interface GigabitEthernet 1/0/1 with IP address 172.18.48.55 (Totally 10 packets dropped).

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. (Optional) Enable the ARP detection logging function.	arp detection log enable	By default, the ARP detection logging function is enabled.

Command reference

arp detection log enable

Use **arp detection log enable** to enable logging for ARP detection.

Use **undo detection log enable** to disable the logging function for ARP detection

Syntax

arp detection log enable

undo arp detection log enable

Default

Logging is enabled for ARP detection

View

System view

Default level

3: Manage level

Examples

```
# Enable logging for ARP detection.
```

```
<Sysname> system-view
```

```
[Sysname] arp detection enable
```

New feature: 802.1X-based dynamic IPv4 source guard binding entries

Overview

To protect 802.1X users from IP attacking, you can enable 802.1X to cooperate with IP source guard. This IP source guard feature generates dynamic IPv4 source guard binding entries based on 802.1X secure entries. It can filter out IPv4 packets from unauthenticated 802.1X users.

To deny any online authenticated 802.1X users to change their IP addresses, you can enable the 802.1X IP freezing function on the authentication port. The port saves the IP addresses of 802.1X users when they get online, and it does not update these IP addresses even if the IP addresses of these users have changed. If an online authenticated 802.1X user changes its IP address, the port denies the user to access the network, because the user's IP address does not match any IPv4 source guard binding entries.

Configuration procedure

Configuration task list

Task	Remarks
Enabling 802.1X	For more information about 802.1X, see <i>Security Configuration Guide</i> .
Enabling the 802.1X IP freezing function	Optional.
Enabling a port to generate 802.1X-based dynamic IPv4 source guard binding entries	N/A
Enabling the IPv4 source guard function on an interface	See the ip verify source { ip-address ip-address mac-address mac-address } command. For more information about IP source guard, see <i>Security Configuration Guide</i> .

Enabling the 802.1X IP freezing function

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable the 802.1X IP freezing function.	dot1x user-ip freeze	By default, the port saves the IP address received from an 802.1X user and updates the IP address when it receives a different IP address from the same user.

Enabling a port to generate 802.1X-based dynamic IPv4 source guard binding entries

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable the port to generate 802.1X-based dynamic IPv4 source guard binding entries.	ip verify source dot1x	By default, this function is disabled.

NOTE:

If the 802.1X client does not upload users' IP addresses to the device, you must enable DHCP snooping or ARP snooping on the device. Then 802.1X can obtain the IP addresses of 802.1X users for the device to generate 802.1X-based dynamic IP source guard binding entries.

Command reference

dot1x user-ip freeze

Syntax

dot1x user-ip freeze
undo dot1x user-ip freeze

View

Layer 2 Ethernet interface view

Default level

2: System level

Description

Use **dot1x user-ip freeze** to enable the 802.1X IP freezing function.

Use **undo dot1x user-ip freeze** to restore the default.

By default, a port saves the IP address received from an 802.1X user and updates the IP address when it receives a different IP address from the same user.

Examples

```
# Enable 802.1X IP freezing on port GigabitEthernet 1/0/1.
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x user-ip freeze
```

ip verify source dot1x

Syntax

```
ip verify source dot1x
undo ip verify source dot1x
```

View

Layer 2 Ethernet interface view

Default level

2: System level

Description

Use **ip verify source dot1x** to enable a port to generate 802.1X-based dynamic IPv4 source guard binding entries.

Use **undo ip verify source dot1x** to remove the 802.1X-based dynamic IPv4 source guard binding entries.

By default, a Layer 2 Ethernet port generates dynamic IPv4 source guard binding entries based on DHCP snooping.

Executing the **undo ip verify source dot1x** command or disabling 802.1X on the port will remove all 802.1X-based dynamic IPv4 source guard binding entries on the port.

The port will remove the dynamic IPv4 source guard binding entry of an 802.1X user after the user gets offline.

Example

Enable port GigabitEthernet 1/0/1 to generate 802.1X-based dynamic IPv4 source guard binding entries.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip verify source dot1x
```

New feature: SSL server policy association with the FTP service

Configuration procedure

For two devices that support secure FTP, you can associate an SSL server policy with the FTP service on the FTP server. Then, the FTP connection will be established over an SSL connection.

Before associating an SSL server policy with the FTP service, you must create the policy and disable FTP server.

To associate an SSL server policy with the FTP service:

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Associate an SSL server policy with the FTP server to ensure data security.	ftp server ssl-server-policy policy-name	By default, no SSL server policy is associated with the FTP server.

Command reference

ftp server ssl-server-policy

Syntax

ftp server ssl-server-policy *policy-name*

undo ftp server ssl-server-policy

Views

System view

Default level

2: System level

Parameters

policy-name: Specifies an SSL server policy by its name, a string of 1 to 16 characters.

Description

Use **ftp server ssl-server-policy** to associate an SSL server policy with the FTP server.

Use **undo ftp server ssl-server-policy** to remove the association.

By default ,no SSL server policy is associated with the FTP server.

Examples

Associate SSL server policy **myssl** with the FTP server.

```
<Sysname> system-view
```

```
[Sysname] ftp server ssl-server-policy myssl
```

New feature: Enabling MAC authentication multi-VLAN mode

Overview

By default, a MAC authentication-enabled port forwards packets for a MAC-authenticated user only in the VLAN where it was authenticated. If the user sends packets with the same MAC address in a different VLAN, the port must re-authenticate the user. After the user passes re-authentication, the device will update the MAC-VLAN mapping entry on the port. For a user that sends various types of traffic (for example, data, video, and audio) in multiple VLANs with the same MAC address, frequent MAC re-authentication downgrades the system performance and affects data transmission quality.

The MAC authentication multi-VLAN mode enables a MAC authentication-enabled port to forward packets for the user in up to five VLANs without re-authentication. When this mode is enabled, the device does not update the original MAC-VLAN mapping entry on the port after the port receives a packet sourced from the authenticated MAC address in a different VLAN. It adds another MAC-VLAN mapping entry for the MAC address.

For example, an IP phone can send tagged and untagged frames, the IP phone is connected to a MAC authentication-enabled port, and the port receives tagged frames in VLAN 2 and untagged frames in VLAN 1. Before you enable the multi-VLAN mode on the port, the port must re-authenticate the IP phone repeatedly, because it sends tagged frames and untagged frames alternately in different VLANs. After you enable the multi-VLAN mode, the port can receive tagged and untagged frames alternately from the IP phone without triggering a MAC re-authentication. The multi-VLAN mode improves the transmission quality of data that is vulnerable to delay and interference.

Configuration procedure

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable MAC authentication multi-VLAN mode.	mac-authentication host-mode multi-vlan	By default, a MAC authentication-enabled port forwards packets for an authenticated user only in the VLAN where the user's MAC address was authenticated.

Command reference

mac-authentication host-mode multi-vlan

Syntax

mac-authentication host-mode multi-vlan
undo mac-authentication host-mode multi-vlan

View

Layer 2 Ethernet interface view

Default level

2: System level

Description

Use **mac-authentication host-mode multi-vlan** to enable MAC authentication multi-VLAN mode on a port.

Use **undo mac-authentication host-mode multi-vlan** to restore the default.

By default, the MAC authentication multi-VLAN mode is disabled on a port. A MAC authentication-enabled port forwards packets for an authenticated user only in the VLAN where the user's MAC address was authenticated.

The multi-VLAN mode enables the MAC authentication-enabled port to forward packets for the authenticated user in up to five VLANs at the same time without re-authentication.

Examples

```
# Enable MAC authentication multi-VLAN mode on port GigabitEthernet 1/0/2.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet 1/0/2] mac-authentication host-mode multi-vlan
```

Modified feature: Specifying multiple secondary HWTACACS servers

Feature change description

In this release, you can specify one primary HWTACACS server and up to 16 secondary HWTACACS servers in the same HWTACACS scheme. When the primary HWTACACS server is unreachable, the device uses a secondary HWTACACS server to process AAA requests.

You can configure a shared key for each HWTACACS server, primary or secondary. The device uses the shared keys to ensure secure communication with HWTACACS servers.

Command changes

Modified command: key (HWTACACS scheme view)

Syntax

key { **accounting** | **authentication** | **authorization** } [**cipher** | **simple**] *key*

Views

HWTACACS scheme view

Change description

Before modification:

- In non-FIPS mode, a plaintext shared key is a string of 1 to 64 characters and a ciphertext shared key is a string of 1 to 117 characters.
- In FIPS mode, a plaintext shared key is a string of 8 to 64 characters and a ciphertext shared key is a string of 8 to 117 characters.

After modification:

- In non-FIPS mode, a plaintext shared key is a string of 1 to 255 characters and a ciphertext shared key is a string of 1 to 373 characters.
- In FIPS mode, a plaintext shared key is a string of 8 to 255 characters and a ciphertext shared key is a string of 8 to 373 characters.

Modified command: primary accounting

Old syntax

primary accounting *ip-address* [*port-number* | **vpn-instance** *vpn-instance-name*] *

New syntax

primary accounting *ip-address* [*port-number* | **key** [**cipher** | **simple**] *key* | **vpn-instance** *vpn-instance-name*] *

Views

HWTACACS scheme view

Change description

The **key** [**cipher** | **simple**] *key* part is added to the **primary accounting** command. You can specify a shared key for secure communication between the device and the primary HWTACACS accounting server. Make sure the shared key configured on the device is the same as the one configured on the server.

- **cipher** *key*: Sets a ciphertext shared key. The *key* argument is case sensitive.
 - In non-FIPS mode, the key is a string of 1 to 373 characters.
 - In FIPS mode, the key is a string of 8 to 373 characters.
- **simple** *key*: Sets a plaintext shared key. The *key* argument is case sensitive.
 - In non-FIPS mode, the key is a string of 1 to 255 characters.
 - In FIPS mode, the key is a string of 8 to 255 characters and must contain digits, uppercase letters, lowercase letters, and special characters.

NOTE:

If you specify neither the **cipher** keyword nor the **simple** keyword, the shared key is set in plain text.

Modified command: primary authentication

Old syntax

primary authentication *ip-address* [*port-number* | **vpn-instance** *vpn-instance-name*] *

New syntax

primary authentication *ip-address* [*port-number* | **key** [**cipher** | **simple**] *key* | **vpn-instance** *vpn-instance-name*] *

Views

HWTACACS scheme view

Change description

The **key** [**cipher** | **simple**] *key* part is added to the **primary authentication** command. You can specify a shared key for secure communication between the device and the primary HWTACACS authentication server. Make sure the shared key configured on the device is the same as the one configured on the server.

- **cipher** *key*: Sets a ciphertext shared key. The *key* argument is case sensitive.
 - In non-FIPS mode, the key is a string of 1 to 373 characters.
 - In FIPS mode, the key is a string of 8 to 373 characters.
- **simple** *key*: Sets a plaintext shared key. The *key* argument is case sensitive.
 - In non-FIPS mode, the key is a string of 1 to 255 characters.
 - In FIPS mode, the key is a string of 8 to 255 characters and must contain digits, uppercase letters, lowercase letters, and special characters.

NOTE:

If you specify neither the **cipher** keyword nor the **simple** keyword, the shared key is set in plain text.

Modified command: primary authorization

Old syntax

primary authorization *ip-address* [*port-number* | **vpn-instance** *vpn-instance-name*] *

New syntax

primary authorization *ip-address* [*port-number* | **key** [**cipher** | **simple**] *key* | **vpn-instance** *vpn-instance-name*] *

Views

HWTACACS scheme view

Change description

The **key [cipher | simple]** key part is added to the **primary authorization** command. You can specify a shared key for secure communication between the device and the primary HWTACACS authorization server. Make sure the shared key configured on the device is the same as the one configured on the server.

- **cipher** key: Sets a ciphertext shared key. The *key* argument is case sensitive.
 - In non-FIPS mode, the key is a string of 1 to 373 characters.
 - In FIPS mode, the key is a string of 8 to 373 characters.
- **simple** key: Sets a plaintext shared key. The *key* argument is case sensitive.
 - In non-FIPS mode, the key is a string of 1 to 255 characters.
 - In FIPS mode, the key is a string of 8 to 255 characters and must contain digits, uppercase letters, lowercase letters, and special characters.

NOTE:

If you specify neither the **cipher** keyword nor the **simple** keyword, the shared key is set in plain text.

Modified command: secondary accounting

Old syntax

secondary accounting *ip-address* [*port-number* | **vpn-instance** *vpn-instance-name*] *

undo secondary accounting

New syntax

secondary accounting *ip-address* [*port-number* | **key [cipher | simple]** *key* | **vpn-instance** *vpn-instance-name*] *

undo secondary accounting [*ip-address*]

Views

HWTACACS scheme view

Change description

This command has the following modifications:

- The **key [cipher | simple]** key part is added to the **secondary accounting** command. You can use this command to specify a shared key for secure communication between the device and a secondary HWTACACS accounting server. Make sure the shared key configured on the device is the same as the one configured on that server.
 - **cipher** key: Sets a ciphertext shared key. The *key* argument is case sensitive.
 - In non-FIPS mode, the key is a string of 1 to 373 characters.
 - In FIPS mode, the key is a string of 8 to 373 characters.
 - **simple** key: Sets a plaintext shared key. The *key* argument is case sensitive.
 - In non-FIPS mode, the key is a string of 1 to 255 characters.
 - In FIPS mode, the key is a string of 8 to 255 characters and must contain digits, uppercase letters, lowercase letters, and special characters.

NOTE:

If you specify neither the **cipher** keyword nor the **simple** keyword, the shared key is set in plain text.

- The *ip-address* argument is added to the **undo secondary accounting** command. You can remove a secondary HWTACACS accounting server with this command by specifying its IP address.

Modified command: secondary authentication

Old syntax

secondary authentication *ip-address* [*port-number* | **vpn-instance** *vpn-instance-name*] *
undo secondary authentication

New syntax

secondary authentication *ip-address* [*port-number* | **key** [**cipher** | **simple**] *key* | **vpn-instance** *vpn-instance-name*] *
undo secondary authentication [*ip-address*]

Views

HWTACACS scheme view

Change description

This command has the following modifications:

- The **key** [**cipher** | **simple**] *key* part is added to the **secondary authentication** command. You can specify a shared key for secure communication between the device and a secondary HWTACACS authentication server. Make sure the shared key configured on the device is the same as the one configured on the server.
 - **cipher** *key*: Sets a ciphertext shared key. The *key* argument is case sensitive.
 - In non-FIPS mode, the key is a string of 1 to 373 characters.
 - In FIPS mode, the key is a string of 8 to 373 characters.
 - **simple** *key*: Sets a plaintext shared key. The *key* argument is case sensitive.
 - In non-FIPS mode, the key is a string of 1 to 255 characters.
 - In FIPS mode, the key is a string of 8 to 255 characters and must contain digits, uppercase letters, lowercase letters, and special characters.

NOTE:

If you specify neither the **cipher** keyword nor the **simple** keyword, the shared key is set in plain text.

- The *ip-address* argument is added to the **undo secondary authentication** command. You can remove a secondary HWTACACS authentication server with this command by specifying its IP address.

Modified command: secondary authorization

Old syntax

secondary authorization *ip-address* [*port-number* | **vpn-instance** *vpn-instance-name*] *
undo secondary authorization

New syntax

secondary authorization *ip-address* [*port-number* | **key** [**cipher** | **simple**] *key* | **vpn-instance** *vpn-instance-name*] *
undo secondary authorization [*ip-address*]

Views

HWTACACS scheme view

Change description

This command has the following modifications:

- The **key** [**cipher** | **simple**] *key* part is added to the **secondary authorization** command. You can specify a shared key for secure communication between the device and a secondary HWTACACS authorization server. Make sure the shared key configured on the device is the same as the one configured on the server.
 - **cipher key**: Sets a ciphertext shared key. The *key* argument is case sensitive.
 - In non-FIPS mode, the key is a string of 1 to 373 characters.
 - In FIPS mode, the key is a string of 8 to 373 characters.
 - **simple key**: Sets a plaintext shared key. The *key* argument is case sensitive.
 - In non-FIPS mode, the key is a string of 1 to 255 characters.
 - In FIPS mode, the key is a string of 8 to 255 characters and must contain digits, uppercase letters, lowercase letters, and special characters.

NOTE:

If you specify neither the **cipher** keyword nor the **simple** keyword, the shared key is set in plain text.

- The *ip-address* argument is added to the **undo secondary authorization** command. You can remove a secondary HWTACACS authorization server with this command by specifying its IP address.

Modified feature: Displaying brief interface information

Feature change description

The **description** keyword was added to the **display interface** command.

If the interface description includes more than 27 characters and the **brief** keyword is specified for the **display interface** command, you can use the **description** keyword to display the full interface description for interfaces. The **display interface** command displays information about interfaces, such as Ethernet interfaces, aggregate interfaces, VLAN interfaces, loopback interfaces, and the null interface.

Command changes

Modified command: display interface

Old syntax

```
display interface [ interface-type ] [ brief [ down ] ] [ | { begin | exclude | include } regular-expression ]
```

```
display interface interface-type interface-number [ brief ] [ | { begin | exclude | include } regular-expression ]
```

New syntax

```
display interface [ interface-type ] [ brief [ down | description ] ] [ | { begin | exclude | include } regular-expression ]
```

```
display interface interface-type interface-number [ brief [ description ] ] [ | { begin | exclude | include } regular-expression ]
```

Views

Any view

Change description

Before modification: The **display interface** command with the **brief** keyword specified displays at most the first 27 characters of an interface description.

After modification: If the interface description includes more than 27 characters and the **brief** keyword is specified for the **display interface** command, you must specify the **description** keyword to display the full description. Without the **description** keyword, the command displays only the first 27 characters.

Modified feature: Displaying brief IP configuration for Layer 3 interfaces

Feature change description

The **description** keyword was added to the **display interface brief** command.

If the interface description includes more than 12 characters, you can use this keyword to display the full interface description for Layer 3 interfaces.

Command changes

Modified command: display ip interface brief

Old syntax

```
display ip interface [ interface-type [ interface-number ] ] brief [ | { begin | exclude | include } regular-expression ]
```

New syntax

```
display ip interface [ interface-type [ interface-number ] ] brief [ description ] [ | { begin | exclude | include } regular-expression ]
```

Views

Any view

Change description

Before modification: If the interface description includes more than 12 characters, only the first 9 characters of an interface description are displayed, followed by an ellipsis (...).

After modification: If the interface description includes more than 12 characters, you must specify the **description** keyword to display the full description. Without the **description** keyword, only the first 9 characters are displayed, followed by an ellipsis (...).

Modified feature: Configuring static multicast MAC address entries

Feature change description

In this release, you can configure a multicast MAC address in the value range of 0100-5Exx-xxxx and 3333-xxxx-xxxx in a static multicast MAC address entry. The x octet represents an arbitrary hexadecimal number from 0 to F.

The multicast MAC addresses used in protocol packets are in this multicast MAC address range. If the multicast MAC address of a protocol packet matches a configured static multicast MAC address entry on the device, one of the following occurs:

- If the protocol packet needs to be processed by the CPU, the configuration of the static multicast MAC address entry does not take effect.
- If the protocol packet needs to be transparently transmitted by the device, the device forwards the packet through the outgoing port in the matching static multicast MAC address entry.

Command changes

Modified command: mac-address multicast

Syntax

In system view:

mac-address multicast *mac-address* **interface** *interface-list* **vlan** *vlan-id*

undo mac-address [**multicast**] [[*mac-address* [**interface** *interface-list*]] **vlan** *vlan-id*]

In Ethernet interface view or Layer 2 aggregate interface view:

mac-address multicast *mac-address* **vlan** *vlan-id*

undo mac-address [**multicast**] *mac-address* **vlan** *vlan-id*

In port group view:

mac-address multicast *mac-address* **vlan** *vlan-id*

undo mac-address multicast *mac-address* **vlan** *vlan-id*

Views

System view, Ethernet interface view, Layer 2 aggregate interface view, port group view

Change description

Before modification: The value of the *mac-address* argument is any legal multicast MAC address except 0100-5Exx-xxxx and 3333-xxxx-xxxx. A multicast MAC address is the MAC address in which the least significant bit of the most significant octet is 1.

After modification: The value of the *mac-address* argument is any legal multicast MAC address. A multicast MAC address is the MAC address in which the least significant bit of the most significant octet is 1.

Modified command: display mac-address multicast

Syntax

display mac-address [*mac-address* [**vlan** *vlan-id*]] [**multicast**] [**vlan** *vlan-id*] [**count**] [[**begin** | **exclude** | **include**] *regular-expression*]

Views

Any view

Change description

Before modification: The value of the *mac-address* argument is any legal multicast MAC address except 0100-5Exx-xxxx and 3333-xxxx-xxxx. A multicast MAC address is the MAC address in which the least signification bit of the most significant octet is 1.

After modification: The value of the *mac-address* argument is any legal multicast MAC address. A multicast MAC address is the MAC address in which the least signification bit of the most significant octet is 1.

R5205L01

This release has the following changes:

- [New feature: Multicast ND](#)
- [New feature: Configuring packet capture](#)
- [Modified feature: Configuring system information for the SNMP agent](#)

New feature: Multicast ND

Configuring multicast ND

Microsoft NLB is a load balancing technology for server clustering developed on Windows Server.

NLB supports load sharing and redundancy among servers within a cluster. To implement fast failover, NLB requires that the switch forwards network traffic to all servers or specified servers in the cluster, and each server filters out unexpected traffic. In a medium or small data center that uses the Windows Server operating system, the proper cooperation of the switch and NLB is very important. For more information about NLB, see the related documents for Windows Server.

Microsoft NLB provides the following packet sending modes to make the switch forward network traffic to all servers or specified servers:

- **Unicast mode**—NLB assigns each cluster member a common MAC address, which is the cluster MAC address, and changes the source MAC address of each sent packet. The switch cannot add the cluster MAC address to its MAC table. In addition, because the cluster MAC address is unknown to the switch, packets destined to it are forwarded on all ports of the switch.
- **Multicast mode**—NLB uses a multicast MAC address that is a virtual MAC address for network communication (for example 0300-5e11-1111).
- **Internet Group Management Protocol (IGMP) multicast mode**—The switch sends packets only out of the ports that connect to the cluster members rather than all ports.

NOTE:

Multicast ND is applicable to only multicast-mode NLB.

To configure multicast ND:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure a static neighbor entry.	ipv6 neighbor <i>ipv6-address mac-address vlan-id port-type port-number</i> [vpn-instance <i>vpn-instance-name</i>]	Optional.
3. Configure a static multicast MAC address entry.	mac-address multicast <i>mac-address interface interface-list vlan vlan-id</i>	No static multicast MAC address entries exist by default.

Command reference

For more information about the **mac-address multicast** command, see *HP 5500 HI Switch Series IP Multicast Command Reference-Release 5203*.

For more information about the **ipv6 neighbor** command, see *HP 5500 HI Switch Series Layer 3—IP Services Command Reference—Release 5203*.

New feature: Configuring packet capture

The packet capture feature facilitates network problem identification. Packets captured are stored in the packet capture buffer on the device. You can display the packets at the CLI, or export them to a **.pcap** file and analyze them by using packet analysis software such as Ethereal or Wireshark.

Configuring the packet capture function

When you configure this function, follow these guidelines:

- After you enable packet capture which uses an ACL, you cannot modify the ACL rules, including adding, deleting, and modifying rules.
- When you enable packet capture which uses an ACL, the actions in the ACL are ignored, and the ACL is only used for traffic classification.
- To release system resources after finishing packet capture, use the **undo packet capture** command to disable this function.

To configure the packet capture function:

Step	Command	Remarks
1. Set packet capture parameters.	packet capture { acl { acl-number ipv6 acl6-number } buffer-size size length capture-length mode { circular linear } }*	Optional.
2. Enable packet capture.	<ul style="list-style-type: none"> • (Approach 1) Start packet capture immediately: packet capture start [acl { acl-number ipv6 acl6-number } buffer-size size length capture-length mode { circular linear }] [packets packet-number seconds second-number]* • (Approach 2) Configure a packet capture schedule: packet capture schedule datetime time date 	<p>Use either approach.</p> <p>You can set packet capture parameters at the same time when you use approach 1.</p> <p>By default, packet capture is disabled, and no packet capture schedule is configured.</p> <p>If you use approach 1, the existing packet capture schedule is invalid.</p>
3. Stop packet capture.	packet capture stop	<p>Optional.</p> <p>Stop packet capture before you display, save, or clear the buffered contents.</p> <p>The device automatically stops packet capture when:</p> <ul style="list-style-type: none"> • The packet capture function operates in linear mode, and the packet capture buffer is full. • The number of packets captured exceeds the upper limit. • The duration of the packet capture process exceeds the upper limit.

Step	Command	Remarks
4. Save the contents in the packet capture buffer.	packet capture buffer save [<i>filename</i>]	Optional. Save the file with a filename in .pcap format.

Displaying and maintaining packet capture

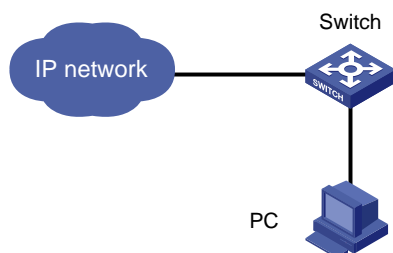
Task	Command	Remarks
Display the current packet capture status.	display packet capture status	Available in any view.
Display the buffered contents.	display packet capture buffer [<i>start-index</i> [<i>end-index</i>]] [length <i>display-length</i>]	Available in any view.
Clear the buffered contents.	reset packet capture buffer	Available in user view.

Packet capture configuration example

Network requirements

As shown in [Figure 11](#), the switch captures the packets from 192.168.1.0/24, and saves the result in a **.pcap** file so that the PC can download the file for packet analysis.

Figure 13 Network diagram



Configuration procedure

1. Enable the packet capture function on the switch:
 - # Create an ACL rule for IPv4 basic ACL 2000 to permit packets with a source address in 192.168.1.0/24.

```

<Switch> system-view
[Switch] acl number 2000
[Switch-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Switch-acl-basic-2000] quit
[Switch] quit

```

 - # Configure the switch to capture packets based on ACL 2000, and start packet capture immediately.

```

<Switch> packet capture start acl 2000

```

 - # Display the packet capture status.

```

<Switch> display packet capture status
Current status :      In process
Mode :              Linear

```

```

Buffer size :          2097152 (bytes)
Buffer used :          1880 (bytes)
Max capture length :   68 (bytes)
ACL information :      Basic or advanced IPv4 ACL 2000
Schedule datetime:     Unspecified
Upper limit of duration : Unspecified (seconds)
Duration :             13 (seconds)
Upper limit of packets : Unspecified
Packets count :        10

```

The output shows that packet capture is ongoing.

2. Save the packet capture result:

Stop packet capture.

```
<Switch> packet capture stop
```

Save the contents in the packet capture buffer to file **test.pcap**.

```
<Switch> packet capture buffer save test.pcap
```

Display the contents and file information in the current directory.

```
<Switch> dir
```

Directory of flash:/

```

0      -rw-      1860  Sep 21 2012 12:52:58  test.pcap
1      drw-      -    Apr 26 2012 12:00:38  seclog
2      -rw- 10479398  Apr 26 2012 12:26:39  logfile.log

```

The output shows that the buffered contents are successfully saved.

Stop packet capture, and release system resources after packet capture is completed.

```
<Switch> undo packet capture
```

The PC can access the switch through FTP or TFTP, save file **test.pcap**, and analyze the packets through packet analysis software such as Wireshark.

Packet capture configuration commands

display packet capture buffer

Syntax

```
display packet capture buffer [ start-index [ end-index ] ] [ length display-length ]
```

View

Any view

Default level

1: Monitor level

Parameters

start-index: Specifies a start packet record by its index in the packet capture buffer. If you do not specify this argument, the earliest packet record is displayed the first in the packet capture buffer by default.

end-index: Specifies an end packet record by its index in the packet capture buffer. If you do not specify this argument, the latest packet record is displayed the last in the packet capture buffer by default.

length *display-length*: Specifies the maximum length of data that can be displayed for a single packet record, in the range of 14 to 256 bytes. The default value is 68.

Description

Use **display packet capture buffer** to display the contents in the packet capture buffer.

- If you do not specify any option, the command displays all packet records in the packet capture buffer.
- This command limits the length of data that can be displayed for a single packet record. To display complete packet records, use the **packet capture buffer save** command to save the contents in a **.pcap** file, and display the contents by using the corresponding software.
- Do not use this command during the packet capturing process.

Related commands: **packet capture start** and **packet capture buffer save**.

Examples

Display all contents in the packet capture buffer.

```
<Sysname> display packet capture buffer
2012-07-26 12:03:15:318  Index 1  GE1/0/2  64 (original 64) Bytes captured
  01 80 c2 00 00 03 1c bd b9 e3 b5 02 81 00 00 01
  88 8e 01 01 00 00 00 00 00 00 00 00 00 00 00
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
2012-07-26 12:03:25:749  Index 2  GE1/0/2  68 (original 90) Bytes captured
  33 33 00 00 00 12 00 00 5E 00 02 50 86 DD 6E 00
  00 00 00 20 70 FF FE 80 00 00 00 00 00 00 00 00
  00 00 00 00 00 81 FF 02 00 00 00 00 00 00 00 00
  00 00 00 00 00 12 31 50 64 01 02 58 6A AE FE 80
  00 00 00 00
```

display packet capture status

Syntax

display packet capture status

View

Any view

Default level

1: Monitor level

Parameters

None

Description

Use **display packet capture status** to display the current packet capture status.

Examples

Display the current packet capture status.

```
<Sysname> display packet capture status
Current status :      In process
Mode :              Linear
Buffer size :       2097152 (bytes)
Buffer used :        0 (bytes)
```

```

Max capture length :      68 (bytes)
ACL information :         Ethernet frame header ACL 4200
Schedule datetime:       Unspecified
Upper limit of duration : Unspecified (seconds)
Duration :               60 (seconds)
Upper limit of packets :  Unspecified
Packets count :          0

```

Table 15 Command output

Field	Description
Current status	Packet capture status: <ul style="list-style-type: none"> • In process—The packet capturing process is ongoing. • Scheduled—The packet capture schedule is configured, but does not start. • Paused—Packet capture is stopped temporarily, and you can display, save, and clear the contents in the packet capture buffer.
Mode	Packet capture mode: <ul style="list-style-type: none"> • Linear. • Circular.
Buffer size	Packet capture buffer size.
Buffer used	Packet capture buffer size in use. One packet record comprises a packet header that records the incoming port, capture time, length of the captured packet and the actual length of the packet, and the data, so it occupies more buffer memory than the maximum captured data.
Max capture length	Maximum length of the packet that can be stored in the packet buffer.
ACL information	ACL type and number for packet capture.
Schedule datetime	Start time of the packet capture schedule.
Upper limit of duration	Upper limit of the packet capture duration.
Duration	Packet capture duration.
Upper limit of packets	Maximum number of packets that can be captured.
Packets count	Number of packets that has been captured.

packet capture

Syntax

```

packet capture { acl { acl-number | ipv6 acl6-number } | buffer-size size | length capture-length |
mode { circular | linear } }*

```

```

undo packet capture [ acl | buffer-size | length | mode ]

```

View

User view

Default level

1: Monitor level

Parameters

acl: Specifies an ACL for packet capture. If you do not specify this keyword, this command captures all packets that the device receives.

acl-number: Specifies the number of an IPv4 ACL:

- 2000 to 2999 for IPv4 basic ACLs
- 3000 to 3999 for IPv4 advanced ACLs
- 4000 to 4999 for Ethernet frame header ACLs

acl6-number: Specifies the number of an IPv6 ACL:

- 2000 to 2999 for IPv6 basic ACLs
- 3000 to 3999 for IPv6 advanced ACLs

buffer-size size: Specifies the packet capture buffer size in the range of 32 to 65535 KB. The default value is 2048.

length capture-length: Specifies the maximum length of the packet that can be stored in the packet buffer, calculated from the first byte of the packet, in the range of 16 to 4000 bytes. The default value is 68. The data out of the range of the maximum length is not recorded.

circular: Specifies the circular packet capture mode. In this mode, packet capture continues even if the buffer is full, and the newly captured packet overwrites the previous records, starting from the earliest one.

linear: Specifies the linear packet capture mode. In this mode, packet capture pauses when the buffer is full. The default mode is linear mode.

Description

Use **packet capture** to set packet capture parameters.

Use **undo packet capture** to restore the default settings, and disable the packet capture function.

- Do not change packet capture parameters during the packet capturing process.
- If you specify a keyword for the **undo packet capture** command, the command restores the default setting for the specified keyword. If you do not specify any keyword, the command restores the default settings for all keywords, and disables the packet capture function.
- After you enable packet capture which uses an ACL, you cannot modify the ACL rules, including adding, deleting, and modifying rules.
- When you enable packet capture which uses an ACL, the actions in the ACL are ignored, and the ACL is only used for traffic classification.

Related commands: **packet capture start**.

Examples

Set the size of the packet capture buffer to 4096 KB, the source address of packets to be captured to 192.168.1.0/24, and start packet capture immediately.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] quit
<Sysname> packet capture buffer-size 4096
<Sysname> packet capture acl 2000
<Sysname> packet capture start
```

Restore the default settings for packet capture parameters, and disable packet capture.

```
<Sysname> undo packet capture
```


packet capture buffer save

Syntax

packet capture buffer save [*filename*]

View

User view

Default level

1: Monitor level

Parameters

filename: Specifies the name of the file to be saved. The filename cannot contain special characters such as backslash (\), slash (/), colon (:), asterisk (*), quotation marks (" "), single quotes(' '), less-than sign (<), greater-than sign (>), tildes (~), and vertical bar (|). If you do not specify this argument, the command saves the file in the default filename **pcapbuffer.pcap**.

Description

Use **packet capture buffer save** to save the contents in the packet capture buffer.

- Save the file with a filename in the **.pcap** format.
- Do not use this command during the packet capturing process.

Related commands: **packet capture**.

Examples

Save the contents in the packet capture buffer to file **example.pcap**.

```
<Sysname> packet capture buffer save example.pcap
```

packet capture schedule

Syntax

packet capture schedule datetime *time date*

undo packet capture schedule

View

User view

Default level

1: Monitor level

Parameters

time: Sets the time in the format of **HH:MM:SS**. **HH** takes a value range of 0 to 23, and **MM** and **SS** take a value range of 0 to 59.

date: Sets the date in the format of **MM/DD/YYYY** or **YYYY/MM/DD**. **MM** takes a value range of 1 to 12, **YYYY** takes a value range of 2000 to 2035, and the value range of **DD** depends on which month the day is in.

Description

Use **packet capture schedule** to configure a packet capture schedule.

Use **undo packet capture schedule** to invalidate the configured packet capture schedule.

By default, no packet capture schedule is configured.

- You can use the **packet capture start** command to enable packet capture as in this command.

- You can use the **packet capture** command to change packet capture parameters before the packet capture schedule starts, or use the **packet capture start** command to start packet capture immediately, and the existing packet capture schedule is invalidated.
- To disable packet capture and invalidate the configured packet capture schedule, execute the **undo packet capture start** command or the **undo packet capture** command without any keyword.

Related commands: **packet capture**.

Examples

Configure a packet capture schedule.

```
<Sysname> packet capture schedule datetime 12:00:00 2012/12/25
```

packet capture start

Syntax

```
packet capture start [ acl { acl-number | ipv6 acl6-number } | buffer-size size | length capture-length | mode { circular | linear } | [ packets packet-number | seconds second-number ] ]*
undo packet capture start
```

View

User view

Default level

1: Monitor level

Parameters

acl: Specifies an ACL for packet capture. If you do not specify this keyword, this command captures all packets that the device receives.

acl-number: Specifies the number of an IPv4 ACL:

- 2000 to 2999 for IPv4 basic ACLs
- 3000 to 3999 for IPv4 advanced ACLs
- 4000 to 4999 for Ethernet frame header ACLs

acl6-number: Specifies the number of an IPv6 ACL:

- 2000 to 2999 for IPv6 basic ACLs
- 3000 to 3999 for IPv6 advanced ACLs

buffer-size *size*: Specifies the packet capture buffer size in the range of 32 to 65535 KB. The default value is 2048.

length *capture-length*: Specifies the maximum length of the packet that can be stored in the packet buffer, calculated from the first byte of the packet, in the range of 16 to 4000 bytes. The default value is 68. The data out of the range of the maximum length is not recorded.

circular: Specifies the circular packet capture mode. In this mode, packet capture continues even if the buffer is full, and the newly captured packet overwrites the previous records, starting from the earliest one.

linear: Specifies the linear packet capture mode. In this mode, packet capture pauses when the buffer is full. The default mode is linear mode.

packets *packet-number*: Sets the upper limit of packets that can be captured, in the range of 1 to 4294967295. The default value is 4294967295. Packet capture pauses when the number of captured packets reaches the upper limit.

seconds *second-number*. Sets the upper limit for packet capture duration, in the range of 1 to 4294967295 seconds. The default value is 4294967295 seconds. Packet capture pauses when the packet capture duration reaches the upper limit.

Description

Use **packet capture start** to start packet capture, and set packet capture parameters at the same time.

Use **undo packet capture start** to disable packet capture.

By default, packet capture is disabled.

- Do not start packet capture again or change parameters, or use the **display packet capture buffer**, **reset packet capture buffer** and **packet capture buffer save** commands during the packet capturing process. To do so, use the **packet capture stop** command to temporarily stop packet capture.
- If packet capture is enabled and an ACL number is specified, but the specified ACL does not exist, no packet is captured. If you modify the ACL rule for the specified ACL, the result of packet capture is not affected. The modified ACL rule takes effect after the **packet capture start** command is successfully executed.
- The **undo packet capture start** command stops packet capture, but the packet capture parameters configured are still effective, and you do not need to reconfigure them when you start packet capture again.

Related commands: **packet capture stop**, **display packet capture status**, and **display packet capture buffer**.

Examples

Set the maximum length of the packet captured as 256 bytes, and start packet capture.

```
<Sysname> packet capture length 256 start
```

packet capture stop

Syntax

packet capture stop

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use **packet capture stop** to temporarily stop packet capture.

- After packet capture is stopped, if you use the **packet capture** command to change packet capture parameters, the contents in the capture buffer are cleared.
- This command does not take effect if packet capture is not started.
- After packet capture is stopped, you can use the **display packet capture buffer**, **reset packet capture buffer**, or **packet capture buffer save** command to display or perform operations on the contents in the packet capture buffer, and use the **packet capture start** command to start packet capture again.

Related commands: **packet capture**, **packet capture start**, **display packet capture buffer**, **reset packet capture buffer**, and **packet capture buffer save**.

Examples

```
# Stop packet capture.  
<Sysname> packet capture stop
```

reset packet capture buffer

Syntax

reset packet capture buffer

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use **reset packet capture buffer** to clear the contents in the packet capture buffer.

Do not use this command during the packet capturing process.

Related commands: **packet capture start**.

Examples

```
# Clear the contents in the packet capture buffer.  
<Sysname> reset packet capture buffer
```

Modified feature: Configuring system information for the SNMP agent

Feature change description

Modify the maximum string length of the *sys-contact* and *sys-location* arguments.

Command changes

Modified command: snmp-agent sys-info

Syntax

```
snmp-agent sys-info { contact sys-contact | location sys-location | version { all | { v1 | v2c | v3 }* } }
```

Views

System view

Change description

Before modification: Both the *sys-contact* and *sys-location* arguments specify a string of 1 to 200 characters.

After modification: Both the *sys-contact* and *sys-location* arguments specify a string of 1 to 255 characters.

R5203P01

This release has no feature changes.

R5203

This chapter includes following contents:

- Modified feature: Enabling/disabling FIPS mode
- Modified feature: Setting the maximum number of the IPv4/IPv6 source guard binding entries on a port
- Modified feature: Setting the IRF link down report delay
- Modified feature: Setting the minimum password length
- Modified feature: Switching the user privilege level
- Modified feature: Upgrading a subordinate member
- Modified feature: Implementing ACL-based IPsec
- Modified feature: Cluster management
- Deleted feature: Disabling Boot ROM access

Modified feature: Enabling/disabling FIPS mode

Feature change description

Added prompt information for the **fips mode enable** and **undo fips mode enable** commands:

```
[Sysname] fips mode enable
FIPS mode change requires a device reboot. Continue?[Y/N]:y
Change the configuration to meet FIPS mode requirements, save the configuration to the
next-startup configuration file, and then reboot to enter FIPS mode.
[Sysname] undo fips mode enable
FIPS mode change requires a device reboot. Continue?[Y/N]:y
Change the configuration to meet non-FIPS mode requirements, save the configuration to
the next-startup configuration file, and then reboot to enter non-FIPS mode.
```

Command changes

None

Modified feature: Setting the maximum number of the IPv4/IPv6 source guard binding entries on a port

Feature change description

Changed the maximum number of the IPv4 and IPv6 source guard binding entries on a port.

Command changes

Modified command: ip verify source max-entries

Syntax

ip verify source max-entries *number*

Views

Layer 2 Ethernet interface view

Change description

Before modification: The value range for the *number* argument is 0 to 1500.

After modification: The value range for the *number* argument is 0 to 2048.

Modified command: ipv6 verify source max-entries

Syntax

ipv6 verify source max-entries *number*

Views

Layer 2 Ethernet interface view

Change description

Before modification: The value range for the *number* argument is 0 to 1500.

After modification: The value range for the *number* argument is 0 to 2048.

Modified feature: Setting the IRF link down report delay

Feature change description

Changed the value range of the *interval* argument.

Command changes

Modified command: irf link-delay

Syntax

irf link-delay *interval*

Views

System view

Change description

Before modification: The value range (in milliseconds) for the *interval* argument is 0 to 3000.

After modification: The value range (in milliseconds) for the *interval* argument is 0 to 10000.

Modified feature: Setting the minimum password length

Feature change description

Changed the value range of the minimum password length.

Command changes

Modified command: password-control length

Syntax

password-control length *length*

undo password-control length

Views

System view, user group view, local user view

Change description

Before modification: The value range for the *length* argument is 8 to 32.

After modification: The value range for the *length* argument is 8 to 32 in FIPS mode and 4 to 32 in non-FIPS mode.

Modified feature: Switching the user privilege level

Feature change description

Changed the user privilege level switching control mechanism.

Command changes

Modified command: super

Syntax

super [*level*]

Views

User view

Change description

Before modification: If a scheme authentication user fails to provide the correct password for the higher privilege level during 3 consecutive attempts, the system does not lock the switching function.

After modification: If a scheme authentication user fails to provide the correct password for the higher privilege level during 5 consecutive attempts, the system locks the switching function, and the user must wait 15 minutes before trying again. Trying again before the 15-minute period elapses restores the wait timer to 15 minutes and restarts the timer.

Modified feature: Upgrading a subordinate member

Feature change description

Changed the value range of the absolute-path string length for the *upgrading-filename* argument.

Command changes

Modified command: `issu load`

Syntax

issu load file *upgrading-filename* **slot** *slot-number* [**force**]

Views

System view

Change description

Before modification: The absolute-path string length for the *upgrading-filename* argument must be in the range of 1 to 136.

After modification: The absolute-path string length for the *upgrading-filename* argument must be in the range of 1 to 63.

Modified feature: Implementing ACL-based IPsec

Feature change description

ACL-based IPsec can protect only traffic that is generated by the device and traffic that is destined for the device. You cannot use an ACL-based IPsec tunnel to protect user traffic. In the ACL that is used to identify IPsec protected traffic, ACL rules that match traffic forwarded through the device do not take effect. For example, an ACL-based IPsec tunnel can protect log messages the device sends to a log server, but it cannot protect traffic that is forwarded by the device for two hosts, even if the host-to-host traffic matches an ACL permit rule.

IKE-based IPsec tunnel for IPv4 packets configuration example

Network requirements

As shown in [Figure 1](#), configure an IPsec tunnel between Switch A and Switch B to protect data flows between Switch A and Switch B. Configure the tunnel to use the security protocol ESP, the encryption algorithm AES-CBC-128, and the authentication algorithm HMAC-SHA1-96.

Figure 1 Network diagram



Configuration procedure

1. Configure Switch A:

Assign an IP address to VLAN-interface 1.

```
<SwitchA> system-view
```

```

[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 2.2.2.1 255.255.255.0
[SwitchA-Vlan-interface1] quit

# Define an ACL to identify data flows from Switch A to Switch B.
[SwitchA] acl number 3101
[SwitchA-acl-adv-3101] rule 0 permit ip source 2.2.2.1 0 destination 2.2.3.1 0
[SwitchA-acl-adv-3101] rule 5 permit ip source 2.2.3.1 0 destination 2.2.2.1 0
[SwitchA-acl-adv-3101] quit

# Create an IPsec proposal named tran1.
[SwitchA] ipsec proposal tran1

# Specify the encapsulation mode as tunnel.
[SwitchA-ipsec-proposal-tran1] encapsulation-mode tunnel

# Specify the security protocol as ESP.
[SwitchA-ipsec-proposal-tran1] transform esp

# Specify the algorithms for the proposal.
[SwitchA-ipsec-proposal-tran1] esp encryption-algorithm aes 128
[SwitchA-ipsec-proposal-tran1] esp authentication-algorithm sha1
[SwitchA-ipsec-proposal-tran1] quit

# Configure the IKE peer.
[SwitchA] ike peer peer
[SwitchA-ike-peer-peer] pre-shared-key Ab12<><>
[SwitchA-ike-peer-peer] remote-address 2.2.3.1
[SwitchA-ike-peer-peer] quit

# Create an IPsec policy that uses IKE for IPsec SA negotiation.
[SwitchA] ipsec policy map1 10 isakmp

# Apply the IPsec proposal.
[SwitchA-ipsec-policy-isakmp-map1-10] proposal tran1

# Apply the ACL.
[SwitchA-ipsec-policy-isakmp-map1-10] security acl 3101

# Apply the IKE peer.
[SwitchA-ipsec-policy-isakmp-map1-10] ike-peer peer
[SwitchA-ipsec-policy-isakmp-map1-10] quit

# Apply the IPsec policy group to VLAN-interface 1.
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ipsec policy map1

```

2. Configure Switch B:

```

# Assign an IP address to VLAN-interface 1.
<SwitchB> system-view
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 2.2.3.1 255.255.255.0
[SwitchB-Vlan-interface1] quit

# Define an ACL to identify data flows from Switch B to Switch A.
[SwitchB] acl number 3101
[SwitchB-acl-adv-3101] rule 0 permit ip source 2.2.3.1 0 destination 2.2.2.1 0
[SwitchB-acl-adv-3101] rule 5 permit ip source 2.2.2.1 0 destination 2.2.3.1 0

```

```

[SwitchB-acl-adv-3101] quit
# Create an IPsec proposal named tran1.
[SwitchB] ipsec proposal tran1
# Specify the encapsulation mode as tunnel.
[SwitchB-ipsec-proposal-tran1] encapsulation-mode tunnel
# Specify the security protocol as ESP.
[SwitchB-ipsec-proposal-tran1] transform esp
# Specify the algorithms for the proposal.
[SwitchB-ipsec-proposal-tran1] esp encryption-algorithm aes 128
[SwitchB-ipsec-proposal-tran1] esp authentication-algorithm sha1
[SwitchB-ipsec-proposal-tran1] quit
# Configure the IKE peer.
[SwitchB] ike peer peer
[SwitchB-ike-peer-peer] pre-shared-key Ab12<><>
[SwitchB-ike-peer-peer] remote-address 2.2.2.1
[SwitchB-ike-peer-peer] quit
# Create an IPsec policy that uses IKE for IPsec SA negotiation.
[SwitchB] ipsec policy use1 10 isakmp
# Apply the ACL.
[SwitchB-ipsec-policy-isakmp-use1-10] security acl 3101
# Apply the IPsec proposal.
[SwitchB-ipsec-policy-isakmp-use1-10] proposal tran1
# Apply the IKE peer.
[SwitchB-ipsec-policy-isakmp-use1-10] ike-peer peer
[SwitchB-ipsec-policy-isakmp-use1-10] quit
# Apply the IPsec policy group to VLAN-interface 1.
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ipsec policy use1

```

3. Verifying the configuration

After the previous configuration, send traffic from Switch B to Switch A. Switch A starts IKE negotiation with Switch B when receiving the first packet. If IKE negotiation is successful and SAs are set up, the traffic between the two switches will be IPsec protected.

IKE configuration example

Network requirements

As shown in [Figure 2](#), configure an IPsec tunnel that uses IKE negotiation between Switch A and Switch B to secure the communication between the two switches.

For Switch A, configure an IKE proposal that uses the sequence number 10 and the authentication algorithm SHA1. Configure Switch B to use the default IKE proposal.

Configure the two routers to use the pre-shared key authentication method.

Figure 2 Network diagram



Configuration procedure

1. Make sure Switch A and Switch B can reach each other.
2. Configure Switch A:

Assign an IP address to VLAN-interface 1.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-vlan-interface1] ip address 1.1.1.1 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

Configure ACL 3101 to identify traffic from Switch A to Switch B..

```
[SwitchA] acl number 3101
[SwitchA-acl-adv-3101] rule 0 permit ip source 1.1.1.1 0 destination 2.2.2.2 0
[SwitchA-acl-adv-3101] rule 1 permit ip source 2.2.2.2 0 destination 1.1.1.1 0
[SwitchA-acl-adv-3101] quit
```

Create IPsec proposal **tran1**.

```
[SwitchA] ipsec proposal tran1
```

Set the packet encapsulation mode to tunnel.

```
[SwitchA-ipsec-proposal-tran1] encapsulation-mode tunnel
```

Use security protocol ESP.

```
[Switch-ipsec-proposal-tran1] transform esp
```

Specify encryption and authentication algorithms.

```
[SwitchA-ipsec-proposal-tran1] esp encryption-algorithm aes 128
[SwitchA-ipsec-proposal-tran1] esp authentication-algorithm sha1
[SwitchA-ipsec-proposal-tran1] quit
```

Create an IKE proposal numbered 10.

```
[SwitchA] ike proposal 10
```

Set the authentication algorithm to **SHA1**.

```
[SwitchA-ike-proposal-10] authentication-algorithm sha
```

Configure the authentication method as pre-shared key.

```
[SwitchA-ike-proposal-10] authentication-method pre-share
```

Set the ISAKMP SA lifetime to 5000 seconds.

```
[SwitchA-ike-proposal-10] sa duration 5000
[SwitchA-ike-proposal-10] quit
```

Create IKE peer **peer**.

```
[SwitchA] ike peer peer
```

Configure the IKE peer to reference IKE proposal 10.

```
[SwitchA-ike-peer-peer] proposal 10
```

Set the pre-shared key.

```
[SwitchA-ike-peer-peer] pre-shared-key Ab12<><>
```

Specify the IP address of the peer security gateway.

```

[SwitchA-ike-peer-peer] remote-address 2.2.2.2
[SwitchA-ike-peer-peer] quit

# Create an IPsec policy that uses IKE negotiation.
[SwitchA] ipsec policy map1 10 isakmp

# Reference IPsec proposal tran1.
[SwitchA-ipsec-policy-isakmp-map1-10] proposal tran1

# Reference ACL 3101 to identify the protected traffic.
[SwitchA-ipsec-policy-isakmp-map1-10] security acl 3101

# Reference IKE peer peer.
[SwitchA-ipsec-policy-isakmp-map1-10] ike-peer peer
[SwitchA-ipsec-policy-isakmp-map1-10] quit

# Apply the IPsec policy to VLAN-interface 1.
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ipsec policy map1

3. Configure Switch B:

# Assign an IP address to VLAN-interface 1.
<SwitchB> system-view
[SwitchB] interface Vlan-interface1
[SwitchB-Vlan-interface1] ip address 2.2.2.2 255.255.255.0
[SwitchB-Vlan-interface1] quit

# Configure ACL 3101 to identify traffic from Switch B to Switch A.
[SwitchB] acl number 3101
[SwitchB-acl-adv-3101] rule 0 permit ip source 2.2.2.2 0 destination 1.1.1.0 0
[SwitchB-acl-adv-3101] rule 1 permit ip source 1.1.1.1 0 destination 2.2.2.2 0
[SwitchB-acl-adv-3101] quit

# Create IPsec proposal tran1.
[SwitchB] ipsec proposal tran1

# Set the packet encapsulation mode to tunnel.
[SwitchB-ipsec-proposal-tran1] encapsulation-mode tunnel

# Use security protocol ESP.
[SwitchB-ipsec-proposal-tran1] transform esp

# Specify encryption and authentication algorithms.
[SwitchB-ipsec-proposal-tran1] esp encryption-algorithm aes 128
[SwitchB-ipsec-proposal-tran1] esp authentication-algorithm sha1
[SwitchB-ipsec-proposal-tran1] quit

# Create an IKE proposal numbered 10.
[SwitchB] ike proposal 10

# Set the authentication algorithm to SHA1.
[SwitchB-ike-proposal-10] authentication-algorithm sha

# Configure the authentication method as pre-shared key.
[SwitchB-ike-proposal-10] authentication-method pre-share

# Set the ISAKMP SA lifetime to 5000 seconds.
[SwitchB-ike-proposal-10] sa duration 5000
[SwitchB-ike-proposal-10] quit

```

```

# Create IKE peer peer.
[SwitchB] ike peer peer

# Configure the IKE peer to reference IKE proposal 10.
[SwitchB-ike-peer-peer] proposal 10

# Set the pre-shared key.
[SwitchB-ike-peer-peer] pre-shared-key Ab12<><>

# Specify the IP address of the peer security gateway.
[SwitchB-ike-peer-peer] remote-address 1.1.1.1
[SwitchB-ike-peer-peer] quit

# Create an IPsec policy that uses IKE negotiation.
[SwitchB] ipsec policy use1 10 isakmp

# Reference IPsec proposal tran1.
[SwitchB-ipsec-policy-isakmp-use1-10] proposal tran1

# Reference ACL 3101 to identify the protected traffic.
[SwitchB-ipsec-policy-isakmp-use1-10] security acl 3101

# Reference IKE peer peer.
[SwitchB-ipsec-policy-isakmp-use1-10] ike-peer peer
[SwitchB-ipsec-policy-isakmp-use1-10] quit

# Apply the IPsec policy to VLAN-interface 1.
[SwitchB-Vlan-interface1] ipsec policy use1

```

Verifying the configuration

After the above configuration, send traffic from Switch B to Switch A. Switch A starts IKE negotiation with Switch B when receiving the first packet. IKE proposal matching starts with the one having the highest priority. During the matching process, lifetime is not involved but it is determined by the IKE negotiation parties.

Command changes

None

Modified feature: Cluster management

Cluster management is not supported in FIPS mode.

Deleted feature: Disabling Boot ROM access

Feature change description

The **undo startup bootrom-access enable** command was deleted and Boot ROM access cannot be disabled.

Command changes

Modified command: undo startup bootrom-access enable

Syntax

startup bootrom-access enable

undo startup bootrom-access enable

Views

User view

E5201

This chapter includes following contents:

- New feature: Configuring a user validity check rule
- New feature: Enabling source IP conflict prompt
- New feature: Supporting IPv6 routes with a prefix length over 64
- New feature: BGP MDT
- New feature: Configuring the maximum number of selected ports allowed for an aggregation group
- New feature: Enabling MAC address migration log notifying
- New feature: Disabling MAC entry aging timer refresh based on destination MAC address
- New feature: PoE power negotiation through Power Via MDI TLV (supported only on PoE-capable switches)
- New feature: Specifying a destination server in a VPN for UDP helper
- New feature: Supporting using a self-signed certificate for HTTPS
- New feature: Setting the maximum number of 802.1X authentication attempts for MAC authentication users
- New feature: Support of 802.1X for issuing VLAN groups
- New feature: Setting the deletion delay time for SAVI
- New feature: Setting a DSCP value for an ISP domain
- New feature: Advanced packet filtering logging
- New feature: PoE
- New feature: Supporting automatically creating RSA key pairs or SSH
- Modified feature: SCP server name
- Modified feature: Configuring portal-free rules to support TCP/UDP port numbers
- Modified feature: Setting the time to wait for a DAD NS from a DHCPv6 client
- Modified feature: Support of voice VLAN for 128 OUI addresses
- Modified feature: Configuring CDP compatibility
- Modified feature: ping ipv6
- Modified feature: Configuring the maximum number of operations that an NQA client can simultaneously perform
- Modified feature: Configuring parameters for an sFlow collector
- Modified feature: Configuring load-sharing criteria for a link aggregation group
- Modified feature: Implementing ACL-based IPsec
- Modified feature: Setting the IRF link down report delay
- Modified feature: Configuring the ABR to advertise a default route to the stub area

New feature: Configuring a user validity check rule

Configuring a user validity check rule

User validity check is supported in this version. With ARP detection enabled, if a user validity check rule is configured, it applies first. The device checks the packet against the configured rules. If a match is found, the ARP packet is processed according to the matching rule. If no match is found, the device checks the packet against static IP source guard binding entries, DHCP snooping entries, 802.1X security entries, and OUI MAC addresses.

Configuration procedure

To configure user validity check:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set rules for user validity check.	arp detection <i>id-number</i> { permit deny } ip { any <i>ip-address</i> [<i>ip-address-mask</i>] } mac { any <i>mac-address</i> [<i>mac-address-mask</i>] } [vlan <i>vlan-id</i>]	Optional. By default, no rule is configured.
3. Enter VLAN view.	vlan <i>vlan-id</i>	N/A
4. Enable ARP detection for the VLAN.	arp detection enable	By default, ARP detection is disabled. For more information about the command, see <i>Security Command Reference</i> .

Command reference

arp detection

Syntax

arp detection *id-number* { **permit** | **deny** } **ip** { **any** | *ip-address* [*ip-address-mask*] } **mac** { **any** | *mac-address* [*mac-address-mask*] } [**vlan** *vlan-id*]

undo arp detection *id-number*

View

System view

Default level

2: System level

Parameters

id-number: Specifies the ID of the rule, in the range of 0 to 511. A lower value refers to a higher priority.

deny: Denies ARP packets matching the rule.

permit: Permit ARP packets matching the rule.

ip { **any** | *ip-address* [*ip-address-mask*] }: Specifies an IP address range for matching sender IP addresses of ARP packets.

- **any**: Matches any sender IP address.
- **ip-address**: Matches the specified sender IP address.
- **ip-address-mask**: Specifies a mask for the IP address, in dotted-decimal format. The *ip-address* argument without a mask indicates a host address.

mac { **any** | *mac-address* [*mac-address-mask*] }: Specifies a MAC address range for matching sender MAC addresses of ARP packets.

- **any**: Matches any sender MAC address.
- **mac-address**: Matches the specified sender MAC address, in the format of H-H-H.
- **mac-address-mask**: Specifies a mask for the MAC address, in the format of H-H-H.

vlan *vlan-id*: Specifies the VLAN where the rule applies. The value range for the *vlan-id* argument is 1 to 4094.

Description

Use **arp detection** to set a rule for user validity check.

Use **undo arp detection** to restore the default.

By default, no rule is set for user validity check.

User validity check inspects each ARP packet received on an ARP untrusted interface against the configured rules. If a match is found, the ARP packet is processed according to the matching rule. If no match is found, the device checks the packet against static IP source guard binding entries, the DHCP snooping entries, 802.1X security entries, and OUI MAC addresses in turn.

Related command: **arp detection enable**.

Examples

Set a rule for user validity check and enable user validity check.

```
<Sysname> system-view
```

```
[Sysname] arp detection 0 permit ip 3.1.1.1 255.255.0.0 mac 0001-0203-0607 ffff-ffff-0000
```

```
[Sysname] vlan 1
```

```
[Sysname-Vlan1] arp detection enable
```

New feature: Enabling source IP conflict prompt

Enabling source IP conflict prompt

When the sender IP address in a gratuitous ARP packet is the same as the IP address of the receiving switch, the switch operates as follows:

- If the source IP conflict prompt is enabled, the receiving switch immediately displays a message telling that IP address conflict occurs.
- If the source IP conflict prompt is disabled, the receiving switch sends a gratuitous ARP packet. After the switch is informed of the conflict by an ARP reply, it displays a message telling that IP address conflict occurs.

To enable source IP conflict prompt:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable source IP conflict prompt.	arp ip-conflict prompt	Optional. By default, the function is disabled.

Command reference

arp ip-conflict prompt

Use **arp ip-conflict prompt** to enable source IP conflict prompt.

Use **undo arp ip-conflict prompt** to restore the default.

Syntax

arp ip-conflict prompt

undo arp ip-conflict prompt

Default

The source IP conflict prompt function is disabled.

Views

System view

Default command level

2: System level

Parameters

None

Examples

```
# Enable source IP conflict prompt.  
<Sysname> system-view  
[Sysname] arp ip-conflict prompt
```

New feature: Supporting IPv6 routes with a prefix length over 64

From this version on, the switch supports up to 128 IPv6 routes with a prefix length over 64.

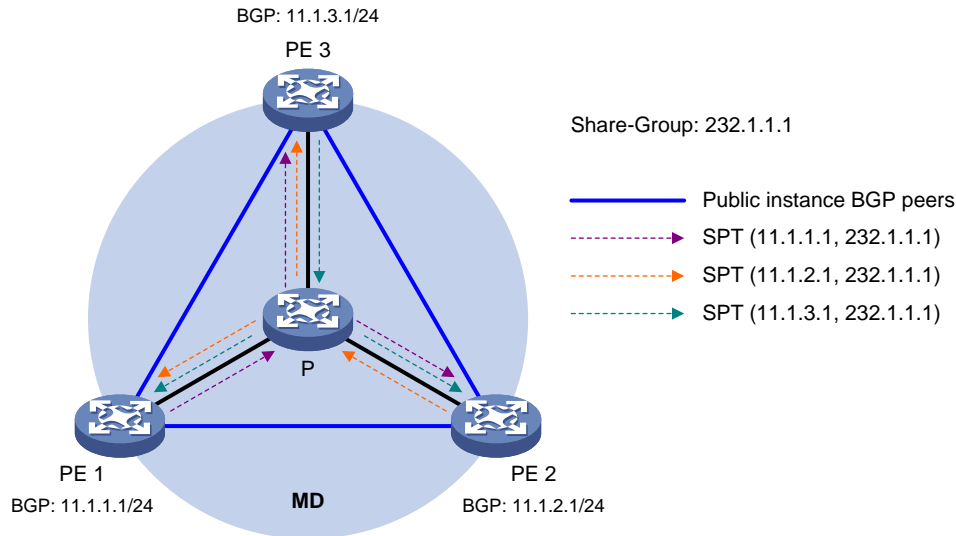
New feature: BGP MDT

Configuring BGP MDT

Multicast VPN is a technique that implements multicast delivery in virtual private networks (VPNs). After multicast VPN is configured, data can be transmitted in multicast in each of the VPN site and the public network.

If PIM-SSM is running in the public network, you must configure BGP MDT so as to create a share-MDT.

Figure 14 Share-MDT establishment in a PIM-SSM network



As shown in Figure 12, PIM-SSM is enabled in the network and all the PE devices support VPN instance A. The process of establishing a share-MDT is as follows:

The public network on PE 1 sends the local BGP MDT routing information, including its BGP interface address and the share-group address, to PE 2 and PE 3. PE 2 and PE 3 perform the same operation to exchange their BGP MDT routing information with one another. After receiving the BGP MDT information from PE1, PE 2 and PE 3 separately send a subscribe message for channel subscription hop by hop toward the BGP interface of PE1. A (11.1.1.1, 232.1.1.1) entry is created on devices on the path toward PE 1 in the public network. Thus an SPT is created in the network, with PE 1 as its root, PE 2 and PE 3 as its leaves.

At the same time, PE 2 and PE 3 separately initiate a similar SPT establishment process. Finally, three independent SPTs are established in the MD. In the PIM-SSM network, the three independent SPTs constitute a share-MDT. A share-MDT can be used for delivering multicast packets, including both multicast protocol packets and multicast data packets.

NOTE:

In PIM-SSM, subscribe messages are used equivalent to join messages.

For more information about multicast VPN and share-MDT, see *Multicast VPN Configuration Guide*.

Configuration prerequisites

Before you configure BGP MDT, complete the following tasks:

- Configure MPLS L3VPN on the public network.
- Configure basic BGP functions on the public network.
- Determine the route reflector cluster ID.

Configuring BGP MDT peers or peer groups

With BGP MDT peers or peer groups configured, a PE exchanges the BGP MDT routing information with other PEs to obtain their addresses and thus establish a share-MDT.

Perform the following configuration on the PE.

To configure BGP MDT peers or peer groups:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enter BGP MDT sub-address family view.	ipv4-family mdt	N/A
4. Enable a BGP MDT peer or peer group.	peer { <i>group-name</i> <i>ip-address</i> } enable	Disabled by default.
5. Add a peer to the BGP MDT peer group.	peer <i>ip-address</i> group <i>group-name</i>	Optional. By default, a BGP MDT peer belongs to no peer groups.

NOTE:

A BGP MDT peer or peer group is a peer or peer group created in BGP-MDT subaddress family view.

Configuring a BGP MDT route reflector

BGP MDT peers in the same AS must be fully meshed to maintain connectivity. However, when many BGP MDT peers exist in an AS, connection establishment among them might cause great expenses. To reduce connections between them, you can configure one of them as a route reflector and specify other routers as clients. The clients establish BGP MDT connections with the route reflector, and the route reflector forwards (reflects) BGP MDT routing information between clients. In this way, the clients need not to be fully meshed. Furthermore, you can disable client-to-client reflection to reduce overloads if the clients have been fully meshed.

The route reflector and its clients form a cluster. In general, a cluster has only one route reflector whose router ID identifies the cluster. However, you can configure several route reflectors in a cluster to improve network reliability, and they must have the same cluster ID configured to avoid routing loops.

Perform the following configuration on the PE.

To configure a BGP MDT route reflector:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enter BGP MDT sub-address family view.	ipv4-family mdt	N/A
4. Configure the local device as a route reflector and specify its clients.	peer { <i>group-name</i> <i>ip-address</i> } reflect-client	By default, neither route reflectors nor clients exist.
5. Disable route reflection between clients.	undo reflect between-clients	Optional. Enabled by default.
6. Configure the cluster ID of the route reflector.	reflector cluster-id { <i>cluster-id</i> <i>ip-address</i> }	Optional. By default, a route reflector uses its router ID as the cluster ID.

Displaying and maintaining BGP MDT

Step	Command	Remarks
1. Display information about a BGP MDT peer group.	display bgp mdt group [<i>group-name</i>] [[{ begin exclude include } <i>regular-expression</i>]	Available in any view
2. Display information about a BGP MDT peer.	display bgp mdt peer [[<i>ip-address</i>] verbose] [[{ begin exclude include } <i>regular-expression</i>]	Available in any view
3. Display BGP MDT routing information.	display bgp mdt { all route-distinguisher <i>route-distinguisher</i> } routing-table [<i>ip-address</i> [<i>mask</i> <i>mask-length</i>]] [[{ begin exclude include } <i>regular-expression</i>]	Available in any view
4. Reset a BGP MDT connection.	reset bgp mdt { <i>as-number</i> <i>ip-address</i> all external group <i>group-name</i> internal }	Available in user view

Command reference

display bgp mdt group

Syntax

display bgp mdt group [*group-name*] [[{ **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

group-name: Displays the information of the specified BGP MDT peer group. A group name is a case-sensitive string of 1 to 47 characters and must not contain any space.

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

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

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

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

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

Description

Use **display bgp mdt group** to display the information of a BGP MDT peer group.

Examples

Display the information of the BGP MDT peer group test.

```
<Sysname> display bgp mdt group test
```

```
BGP peer-group is test
Remote AS 2004
Type : external
Maximum allowed prefix number: 4294967295
Threshold: 75%
Configured hold timer value: 180
Keepalive timer value: 60
Minimum time between advertisement runs is 30 seconds
Connect-interface has been configured
Multi-hop ebgp been enabled
Peer Preferred Value: 0
No routing policy is configured
Members:
Peer                AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down  State
2.2.2.1             2004      0        0      0      0 00:01:21 Active
```

Table 16 Command output

Field	Description
BGP peer-group	BGP peer group name.
Remote AS	AS number of the peer group.
Type	Type of the peer group: <ul style="list-style-type: none"> external—EBGP peer group. internal—IBGP peer group.
Maximum allowed prefix number	Maximum number of allowed prefixes.
Threshold	Percentage of received prefixes from the peer group to maximum prefixes allowed to receive from the peer group.
Configured hold timer value	Holdtime interval.
Keepalive timer value	Keepalive interval.
Minimum time between advertisement runs	Minimum route advertisement interval.
Connect-interface has been configured	The source interface for TCP connection is configured.
Multi-hop ebgp been enabled	The hop count of the peer's TCP connection can exceed 1 but cannot exceed the configured limit.
Peer Preferred Value	Preferred value specified for the routes from the peer.
Members	Detailed information of the members in the peer group.
Peer	IP address of the peer.
AS	AS number of the peer.
MsgRcvd	Number of received messages.
MsgSent	Number of sent messages.
OutQ	Number of messages to be sent.
PrefRcv	Number of received prefixes.

Field	Description
Up/Down	Length of time since the session was established/time elapsed in the current state (before the session is established).
State	<p>State of the peer:</p> <ul style="list-style-type: none"> • Active—Waiting for reestablishing a TCP connection after a establishment failure. • Connect—A TCP connection is required but not established yet. • Established—A TCP connection is established. • Idle—No TCP connections are required after the peer relationship is configured. • Idle(Admin)—The peer is configured at the CLI not to require any TCP connection. • Openconfirm—Waiting for the keepalive message after receiving an open message. • Opensent—An open message is successfully sent to the peer.

display bgp mdt peer

Syntax

display bgp mdt peer [[*ip-address*] **verbose**] [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ip-address: Displays the information of the specified BGP MDT peer.

verbose: Displays detailed information.

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

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

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

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

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

Description

Use **display bgp mdt peer** to display BGP MDT peer information.

Examples

Display the detailed information of the BGP MDT peer 2.2.2.1.

```
<Sysname> display bgp mdt peer 2.2.2.1 verbose
```

```
Peer: 2.2.2.1    Local: 2.2.2.2
Type: IBGP link
BGP version 4, remote router ID 1.1.1.1
BGP current state: Established, Up for 00h01m51s
```



```

BGP current event: RecvKeepalive
BGP last state: OpenConfirm
Port: Local - 1029 Remote - 179
Configured: Active Hold Time: 180 sec Keepalive Time: 60 sec
Received : Active Hold Time: 180 sec
Negotiated: Active Hold Time: 180 sec Keepalive Time:60 sec
Peer optional capabilities:
Peer support bgp multi-protocol extended
Peer support bgp route refresh capability
Address family IPv4 Unicast: advertised and received
Address family IPv4 MDT: advertised and received

```

```

Received: Total 5 messages, Update messages 1
Sent: Total 4 messages, Update messages 0
Maximum allowed prefix number: 4294967295
Threshold: 75%
Minimum time between advertisement runs is 30 seconds
Optional capabilities:
Route refresh capability has been enabled
Connect-interface has been configured
Multi-hop ebgp been enabled
Peer Preferred Value: 0

```

```

Routing policy configured:
No routing policy is configured

```

Table 17 Command output

Field	Description
Peer	IP address of the peer.
Local	Local router ID.
Type	Peer types <ul style="list-style-type: none"> • IBGP link, indicating IBGP peers. • EBGP link, indicating EBGP peers.
remote router ID	Router ID of the peer.
BGP current state	Current state of the BGP peer: <ul style="list-style-type: none"> • Active—Waiting for reestablishing a TCP connection after a establishment failure. • Connect—A TCP connection is required but not established yet. • Established—A TCP connection is established between peers. • Idle—No TCP connections are required after the peer relationship is configured. • Idle(Admin)—The peer is configured at the CLI not to require any TCP connection. • Openconfirm—Waiting for the keepalive message after receiving an open message. • Opensent—An open message is successfully sent to the peer.

Field	Description
BGP current event	<p>Current event of the peer:</p> <ul style="list-style-type: none"> • AdvTimerExpired—The route advertisement timer expires. • ConnClosed—The TCP connection is closed. • ConnOpen—A TCP connection is required. • ConnOpenFailed—Fail to establish a TCP connection. • CRTTimerExpired—The connect timer expires. • HOLDTimerExpired—The holdtime timer expires. • KATTimerExpired—The keepalive timer expires. • RecvKeepalive—A keepalive message is received from the peer. • RecvNotification—A notification message is received from the peer. • RecvOpen—An open message is received from the peer. • RecvRouteRefresh—A route-refresh message is received from the peer. • RecvUpdate—An update message is received from the peer. • Start—No TCP connections are required after the peer relationship is configured. • Stop—The peer is configured not to require any TCP connection at the CLI. • TransFatalError—A fatal mistake occurs during the establishment of the TCP connection.
BGP last state	<p>Previous state of the peer:</p> <ul style="list-style-type: none"> • Active—Waiting for reestablishing a TCP connection after an establishment failure. • Connect—A TCP connection is required but not established yet. • Established—A TCP connection is established between peers. • Idle—No TCP connections are required after the peer relationship is configured. • Idle(Admin)—The peer is configured at the CLI not to require any TCP connection. • Openconfirm—Waiting for the keepalive message after receiving an open message. • Opensent—An open message is successfully sent to the peer.
Port	Local and remote TCP port numbers for establishing a TCP connection.
Configured	<p>Locally configured timer value:</p> <ul style="list-style-type: none"> • Active Hold Time—The holdtime interval for the connection to the peer. • Keepalive Time—The keepalive interval for the connection to the peer.
Received	<p>Received timer settings on the peer:</p> <p>Active Hold Time—The holdtime interval for the connection to the peer.</p>
Negotiated	<p>Negotiated timer settings:</p> <ul style="list-style-type: none"> • Active Hold Time—The holdtime interval for the connection to the peer. • Keepalive Time—The keepalive interval for the connection to the peer.
Peer optional capabilities	Optional capabilities supported by the peer.
Peer support bgp multi-protocol extended	The peer supports multiprotocol BGP extensions.
Peer support bgp route refresh capability	The peer supports the BGP route refresh function.
Address family IPv4 Unicast: advertised and received	Routes are advertised and received in IPv4 unicasts.

Field	Description
Address family IPv4 MDT: advertised and received	Routes are advertised and received in IPv4 multicasts.
Received	Total numbers of received packets and updates.
Sent	Total numbers of sent packets and updates.
Maximum allowed prefix number	Maximum number of allowed prefixes.
Threshold	Percentage of received prefixes from the peer group to maximum prefixes allowed to receive from the peer group.
Minimum time between advertisement runs	Minimum route advertisement interval.
Optional capabilities	Optional capabilities enabled by the peer.
Connect-interface has been configured	The source interface for TCP connection is configured.
Multi-hop ebgp been enabled	The hop count of the peer's TCP connection can exceed 1 but cannot exceed the configured limit.
Peer Preferred Value	Preferred value specified for the routes from the peer.
Routing policy configured	Local routing policy.

display bgp mdt routing-table

Syntax

```
display bgp mdt { all | route-distinguisher route-distinguisher } routing-table [ ip-address [ mask | mask-length ] ] [ { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

all: Displays the information of all the BGP MDT routes.

route-distinguisher *route-distinguisher*: Displays the BGP MDT routing information of the specified route distinguisher. *route-distinguisher* identifies the route distinguisher name, a string of 3 to 21 characters in the form of nn:nn or IP-address:nn.

ip-address: Specifies a destination IP address.

mask: Specifies the network mask, 225.225.225.225 by default.

mask-length: Specifies the mask length, in the range of 0 to 32. The default is 32.

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

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

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

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

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

Description

Use **display bgp mdt routing-table** to display BGP MDT routing information.

Examples

Display BGP MDT routing information.

```
<Sysname> display bgp mdt all routing-table
```

```
BGP Local router ID is 2.2.2.2
```

```
Status codes: * - valid, ^ - VPNv4 best, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

```
Origin : i - IGP, e - EGP, ? - incomplete
```

```
Total number of MDT routes: 1
```

```
Route Distinguisher: 100:1
```

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*> 1.1.1.1/32	3.3.3.3	0	100	10	?

Table 18 Command output

Field	Description
Origin	<ul style="list-style-type: none">i – IGP (originated in the AS).e – EGP (learned through EGP).? – incomplete (learned by some other means).
Total number of MDT routes	Total number of MDT routes.
Network	MD source address displayed in the BGP routing table.
NextHop	Next hop.
MED	Metric associated with the destination network.
LocPrf	Local preference value.
PrefVal	Preferred value of the route.
Path	AS_PATH attribute, recording the ASs the packet has passed to avoid routing loops.
Ogn	Origin attribute of the route, which can be one of the following values: <ul style="list-style-type: none">i—Indicates that the route is interior to the AS. Aggregate routes and the routes injected with the network command are considered IGP routes.e—Indicates that the route is learned from the Exterior Gateway Protocol (EGP).?—Indicates that the origin of the route is unknown, such as the MDT routes redistributed from other routing protocols.

ipv4-family mdt

Syntax

```
ipv4-family mdt
undo ipv4-family mdt
```

View

BGP view

Default level

2: System level

Parameters

None

Description

Use **ipv4-family mdt** to enter BGP-MDT sub-address family view.

Use **undo ipv4-family mdt** to remove all the settings made in BGP-MDT sub-address family view.

Examples

Enter BGP-MDT sub-address family view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family mdt
[Sysname-bgp-af-mdt]
```

peer enable (BGP-MDT sub-address family view)

Syntax

```
peer { group-name | ip-address } enable
undo peer { group-name | ip-address } enable
```

View

BGP-MDT sub-address family view

Default level

2: System level

Parameters

group-name: Specifies a BGP MDT peer group by its name, a case-sensitive string of 1 to 47 characters. A peer group name must not contain any space.

ip-address: Specifies a BGP MDT peer by its IP address.

Description

Use **peer enable** to enable the specified peer or peer group.

Use **undo peer enable** to disable the specified peer or peer group.

By default, no BGP MDT peer or peer group is enabled.

The BGP peer or peer group must be configured before this command can take effect.

Related commands: **group**, **peer as-number**, and **peer group** (*Layer 3—IP Routing Command Reference*).

Examples

Configure and enable the BGP MDT peer 18.10.0.9.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 18.10.0.9 as-number 100
[Sysname-bgp] ipv4-family mdt
[Sysname-bgp-af-mdt] peer 18.10.0.9 enable
```

peer group (BGP-MDT sub-address family view)

Syntax

peer *ip-address* **group** *group-name*
undo peer *ip-address* **group** *group-name*

View

BGP-MDT sub-address family view

Default level

2: System level

Parameters

ip-address: Specifies a BGP MDT peer by its IP address.

group-name: Specifies a BGP MDT peer group by its name, a case-sensitive string of 1 to 47 characters. A peer group name must not contain any space.

Description

Use **peer group** to add a peer to the BGP MDT peer group.

Use **undo peer group** to delete a specified peer from the peer group.

By default, a peer belongs to no peer groups.

The BGP MDT peer and peer group must be configured and enabled before this command can take effect.

Related commands: **peer enable**.

Examples

Configure and enable the BGP MDT peer 10.1.1.1 and the peer group test, and then add the peer to the peer group.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test
[Sysname-bgp] peer test as-number 2004
[Sysname-bgp] peer 10.1.1.1 group test
[Sysname-bgp] ipv4-family mdt
[Sysname-bgp-af-mdt] peer test enable
[Sysname-bgp-af-mdt] peer 10.1.1.1 enable
[Sysname-bgp-af-mdt] peer 10.1.1.1 group test
```

peer reflect-client (BGP-MDT sub-address family view)

Syntax

peer { *group-name* | *ip-address* } **reflect-client**

undo peer { *group-name* | *ip-address* } **reflect-client**

View

BGP-MDT sub-address family view

Default level

2: System level

Parameters

group-name: Specifies a BGP MDT peer group by its name, a case-sensitive string of 1 to 47 characters. A peer name must not contain any space.

ip-address: Specifies a BGP MDT peer by its IP address.

Description

Use **peer reflect-client** to configure the router as a route reflector and specify a peer or peer group as its client.

Use **undo peer reflect-client** to remove the configuration.

By default, neither route reflectors nor clients are configured.

Before you configure this command, BGP MDT peers or peer groups should be configured.

Your configuration will overwrite the old configuration (if any).

Related commands: **peer enable**, **reflect between-clients**, and **reflect cluster-id**.

Examples

Configure and activate BGP MDT peer group **test**, and then configure the local device as a route reflector and specify the BGP MDT peer group test as a client.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test
[Sysname-bgp] ipv4-family mdt
[Sysname-bgp-af-mdt] peer test enable
[Sysname-bgp-af-mdt] peer test reflect-client
```

reflect between-clients (BGP-MDT sub-address family view)

Syntax

reflect between-clients

undo reflect between-clients

View

BGP-MDT sub-address family view

Default level

2: System level

Parameters

None

Description

Use **reflect between-clients** to enable route reflection between clients.

Use **undo reflect between-clients** to disable this function.

By default, route reflection between clients is enabled.

Related commands: **peer reflect-client** and **reflector cluster-id**.

Examples

```
# Disable route reflection between clients.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family mdt
[Sysname-bgp-af-mdt] undo reflect between-clients
```

reflector cluster-id (BGP-MDT sub-address family view)

Syntax

```
reflector cluster-id { cluster-id | ip-address }
undo reflector cluster-id
```

View

BGP-MDT sub-address family view

Default level

2: System level

Parameters

cluster-id: Specifies a route reflector by its cluster ID, in the range of 1 to 4294967295.

ip-address: Specifies a route reflector by its IP address, which is the IP address of the specified BGP MDT peer.

Description

Use **reflector cluster-id** to configure the cluster ID of the route reflector.

Use **undo reflector cluster-id** to remove the configured cluster ID.

By default, a route reflector uses its router ID as the cluster ID.

In general, a cluster has only one route reflector whose router ID identifies the cluster. However, you can configure several route reflectors in a cluster to improve network reliability, and they must have the same cluster ID configured to avoid routing loops.

Related commands: **reflect between-clients** and **peer reflect-client**.

Examples

```
# Specify 80 as the cluster ID for the route reflector.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family mdt
[Sysname-bgp-af-mdt] reflector cluster-id 80
```

reset bgp mdt

Syntax

```
reset bgp mdt { as-number | ip-address | all | external | group group-name | internal }
```

View

User view

Default level

2: System level

Parameters

as-number: Resets BGP MDT connections to peers in the specified AS, in the range of 1 to 4294967295.

ip-address: Resets the connection with the specified BGP MDT peer.

all: Resets all the BGP MDT connections.

external: Resets all the EBGP MDT connections.

group group-name: Resets connections with the specified BGP peer group. A peer group name is a case-sensitive string of 1 to 47 characters and must not contain any space.

internal: Resets all the IBGP MDT connections.

Description

Use **reset bgp mdt** to reset BGP MDT connections.

Examples

Reset all the BGP MDT connections.

```
<Sysname> reset bgp mdt all
```

New feature: Configuring the maximum number of selected ports allowed for an aggregation group

Configuring the maximum number of selected ports allowed for an aggregation group

By default, the maximum number of Selected ports allowed in an aggregation group depends on the hardware capabilities of the member ports. After you manually configure the maximum number of Selected ports in an aggregation group, the maximum number of Selected ports allowed in the aggregation group is the lower value of the two upper limits.

You can configure redundancy between two ports using the following guideline: Assign two ports to an aggregation group, and configure the maximum number of Selected ports allowed in the aggregation group as 1. In this way, only one Selected port is allowed in the aggregation group at any point in time, while the Unselected port serves as a backup port.

Configuration guidelines

Follow these guidelines when you configure the port threshold settings:

- Make sure the two link aggregation ends have the same maximum numbers of selected ports.

Make sure you understand the following impacts of the port threshold settings:

- Configuring the maximum number of Selected ports in an aggregation group may cause some of the selected member ports in the aggregation group to become unselected.

Configuration procedure

To configure the maximum number of Selected ports allowed for an aggregation group:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter aggregate interface view.	<ul style="list-style-type: none"> Enter Layer 2 aggregate interface view: interface bridge-aggregation <i>interface-number</i> Enter Layer 3 aggregate interface view: interface route-aggregation <i>interface-number</i> 	Use either command.
3. Configure the maximum number of Selected ports allowed for the aggregation group.	link-aggregation selected-port maximum <i>number</i>	By default, the maximum number of Selected ports allowed in an aggregation group depends on only the hardware capabilities of the member ports.

Command reference

link-aggregation selected-port maximum

Syntax

link-aggregation selected-port maximum *number*

undo link-aggregation selected-port maximum

View

Layer 2 aggregate interface view, Layer 3 aggregate interface view

Default level

2: System level

Parameters

number: Specifies the maximum number of Selected ports allowed in an aggregation group. This argument ranges from 1 to 8.

Description

Use **link-aggregation selected-port maximum** to configure the maximum number of Selected ports allowed in the aggregation group.

Use **undo link-aggregation selected-port maximum** to restore the default setting.

By default, the maximum number of Selected ports allowed in an aggregation group is limited only by the hardware capabilities of the member ports.

Executing this command may cause some of the member ports in the aggregation group to become unselected.

The maximum numbers of Selected ports for the local and peer aggregation groups must be consistent.

Examples

Configure the maximum number of Selected ports as 3 in the aggregation group corresponding to Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Sysname> system-view
```

```
[Sysname] interface bridge-aggregation 1
```

```
[Sysname-Bridge-Aggregation1] link-aggregation selected-port maximum 3
```

New feature: Enabling MAC address migration log notifying

Enabling MAC address migration log notifying

This feature records and notifies MAC address migration information, including MAC addresses that migrate, IDs of VLANs to which MAC addresses belong, source interfaces from which MAC addresses migrate, and current interfaces with which MAC addresses associate, last migration time, and migration times in the last one minute.

MAC address migration refers to this process: a device learns a MAC address from an interface, Port A for example, and the device later learns the MAC address from another interface, Port B for example. If Port A and Port B belong to the same VLAN, the outgoing interface in the entry for the MAC address is changed to Port B from Port A, which means that the MAC address migrates from Port A to Port B.

When the switch is used as an access device at a data center, a migration of a virtual machine between servers might cause a MAC address migration on the switch. For example, when a virtual machine migrates from the server connected to interface A to the server connected to interface B, a log is generated to record and report the migration.



TIP:

If a MAC address migrates between two specific interfaces frequently, a Layer 2 loop probably occurs in the network. To discover and locate Layer 2 loops, you can enable MAC address migration log notifying.

To enable MAC address migration log notifying:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable MAC address migration log notifying.	mac-flapping notification enable	By default, MAC address migration log notifying is disabled.

Command reference

mac-flapping notification enable

Syntax

mac-flapping notification enable
undo mac-flapping notification enable

View

System view

Default level

2: System level

Parameters

None.

Description

Use **mac-flapping notification enable** to enable MAC address migration log notifying.

Use **undo mac-flapping notification enable** to disable the MAC address migration notifying.

A MAC address migration log contains a MAC address, ID of the VLAN to which the MAC address belongs, source interface from which the MAC address migrates, and the current interface with which the MAC address associates.

By default, MAC address migration log notifying is disabled.

After enabling MAC address migration log notifying, the MAC address migration log of the last 1 minute are displayed once every 1 minute.

Up to 10 logs can be saved on the switch in 1 minute.

Examples

Enable MAC address migration log notifying.

```
<Sysname> system-view
```

```
[Sysname] mac-flapping notification enable
```

```
[Sysname]
```

```
%Sep 21 14:09:22:420 2012 HP MAC/5/MAC_FLAPPING: MAC address 0000-0012-0034 in vlan 500  
has flapped from port GigabitEthernet1/0/16 to port GigabitEthernet1/0/1 1 time(s).
```

The output shows that the MAC address 0000-0012-0034 belongs to VLAN 500, the source interface from which the MAC address migrates from is GE 1/0/16, the current interface with which the MAC address associates is GE 1/0/1, and the MAC address migrates one time in the last one minute.

New feature: Disabling MAC entry aging timer refresh based on destination MAC address

Disabling MAC entry aging timer refresh based on destination MAC address

To accommodate network changes, the MAC address table keeps updating. Each dynamic MAC address entry has an aging timer. When the device receives a packet with the source or destination MAC address matching a dynamic MAC address entry, it restarts the aging timer for the entry.

If you want the device to restart the aging timer of dynamic entries for only matching source MAC addresses, disable MAC entry aging timer refresh based on destination MAC address.

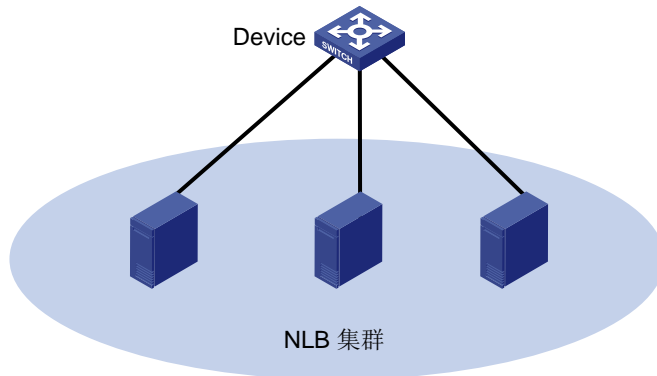
To disable MAC entry aging timer refresh based on destination MAC address:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Disable MAC entry aging timer refresh based on destination MAC address.	mac-address destination-hit disable	By default, MAC entry aging timer refresh based on destination MAC address is enabled.

Application example

Microsoft Network Load Balancing (NLB) is a load balancing technology for server clustering developed on Windows Server.

Figure 15 NLB cluster



NLB supports load sharing and redundancy among servers within a cluster. To implement fast failover, NLB requires that the switch forwards network traffic to all servers or specified servers in the cluster, and each server filters out unexpected traffic.

In NLB unicast mode, when a server joins the cluster or a failover occurs, a packet with a virtual source MAC address is sent. The switch then adds the virtual MAC address to its MAC address table, and packets destined for the server use the virtual MAC address (although not used by the server) as their destination address. If the virtual MAC address never ages out, the switch forwards packets only through the port associated with the virtual MAC address rather than all ports connected to the servers within the cluster.

To address this issue, disable MAC entry aging timer refresh based on destination MAC address to age out the virtual MAC address, so that the switch can forward packets to all servers within the cluster.

Command reference

mac-address destination-hit disable

Use **mac-address destination-hit disable** to disable MAC entry aging timer refresh based on destination MAC address.

Use **undo mac-address destination-hit disable** to restore the default.

Syntax

mac-address destination-hit disable

undo mac-address destination-hit disable

Default

MAC entry aging timer refresh based on destination MAC address is enabled.

View

System view

Default command level:

2: System level

Examples

Disable MAC entry aging timer refresh based on destination MAC address.

```
<Sysname> system-view
```

```
[Sysname] mac-address destination-hit disable
```

New feature: PoE power negotiation through Power Via MDI TLV (supported only on PoE-capable switches)

Configuring PoE power negotiation through Power Via MDI TLV

- With this feature enabled, a PSE device can automatically negotiate PoE power with connected PDs. To enable this feature, you only need to enable LLDP, and enable PoE on the PSE device and on the specific PoE interface.
- If you configure the **poe max-power** *max-power* command to specify the maximum power allocated to a PoE interface of the PSE device, the configured value applies and PoE power autonegotiation is disabled.

Command reference

You can use the `display lldp local-information` and `display lldp neighbor-information` commands to view PoE power negotiation information.

Modified command: display lldp local-information

Syntax

```
display lldp local-information [ global | interface interface-type interface-number ] [ | { begin | exclude | include } regular-expression ]
```

Views

Any view

Change description

PoE power negotiation information was added to the output.

Display all LLDP information to be sent. (This example displays only the information added for this feature.)

```
<Sysname> display lldp local-information
...
LLDP local-information of port 1[GigabitEthernet1/0/1]:
...
Power type           : Type 2 PSE
Power source         : Primary
Power priority       : High
PD requested power value : 25.5(w)
PSE allocated power value : 25.5(w)
...
```

Table 19 Command output

Field	Description
Power type	Power type when the device supports PoE. Type 2 PSE supplies power from 0 to 30 W, a voltage from 50 to 57 V, and a maximum current of 600 mA.

Field	Description
Power source	Power supply type of a PSE when the device supports PoE: <ul style="list-style-type: none"> • Unknown—Unknown power supply. • Primary—Primary power supply. • Backup—Backup power supply.
Power priority	Power supply priority on a PSE when the device supports PoE: <ul style="list-style-type: none"> • Unknown—Unknown priority. • Critical—Priority 1. • High—Priority 2. • Low—Priority 3.
PD requested power value	Power (in watts) required by the PD that connects to the port. This field appears only on the devices that support PoE.
PSE allocated power value	Power (in watts) supplied by the PSE to the connecting port. This field appears only on the devices that support PoE.

Modified command: display lldp neighbor-information

Syntax

display lldp neighbor-information [**brief** | **interface** *interface-type interface-number* [**brief**] | **list** [**system-name** *system-name*]] [{ **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Change description

PoE power negotiation information was added in the output.

Display the LLDP information sent from the neighboring devices received through all ports. (This example displays only the information added for this feature.)

```
<Sysname> display lldp neighbor-information
...
LLDP neighbor-information of port 1[GigabitEthernet1/0/1]:
...
Power type           : Type 2 PD
Power source         : PSE and local
Power priority       : High
PD requested power value : 25.5(w)
PSE allocated power value : 25.5(w)
...
```

Table 20 Command output

Field	Description
Power type	This field appears only on the devices that support PoE. PD type of an LLDP neighboring device which is a PD device: <ul style="list-style-type: none"> • Type 1 PD—This type power from 0 to 15.4 W, a voltage from 44 to 57 V, and a maximum current of 350 mA. • Type 2 PD—This type requires power from 0 to 30 W, a voltage from 50 to 57 V, and a maximum current of 600 mA.

Field	Description
Power source	<p>This field appears only on the devices that support PoE.</p> <p>Power source type of an LLDP neighboring device which is a PD device:</p> <ul style="list-style-type: none"> • Unknown—Unknown power supply. • PSE—PSE power supply. • Local—Local power supply. • PSE and local—PSE and local power supply.
Power priority	<p>This field appears only on the devices that support PoE.</p> <p>Powered priority of ports on an LLDP neighboring device which is a PD device:</p> <ul style="list-style-type: none"> • Unknown—Unknown priority. • Critical—Priority 1. • High—Priority 2. • Low—Priority 3.
PD requested power value	<p>This field appears only on the devices that support PoE.</p> <p>Power (in watts) requested by the LLDP neighboring device which is a PD device.</p>
PSE allocated power value	<p>This field appears only on the devices that support PoE.</p> <p>Power (in watts) supplied by the PSE to the LLDP neighboring device which is a PD device.</p>

New feature: Specifying a destination server in a VPN for UDP helper

Specifying a destination server in a VPN for UDP helper

You can specify the VPN to which the destination server belongs for UDP helper.

Command reference

Modified command: udp-helper server

Syntax

udp-helper server [**vpn-instance** *vpn-instance-name*] *ip-address*

Views

Interface view

Change description

Before modification: Option **vpn-instance** *vpn-instance-name* was not supported.

After modification: Option **vpn-instance** *vpn-instance-name* is supported.

New feature: Supporting using a self-signed certificate for HTTPS

The switch supports simplified HTTPS login. To make the switch operate in this mode, you only need to enable HTTPS service on the switch. The switch will use a self-signed certificate (a certificate that is generated and signed by the switch itself, rather than a CA). If you specify an SSL server policy for the HTTPS service before enabling HTTPS service but do not specify the PKI domain for the SSH server, the switch still uses self-signed certificate. After you specify a PKI domain for the SSH server, the switch uses the PKI domain to obtain a certificate for the SSH server from the CA and uses the obtained certificate.

New feature: Setting the maximum number of 802.1X authentication attempts for MAC authentication users

Setting the maximum number of 802.1X authentication attempts for MAC authentication users

When both MAC authentication and 802.1X authentication are enabled on a port, if a MAC-authenticated user sends an EAP packet to the device for 802.1X authentication, the device performs 802.1X authentication for the user by default. If the user passes 802.1X authentication, the user goes online as an 802.1X user. If the user fails 802.1X authentication, the user might try the authentication multiple times, depending on the configuration on the client. If you do not want such users to try 802.1X authentication for too many times, you can perform the following task on the device to limit the number of authentication failures.

To set the maximum number of 802.1X authentication attempts for MAC authentication users:

Step	Command
1. Enter system view.	system-view
2. Enter Layer 2 Ethernet interface view.	interface <i>interface-type interface-number</i>
3. Set the maximum number of 802.1X authentication attempts for MAC authentication users.	dot1x attempts max-fail <i>unsuccessful-attempts</i>

Command reference

dot1x attempts max-fail

Use **dot1x attempts max-fail** to set the maximum number of 802.1X authentication attempts that a MAC-authenticated user can try.

Use **undo dot1x attempts max-fail** to restore the default.

Syntax

dot1x attempts max-fail *unsuccessful-attempts*

undo dot1x attempts max-fail

Default

The device allows a user that have passed MAC authentication to perform 802.1X authentication, and the maximum number of 802.1X authentication attempts that the user can try is determined by the configuration on the authentication client.

Views

Layer 2 Ethernet interface view

Default command level:

2: System level

Parameters

unsuccessful-attempts: Sets the maximum number of 802.1X authentication attempts that a MAC-authenticated user can try. The value range for this argument is 1 to 50.

Examples

On port GigabitEthernet 1/0/1, set the maximum number of 802.1X authentication attempts that a MAC-authenticated user can try to 3.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x attempts max-fail 3
```

New feature: Support of 802.1X for issuing VLAN groups

Support of 802.1X for issuing VLAN groups

After an 802.1X user passes the authentication on the server, the server delivers the authorization information to the device. If the server has specified the VLAN which is to be assigned to the user, the server contains the VLAN information in the authorization information to be delivered to device. Then, the device assigns the port through which the user performs authentication and logs in to the server-assigned VLAN.

The authentication server running the earlier releases issues a VLAN ID or VLAN name, and supports issuing only the specified VLAN. In this release or later, you can configure a VLAN group on the device, and the authentication server issues a VLAN group name. After the authentication server issues a VLAN group name, the access device selects a VLAN ID in the VLAN group and assigns the VLAN ID to a user.

The access device selects a VLAN ID from the VLAN group following these rules:

1. Select a VLAN with the least users.
2. Select the first queried VLAN if multiple VLANs have the same number of users.

For example, a VLAN group contains VLAN 2 and VLAN 3, VLAN 3 has been assigned to three users who have passed the authentication, and VLAN 2 has been assigned to two users who have passed the authentication. When a user passes the authentication, VLAN 2 is assigned to the user.

By issuing a VLAN group, you can balance the number of users in each VLAN, reduce the broadcasts in each VLAN, and improve the efficiency.

Configuring a VLAN group

You can create a VLAN group and add multiple VLAN IDs to a VLAN group.

To configure a VLAN group:

Step	Command
1. Enter system view.	system-view
2. Create a VLAN group and enter VLAN group view.	vlan-group <i>group-name</i>
3. Assign the specified VLANs to the VLAN group.	vlan-list <i>vlan-list</i>

NOTE:

If a super VLAN is added to a VLAN group, the device ignores the super VLAN when selecting a server-assigned VLAN for a user passing the authentication.

Command reference

vlan-group

Use **vlan-group** to create a VLAN group and enter VLAN group view.

Use **undo vlan-group** to delete the specified VLAN group.

Syntax

vlan-group *group-name*

undo vlan-group *group-name*

Default

No VLAN group exists.

Views

System view

Default command level

3: Manage level

Parameters

group-name: VLAN group name, which is a case-sensitive string of 1 to 31 characters and must start with a letter.

Examples

Create a VLAN group named **test**, and enter VLAN group view.

```
<Sysname> system-view
```

```
[Sysname] vlan-group test
```

vlan-list

Use **vlan-list** to configure member VLANs for the VLAN group.

Use **undo vlan-list** to delete member VLANs from the VLAN group.

Syntax

vlan-list *vlan-list*

undo vlan-list *vlan-list*

Views

VLAN group view

Default command level

2: System level

Parameters

vlan-list: Specifies a VLAN list in the form of *vlan-list* = { *vlan-id1* [*to* *vlan-id2*] } <1-10>. The value range for both the *vlan-id1* and *vlan-id2* arguments is 1 to 4094 and *vlan-id1* cannot be greater than *vlan-id2*. <1-10> indicates that you can specify up to ten VLAN lists.

Usage guidelines

You can add VLANs that have not been created to a VLAN group.

You can add a VLAN to multiple VLAN groups.

Repeat this command to configure multiple member VLANs for a VLAN group.

If a super VLAN is added to a VLAN group, the device ignores the super VLAN when selecting a server-assigned VLAN for a user passing the authentication.

Examples

Add VLANs 6, 7, and 8 to the VLAN group named **test**.

```
<Sysname> system-view
[Sysname] vlan-group test
[Sysname-vlan-group-test] vlan-list 6 7 8
```

New feature: Setting the deletion delay time for SAVI

Setting the deletion delay time for SAVI

The SAVI feature enables the access switch to check the validity of the source addresses of DHCPv6 protocol packets, ND protocol packets, and IPv6 data packets against the ND snooping entries, DHCPv6 snooping entries, and IP source guard bindings.

After a port is down, the switch can wait for a period of delay time before deleting the DHCPv6 snooping entries and ND snooping entries for that port. The deletion delay time is configurable. This delay ensures a valid IPv6 user to access the port for the event that a port goes down and resumes during that period.

Table 1 Setting the deletion delay time for SAVI

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable SAVI.	ipv6 savi strict	By default, SAVI is disabled.
3. Setting the deletion delay time for SAVI.	ipv6 savi down-delay time	The default setting is 30 seconds.

Command reference

ipv6 savi down-delay

Use **ipv6 savi down-delay** to set the deletion delay time for SAVI.

Use **undo ipv6 savi down-delay** to restore the default.

Syntax

```
ipv6 savi down-delay time  
undo ipv6 savi down-delay
```

Default

The deletion delay time is 30 seconds.

Views

System view

Default command level

2: System level

Parameters

time: Specifies the delay time in the range of 0 to 86400 seconds.

Usage guidelines

If a port is down for a period of time that exceeds the deletion delay time, the switch deletes the DHCPv6 snooping entries and ND snooping entries for that port.

Examples

Set the deletion delay time for SAVI to 360 seconds.

```
<Sysname> system-view
```

```
[Sysname] ipv6 savi down-delay 360
```

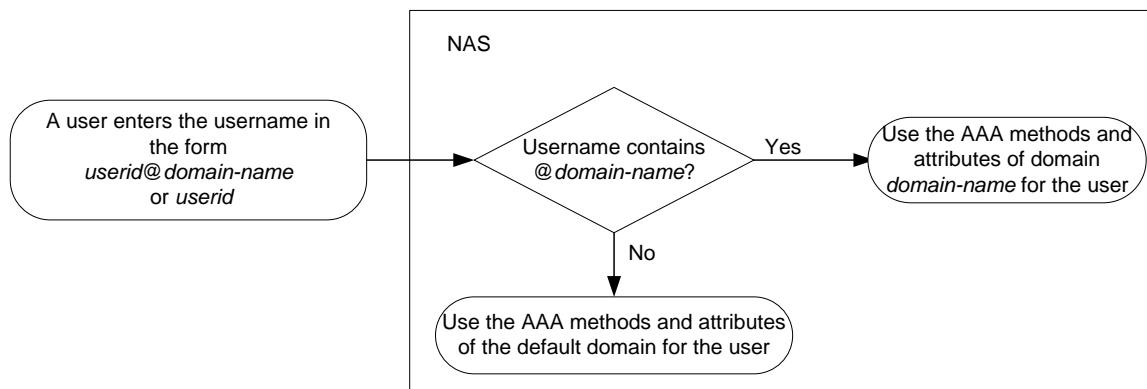
New feature: Setting a DSCP value for an ISP domain

Setting a DSCP value for an ISP domain

AAA typically uses a client/server model. The client runs on the network access server (NAS), which is also referred to as the access device. The server maintains user information centrally. In an AAA network, the NAS is a server for users, but a client for AAA servers.

A NAS manages users based on ISP domains. On a NAS, each user belongs to one ISP domain. A NAS determines the ISP domain for a user by the username entered by the user at login, as shown in [Figure 1](#).

Figure 1 Determining the ISP domain of a user by the username



Perform this task to set a DSCP value for an ISP domain.

The device sets the specified DSCP value in IP packets from authenticated users in the ISP domain, which is identified in the login username *userid@domain-name*. Policy-based routing routes IP packets to different destinations based on the DSCP value. This feature is only applicable to ISP domains that use the same scheme for Layer 3 portal authentication.

For more information about policy-based routing, see *Layer 3—IP Routing Configuration Guide*. For more information about Layer 3 portal authentication, see "Configuring portal."

Purpose	Command	Remarks
Enter system view.	system-view	N/A
Enter ISP domain view.	domain <i>isp-name</i>	N/A
Set a DSCP value for the ISP domain.	dscp <i>dscp-value</i>	Optional. By default, no DSCP is specified for an ISP domain.

Command reference

dscp (ISP domain view)

Syntax

dscp *dscp-value*

undo dscp

View

ISP domain view

Parameters

dscp-value: DSCP value of an ISP domain, which ranges from 0 to 63.

Description

Use the **dhcpc dscp** command to set the DSCP value for the ISP domain. After a user that uses the ISP domain passes the authentication, the switch assigns the DSCP value to IP packets from the user.

Use the **undo dhcpc dscp** command to restore the default.

By default, no DSCP value is set for an ISP domain, and the DSCP value of IP packets from a user passing the authentication does not change.

Examples

Set the DSCP value to 6 for ISP domain **test**.

```
<Sysname> system-view
```

```
[Sysname] domain aaa
```

```
[Sysname-isp-aaa] dscp 6
```

New feature: Advanced packet filtering logging

The advanced packet filtering logging feature provides packet filtering information including the number of matching packets and packet information.

The following is an example of an advanced packet filtering log. It shows that Telnet access to 10.253.10.299 from 10.253.23.181 was denied, and one matching packet.

```
*Feb 6 16:10:24: %SEC-6-IPACCESSLOGP: list 120 denied tcp 10.253.23.181(1281) ->
10.253.10.229(23), 1 packet
```

Configuring advanced packet filtering logging

You can configure both the advanced and basic packet filtering logging features on the device. Basic packet filtering logging provides only the number of matching packets.

To configure advanced packet filtering logging:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable advanced IPv4 packet filtering logging and set the interval for generating and outputting logs.	acl flow logging interval <i>interval-value</i>	By default, the interval is 0 minutes, and the device does not log IPv4 packet filtering events.
3. Enable advanced IPv6 packet filtering logging and set the interval for generating and outputting logs.	acl ipv6 flow logging interval <i>interval-value</i>	By default, the interval is 0 minutes, and the device does not log IPv6 packet filtering events.

Command reference

acl flow logging interval

Use **acl flow logging interval** to enable advanced IPv4 packet filtering logging and set the interval for generating and outputting logs.

Use **undo acl flow logging interval** to restore the default.

Syntax

acl flow logging interval *interval-value*

undo acl flow logging interval

Views

System view

Default

The device does not perform advanced IPv4 packet filtering logging, and the interval is 0 minutes.

Default command level

2: System level

Parameters

interval-value: Specifies the interval in minutes at which advanced IPv4 packet filtering logs are generated and output. The value is in the range of 0 to 1440, and must be a multiple of five. To disable the packet filtering logging, set the value to 0.

Usage guidelines

This advanced IPv4 packet filtering logging feature applies to only IPv4 basic and advanced ACLs.

To use this feature for an IPv4 basic or advanced ACL, specify the **logging** keyword in the ACL rules and configure the **acl flow logging interval** command. Then the device periodically generates and outputs packet filtering logs to the information center.

Examples

Enable advanced IPv4 packet filtering logging and set the interval to 10 minutes for generating and outputting logs.

```
<Sysname> system-view
```

```
[Sysname] acl flow logging interval 10
```

acl ipv6 flow logging interval

Use **acl ipv6 flow logging interval** to enable advanced IPv6 packet filtering logging and set the interval for generating and outputting logs.

Use **undo acl ipv6 flow logging interval** to restore the default.

Syntax

acl ipv6 flow logging interval *interval-value*

undo acl ipv6 flow logging interval

Views

System view

Default

The device does not perform advanced IPv6 packet filtering logging, and the interval is 0 minutes.

Default command level

2: System level

Parameters

interval-value: Specifies the interval in minutes at which advanced IPv6 packet filtering logs are generated and output. The value is in the range of 0 to 1440, and must be a multiple of five. To disable the packet filtering logging, set the value to 0.

Usage guidelines

This advanced IPv6 packet filtering logging feature applies to only IPv6 basic and advanced ACLs.

To use this feature for an IPv6 basic or advanced ACL, specify the **logging** keyword in the ACL rules and configure the **acl ipv6 flow logging interval** command. Then the device periodically generates and outputs packet filtering logs to the information center.

Examples

Enable advanced IPv6 packet filtering logging and set the interval to 10 minutes for generating and outputting logs.

```
<Sysname> system-view
```

```
[Sysname] acl ipv6 flow logging interval 10
```

New feature: PoE

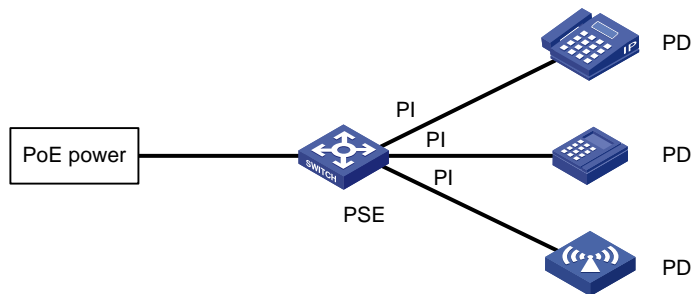
Overview

IEEE 802.3af-compliant power over Ethernet (PoE) enables a power sourcing equipment (PSE) to supply power to powered devices (PDs) through Ethernet interfaces over straight-through twisted pair cables. Examples of PDs include IP telephones, wireless APs, portable chargers, card readers, Web cameras, and data collectors. A PD can also use a different power source from the PSE at the same time for power redundancy.

As shown in [Figure 14](#), a PoE system comprises the following elements:

- **PoE power**—The entire PoE system is powered by the PoE power.
- **PSE**—The PSE supplies power for PDs. A PSE can examine the Ethernet cables connected to PoE interfaces, search for PDs, classify them, and supply power to them. When detecting that a PD is unplugged, the PSE stops supplying power to the PD. A PSE can be built-in (Endpoint) or external (Midspan). The switch uses built-in PSEs. To display the mapping between a PSE ID and the slot number of an interface card, execute the **display poe device** command.
The PSE ID is the *switch member ID* × 3 + 1. For example, if the member ID of the device is 3, the PSE ID of the device is 3 × 3 + 1 = 10.
- **PI**—An Ethernet interface with the PoE capability is called PoE interface.
- **PD**—A PD receives power from the PSE. You can also connect a PD to a redundant power source for reliability.

Figure 16 PoE system diagram



PoE configuration task list

You can configure a PoE interface directly at the CLI or by configuring a PoE profile and applying the PoE profile to the PoE interface.

To configure a single PoE interface, configure it at the CLI. To configure several PoE interfaces in batches, use the PoE profile. For a PoE configuration parameter of a PoE interface, you can select only one mode (including modification and removal of a PoE interface).

Configuration guidelines

- Before configuring PoE, make sure the PoE power supply and PSE are operating normally. Otherwise, either you cannot configure PoE or the PoE configuration does not take effect.
- If the PoE power supply is turned off while a device is starting up, the PoE configuration in the PoE profile might become invalid.

Complete these tasks to configure PoE:

Task	Remarks
Enabling PoE for a PoE interface	Required.
Enabling the PSE to detect nonstandard PDs	Optional.
Configuring the maximum PoE interface power	Optional.
Configuring PoE interface power management	Optional.
Configuring the PoE monitoring function:	
<ul style="list-style-type: none"> • Configuring PSE power monitoring 	Optional.

Task	Remarks
<ul style="list-style-type: none"> Monitoring PD 	Optional. The device automatically monitors PDs when supplying power to them, so no configuration is required.
Configuring PoE interface through PoE profile:	
<ul style="list-style-type: none"> Configuring PoE profile 	Optional.
<ul style="list-style-type: none"> Applying a PoE profile 	Optional.
Upgrading PSE processing software in service	Optional.

Enabling PoE for a PoE interface

The system does not supply power to or reserve power for the PDs connected to a PoE interface unless the PoE interface is enabled with the PoE function.

You can enable PoE for a PoE interface if the PoE interface does not result in PoE power overload. Otherwise, whether you can enable PoE for the PoE interface depends on whether the PoE interface is enabled with the PoE power management function. For more information about PoE interface power management, see "[Configuring PoE interface power management](#)."

- If the PoE interface is not enabled with the PoE power management function, you cannot enable PoE for the PoE interface.
- If the PoE interface is enabled with the PoE power management function, you can enable PoE for the PoE interface. Whether the PDs can be powered depends on other factors, such as the power supply priority of the PoE interface.

The PSE supplies power over category 3/5 twisted pair cable for a PoE interface in the following modes:

- Over signal wires**—The PSE uses data pairs (pins 1, 2 and 3, 6) to supply DC power to PDs.
- Over spare wires**—The PSE uses spare pairs (pins 4, 5 and 7, 8) to supply DC power to PDs.

When the sum of the power consumption of all powered PoE interfaces on a PSE exceeds the maximum power of the PSE, the system considers the PSE as overloaded. The maximum PSE power is user configurable.

A PSE can supply power to a PD only when the selected power supply mode is supported by both the PSE and PD. If the PSE and PD support different power supply modes (for example, the PSE does not support power over spare wires, while the PD supports power over spare wires), you have to change the order of the lines in the twisted pair cable to supply power to the PD.

The switch's PoE interfaces can supply power only over signal wires.

To enable PoE for a PoE interface:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter PoE interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable PoE for the PoE interface.	poe enable	By default, this function is disabled.

Step	Command	Remarks
4. Configure a description for the PD connected to the PoE interface.	poe pd-description <i>text</i>	Optional. By default, no description for the PD connected to the PoE interface is available.

Enabling the PSE to detect nonstandard PDs

There are standard PDs and nonstandard PDs. Usually, the PSE can detect only standard PDs and supply power to them. The PSE can detect nonstandard PDs and supply power to them only if you enable the PSE to detect nonstandard PDs.

To enable the PSE to detect nonstandard PDs:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the PSE to detect nonstandard PDs.	poe legacy enable pse <i>pse-id</i>	By default, the PSE can detect only standard PDs.

Configuring the maximum PoE interface power

The maximum PoE interface power is the maximum power that the PoE interface can provide to the connected PD. If the PD requires more power than the maximum PoE interface power, the PoE interface does not supply power to the PD.

To configure the maximum PSE power:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter PoE interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the maximum power for the PoE interface.	poe max-power <i>max-power</i>	Optional. The default is 30000 milliwatts.

Configuring PoE interface power management

The power supply priority of a PD depends on the priority of the PoE interface. In descending order, the power-supply priority levels of a PoE interface are critical, high, and low. Power supply to a PD is subject to PoE interface power management policies.

All PSEs implement the same PoE interface power management policies. If PoE supplies power to a PD, the following actions occur:

- If the PoE power is overloaded and PSE power management is not enabled, no power is supplied to a new PD.
- If the PoE power is overloaded and a PSE power-management-priority policy is enabled, the PD that has a lower priority is first disconnected to guarantee the power supply to a new PD that has a higher priority.

The guaranteed remaining PoE power is the maximum PoE power minus the power allocated to the critical PoE interface, regardless of whether PoE is enabled for the PoE interface. If this is lower than the maximum power of the PoE interface, you cannot set the power priority of the PoE interface to

critical. Otherwise, you can set the power priority to **critical**, and this PoE interface preempts the power of the PoE interface that has a lower priority level. In this case, the PoE interface whose power is preempted is disconnected, but its configuration remains unchanged. If you change the priority of the PoE interface from **critical** to a lower level, the PDs connecting to other PoE interfaces have an opportunity to be powered.

A guard band of 19 watts guard band is reserved for each PoE interface on the device to prevent a PD from powering off because of a sudden increase of power. If the remaining power of the PSE where the PoE interfaces reside is lower than 19 watts and no priority is configured for a PoE interface, the PSE does not supply power to the new PD. If the remaining power of the PSE where the PoE interfaces reside is lower than 19 watts but priority is configured for PoE interfaces, the PoE interface that has a higher priority can preempt the power of the PoE interface that has a lower priority to ensure normal operation of the higher priority interface.

If a sudden increase of the PD power results in PSE power overload, power supply to the PD on the PoE interface that has a lower priority is stopped to ensure power supply to the PD that has a higher priority.

Configuration prerequisites

Enable PoE for PoE interfaces.

Configuration procedure

To configure PoE interface power management:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the PoE interface power management priority policy.	poe pd-policy priority	By default, this policy is not configured.
3. Enter PoE interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
4. Configure the power supply priority for a PoE interface.	poe priority { critical high low }	Optional. By default, low is the power supply priority for the PSE.

Configuring the PoE monitoring function

With the PoE monitoring function enabled, the system monitors the parameter values related to PoE power supply, PSE, PD, and device temperature in real time. When a specific value exceeds the limited range, the system automatically takes self-protection measures.

Configuring PSE power monitoring

When the PSE power exceeds or drops below the specified threshold, the system sends trap messages.

To configure a power alarm threshold for the PSE:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure a power alarm threshold for the PSE.	poe utilization-threshold <i>utilization-threshold-value</i> pse <i>pse-id</i>	Optional. The default setting is 80%.

Monitoring PD

When a PSE starts or ends power supply to a PD, the system sends a trap message.

Configuring PoE interface through PoE profile

You can configure a PoE interface either at the CLI or by using a PoE profile and applying the PoE profile to the PoE interface.

To configure a single PoE interface, configure it at the CLI. To configure PoE interfaces in batches, use a PoE profile.

A PoE profile is a collection of configurations that contain multiple PoE features. On large-scale networks, you can apply a PoE profile to multiple PoE interfaces, and these interfaces have the same PoE features. If the PoE interface connecting to a PD changes to another one, apply the PoE profile applied on the originally connected interface to the currently connected interface instead of reconfiguring the features defined in the PoE profile one by one, simplifying the PoE configurations.

The device supports multiple PoE profiles. You can define PoE configurations based on each PD, save the configurations for different PDs into different PoE profiles, and apply the PoE profiles to the access interfaces of PDs accordingly.

Configuring PoE profile

If a PoE profile is applied, it cannot be deleted or modified before you cancel its application.

The **poe max-power** *max-power* and **poe priority** { **critical** | **high** | **low** } commands must be configured in only one way, that is, either at the CLI or by configuring PoE profile.

A PoE parameter on a PoE interface must be configured, modified and deleted in only one way. If a parameter configured in a way (for example, at the CLI) is then configured in the other way (for example, through PoE profile), the latter configuration fails and the original one is still effective. To make the latter configuration effective, you must cancel the original one first.

To configure a PoE profile:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a PoE profile, and enter PoE profile view.	poe-profile <i>profile-name</i> [<i>index</i>]	N/A
3. Enable PoE for the PoE interface.	poe enable	By default, this function is disabled.
4. Configure the maximum power for the PoE interface.	poe max-power <i>max-power</i>	Optional. By default, 30000 milliwatts is the maximum power for the PoE interface.
5. Configure power supply priority for the PoE interface.	poe priority { critical high low }	Optional. By default, low is the power supply priority for the PoE interface.

Applying a PoE profile

You can apply a PoE profile in either system view or interface view. If you perform application to a PoE interface in both views, the latter application takes effect. To apply a PoE profile to multiple PoE interfaces, the system view is more efficient.

A PoE profile can apply to multiple PoE interfaces, but a PoE interface can have only one PoE profile.

To apply a PoE profile to multiple interfaces in system view:

Step	Command
1. Enter system view.	system-view
2. Apply a PoE profile to one or multiple PoE interfaces.	apply poe-profile { index <i>index</i> name <i>profile-name</i> } interface <i>interface-range</i>

To apply a PoE profile to an interface in interface view:

Step	Command
1. Enter system view.	system-view
2. Enter PoE interface view.	interface <i>interface-type interface-number</i>
3. Apply a PoE profile to the PoE interface.	apply poe-profile { index <i>index</i> name <i>profile-name</i> }

Upgrading PSE processing software in service

You can upgrade the PSE processing software in service in either of the following two modes:

- **Refresh mode**—Enables you to update the PSE processing software without deleting it. Normally, you can upgrade the PSE processing software in the refresh mode through the command line.
- **Full mode**—Deletes the PSE processing software and reloads it. If the PSE processing software is damaged (in this case, you can execute none of PoE commands successfully), you can upgrade the PSE processing software in full mode to restore the PSE function.

An in-service PSE processing software upgrade may be unexpectedly interrupted (for example, an error results in device reboot). If you fail to upgrade the PSE processing software in full mode after reboot, you can power off the device and restart it before upgrading it in full mode again. After upgrade, restart the device manually to make the new PSE processing software take effect.

To upgrade the PSE processing software in service:

Step	Command
1. Enter system view.	system-view
2. Upgrade the PSE processing software in service.	poe update { full refresh } <i>filename</i> pse <i>pse-id</i>

Displaying and maintaining PoE

Task	Command	Remarks
Display PSE information.	display poe device [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display the power supplying state of the specified PoE interface.	display poe interface [<i>interface-type interface-number</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view

Task	Command	Remarks
Display power information for PoE interfaces.	display poe interface power [<i>interface-type interface-number</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display information about PSE.	display poe pse [<i>pse-id</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display the power supply states of all PoE interfaces connected to the PSE.	display poe pse pse-id interface [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display power information for all PoE interfaces connected to the PSE.	display poe pse pse-id interface power [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display the configurations and applications of the PoE profile.	display poe-profile [index <i>index</i> name <i>profile-name</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display the configurations and applications of the PoE profile applied to the specified PoE interface.	display poe-profile interface <i>interface-type interface-number</i> [{ begin exclude include } <i>regular-expression</i>]	Available in any view

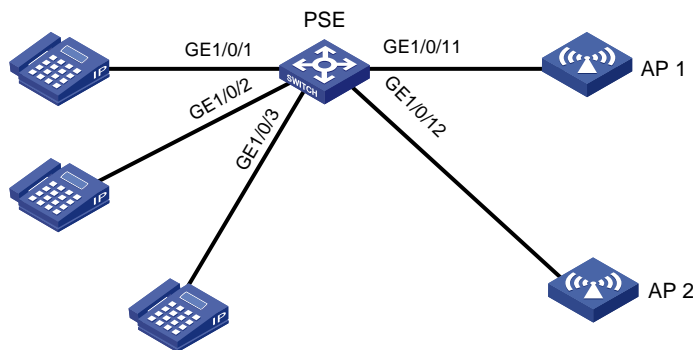
PoE configuration example

Network requirements

As shown in Figure 15, the device supplies power to PDs through its PoE interfaces:

- GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 are connected to IP telephones.
- GigabitEthernet 1/0/11 and GigabitEthernet 1/0/12 are connected to APs.
- The power supply priority of IP telephones is higher than that of the APs, for which the PSE supplies power to IP telephones first when the PSE power is overloaded.
- The maximum power of AP2 connected to GigabitEthernet 1/0/12 does not exceed 9000 milliwatts.

Figure 17 Network diagram



Configuration procedure

Enable PoE and specify the **critical** power supply priority on GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```

[Sysname-GigabitEthernet1/0/1] poe enable
[Sysname-GigabitEthernet1/0/1] poe priority critical
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] poe enable
[Sysname-GigabitEthernet1/0/2] poe priority critical
[Sysname-GigabitEthernet1/0/2] quit
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] poe enable
[Sysname-GigabitEthernet1/0/3] poe priority critical
[Sysname-GigabitEthernet1/0/3] quit

# Enable PoE on GigabitEthernet 1/0/11 and GigabitEthernet 1/0/12, and configure the maximum
power of GigabitEthernet 1/0/12 as 9000 milliwatts.
[Sysname] interface gigabitethernet 1/0/11
[Sysname-GigabitEthernet1/0/11] poe enable
[Sysname-GigabitEthernet1/0/11] quit
[Sysname] interface gigabitethernet 1/0/12
[Sysname-GigabitEthernet1/0/12] poe enable
[Sysname-GigabitEthernet1/0/12] poe max-power 9000

```

Troubleshooting PoE

Setting the priority of a PoE interface to **critical** fails

Analysis

- The guaranteed remaining power of the PSE is lower than the maximum power of the PoE interface.
- The priority of the PoE interface is already set.

Solution

- In the first case, either increase the maximum PSE power or reduce the maximum power of the PoE interface if the guaranteed remaining power of the PSE cannot be modified.
- In the second case, remove the priority that is already configured.

Failure to apply a PoE profile to a PoE interface

Analysis

- Some configurations in the PoE profile are already configured.
- Some configurations in the PoE profile do not meet the configuration requirements of the PoE interface.
- Another PoE profile is already applied to the PoE interface.

Solution

- In the first case, remove the original configurations of those configurations.
- In the second case, modify the configurations in the PoE profile.
- In the third case, remove the application of the undesired PoE profile to the PoE interface.

Failure to configure an AC input under-voltage threshold

Analysis

The AC input under-voltage threshold is greater than or equal to the AC input over-voltage threshold.

Solution

Set the AC input under-voltage threshold lower than the AC input over-voltage threshold.

PoE configuration commands

apply poe-profile

Syntax

```
apply poe-profile { index index | name profile-name }  
undo apply poe-profile { index index | name profile-name }
```

View

PoE interface view

Default level

2: System level

Parameters

index *index*: Specifies a PoE configuration file by its index number in the range of 1 to 100.

name *profile-name*: Specifies a PoE configuration file by its name, a string of 1 to 15 characters.

Description

Use **apply poe-profile** to apply a PoE configuration file to a PoE interface.

Use **undo apply poe-profile** to remove a PoE configuration file from a PoE interface.

The index number, instead of the name, of the PoE configuration file is displayed when you execute the **display this** command.

Related commands: **display poe-profile** and **apply poe-profile interface**.

Examples

Apply the PoE configuration file named **forIPphone** to PoE interface GigabitEthernet 1/0/20.

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/20  
[Sysname-GigabitEthernet1/0/20] apply poe-profile name forIPphone  
[Sysname-GigabitEthernet1/0/20] display this  
#  
interface GigabitEthernet1/0/20  
    apply poe-profile index 1  
#  
return
```

apply poe-profile interface

Syntax

```
apply poe-profile { index index | name profile-name } interface interface-range
```

undo apply poe-profile { **index** *index* | **name** *profile-name* } **interface** *interface-range*

View

System view

Default level

2: System level

Parameters

index *index*: Specifies a PoE configuration file by its index number in the range of 1 to 100.

name *profile-name*: Specifies a PoE configuration file by its name, a string of 1 to 15 characters.

interface-range: Specifies a range of Ethernet interfaces in the form of *interface-type interface-number* [**to** *interface-type interface-number*], where *interface-type interface-number* represents the interface type and interface number. The start interface number must be smaller than the end interface number. If an interface in the specified range does not support PoE, it is ignored when the PoE configuration file is applied.

Description

Use **apply poe-profile interface** to apply a PoE configuration file to a range of PoE interfaces.

Use **undo apply poe-profile interface** to remove a PoE configuration file from a range of PoE interfaces.

Related commands: **display poe-profile interface** and **apply poe-profile**.

Examples

Apply the PoE configuration file named **forIPphone** to PoE interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
```

```
[Sysname] apply poe-profile name forIPphone interface gigabitethernet 1/0/1
```

Apply the PoE configuration file with index number 1 to PoE interfaces GigabitEthernet 1/0/2 through GigabitEthernet 1/0/8.

```
<Sysname> system-view
```

```
[Sysname] apply poe-profile index 1 interface gigabitethernet 1/0/2 to gigabitethernet 1/0/8
```

display poe device

Syntax

display poe device [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

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

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

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

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

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

Description

Use **display poe device** to display brief PSE information, including the ID, slot number, and state of PSEs.

Examples

Display PSE information. The output depends on the device model.

```
<Sysname> display poe device
```

PSE ID	SlotNo	SubSNo	PortNum	MaxPower(W)	State	Model
4	1	0	48	370	off	LSW124POED-M+S

Table 21 Command output

Field	Description
PSE ID	ID of the PSE.
SlotNo	Slot number of the PSE.
SubSNo	Sub-slot number of the PSE.
PortNum	Number of PoE interfaces on the PSE.
MaxPower(W)	Maximum power of the PSE.
State	PSE state: <ul style="list-style-type: none">• on—The PSE is supplying power.• off—The PSE stops supplying power.• faulty—The PSE fails.
Model	PSE model.

display poe interface

Syntax

```
display poe interface [ interface-type interface-number ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

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

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

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

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

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

Description

Use **display poe interface** to display power supplying information for PoE interfaces.

If no interface is specified, this command displays power supplying information for all PoE interfaces.

Examples

Display power supplying information for GigabitEthernet 1/0/1.

```
<Sysname> display poe interface gigabitethernet 1/0/1
Port Power Enabled           : enabled
Port Power Priority          : high
Port Operating Status        : on
Port IEEE Class              : 0
Port Detection Status        : delivering-power
Port Power Mode              : signal
Port Current Power           : 3600      mW
Port Average Power           : 3662      mW
Port Peak Power              : 3900      mW
Port Max Power               : 15400     mW
Port Current                 : 71        mA
Port Voltage                 : 50.9      V
Port PD Description          : IP Phone For Room 101
```

Table 22 Command output

Field	Description
Port Power Enabled	PoE state: <ul style="list-style-type: none"> enabled. disabled.
Port Power Priority	Power priority of the PoE interface: <ul style="list-style-type: none"> critical (highest) high low
Port Operating Status	Operating state of a PoE interface: <ul style="list-style-type: none"> off—PoE is disabled. on—Power is supplied for a PoE interface normally. power-lack—Guaranteed remaining power of the PSE is not high enough to supply power for a critical PoE interface. power-deny—PSE refuses to supply power. The power required by the powered device (PD) is higher than the configured power. power-itself—External equipment is supplying power for itself. power-limit—PSE is supplying a limited power. The power required by the PD is higher than the configured power and the PSE still supplies the configured power.
Port IEEE class	PD power class: 0, 1, 2, 3, or 4. If PoE is not supported, this field displays a hyphen (-).
Port Detection Status	Power detection state of a PoE interface: <ul style="list-style-type: none"> disabled—PoE function is disabled. searching—PoE interface is searching for the PD. delivering-power—PoE interface is supplying power for the PD. fault—There is a fault defined in 802.3af. test—PoE interface is under test. other-fault—There is a fault other than defined in 802.3af. pd-disconnect—PD is disconnected.
Port Power Mode	Power mode of a PoE interface. signal indicates that power is supplied over signal cables.

Field	Description
Port Current Power	Current power of a PoE interface, including PD consumption power and transmission loss. Transmission loss usually does not exceed one watt.
Port Average Power	Average power of a PoE interface.
Port Peak Power	Peak power of a PoE interface.
Port Max Power	Maximum power of a PoE interface.
Port Current	Current of a PoE interface.
Port Voltage	Voltage of a PoE interface.
Port PD Description	Description of the PD connected to the PoE interface, which is used to identify the type and location of the PD.

Display power supplying information for all PoE interfaces.

```
<Sysname> display poe interface
```

Interface	Status	Priority	CurPower (W)	Operating Status	IEEE	Detection Class Status
PSE : 4						
GE1/0/1	disabled	low	0.0	off	0	disabled
GE1/0/2	disabled	low	0.0	off	0	disabled
GE1/0/3	disabled	low	0.0	off	0	disabled
GE1/0/4	disabled	low	0.0	off	0	disabled
GE1/0/5	enabled	low	0.0	off	0	searching
GE1/0/6	enabled	low	0.0	off	0	searching
GE1/0/7	disabled	low	0.0	off	0	disabled
GE1/0/8	disabled	low	0.0	off	0	disabled
...						
GE1/0/47	disabled	low	0.0	off	0	disabled
GE1/0/48	disabled	low	0.0	off	0	disabled
--- 0 port(s) on, 0.0 (W) consumed, 800.0 (W) remaining ---						

Table 23 Command output

Field	Description
Interface	Shortened form of a PoE interface.
Enable	PoE state: <ul style="list-style-type: none"> enabled. disabled.
Priority	Power priority of a PoE interface: <ul style="list-style-type: none"> critical (highest) high low
CurPower	Current power of a PoE interface.

Field	Description
Operating Status	<p>Operating state of a PoE interface:</p> <ul style="list-style-type: none"> • off—PoE is disabled. • on—Power is supplied for a PoE interface normally. • power-lack—Guaranteed remaining power of the PSE is not high enough to supply power for a critical PoE interface. • power-deny—PSE refuses to supply power. The power required by the powered device (PD) is higher than the configured power. • power-itself—External equipment is supplying power for itself. • power-limit—PSE is supplying a limited power. The power required by the PD is higher than the configured power and the PSE still supplies the configured power.
IEEE class	PD power class defined by IEEE.
Detection Status	<p>Power detection state of a PoE interface:</p> <ul style="list-style-type: none"> • disabled—PoE function is disabled. • searching—PoE interface is searching for the PD. • delivering-power—PoE interface is supplying power for the PD. • fault—There is a fault defined in 802.3af. • test—PoE interface is under test. • other-fault—There is a fault other than defined in 802.3af. • pd-disconnect—PD is disconnected.
port(s) on	Number of PoE interfaces that are supplying power.
consumed	Power consumed by the current PoE interface.
Remaining	Remaining power that the PSE can still supply.

display poe interface power

Syntax

```
display poe interface power [ interface-type interface-number ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

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

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

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

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

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

Description

Use **display poe interface power** to display power information and settings for PoE interfaces.

If no interface is specified, this command displays power information for all PoE interfaces.

Examples

Display power information for GigabitEthernet 1/0/1.

```
<Sysname> display poe interface power GigabitEthernet 1/0/1
Interface    CurPower    PeakPower    MaxPower    PD Description
              (W)         (W)          (W)
GE1/0/1      0.0         0.0          30.0
```

Display power information for all PoE interfaces.

```
<Sysname> display poe interface power
Interface    CurPower    PeakPower    MaxPower    PD Description
              (W)         (W)          (W)
PSE : 4
GE1/0/1      0.0         0.0          15.4
GE1/0/2      0.0         0.0          30.0
GE1/0/3      0.0         0.0          30.0
GE1/0/4      0.0         0.0          30.0
GE1/0/5      0.0         0.0          30.0
GE1/0/6      0.0         0.0          30.0
GE1/0/7      0.0         0.0          30.0
GE1/0/8      0.0         0.0          30.0
...
GE1/0/47     0.0         0.0          30.0
GE1/0/48     0.0         0.0          30.0
--- 0 port(s) on, 0.0 (W) consumed, 800.0 (W) remaining ---
```

Table 24 Command output

Field	Description
Interface	Shortened form of a PoE interface.
CurPower	Current power of a PoE interface.
PeakPower	Peak power of a PoE interface.
MaxPower	Maximum power of a PoE interface.
PD Description	Description of the PD connected with a PoE interface. When the description contains more than 34 characters, the first 30 characters followed by four dots are displayed.
port(s) on	Number of PoE interfaces that are supplying power.
consumed	Power consumed by all PoE interfaces.
Remaining	Remaining power that the PSE can still supply.

display poe pse

Syntax

```
display poe pse [ pse-id ] [ { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

pse-id: Specifies a PSE by its ID. To view PSE ID and slot mappings, use the **display poe device** command. If no PSE is specified, this command displays information about all PSEs.

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

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

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

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

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

Description

Use **display poe pse** to display detailed PSE information, including its software version, hardware version, power settings, and power statistics.

Examples

Display detailed information about the PSE.

```
<Sysname> display poe pse
PSE ID                : 4
PSE Slot No           : 1
PSE SubSlot No        : 0
PSE Model              :
PSE Power Enabled      : enabled
PSE Power Priority     : -
PSE Current Power      : 0          W
PSE Average Power      : 0          W
PSE Peak Power         : 0          W
PSE Max Power          : 800        W
PSE Remaining Guaranteed : 800      W
PSE CPLD Version       : -
PSE Software Version   : 400
PSE Hardware Version   : 57603
PSE Legacy Detection   : disabled
PSE Utilization-threshold : 80
PSE Pd-policy Mode     : disable
PSE PD Disconnect Detect Mode : DC
```

Table 25 Command output

Field	Description
PSE Slot No	Member of the PSE
PSE SubSlot No	Subslot number of the PSE
PSE Model	Model of the PSE module
PSE Power Enabled	PoE state, enabled or disabled
PSE Power Priority	Power priority of the PSE

Field	Description
PSE Current Power	Current power of the PSE
PSE Average Power	Average power of the PSE
PSE Peak Power	Peak power of the PSE
PSE Max Power	Maximum power of the PSE
PSE Remaining Guaranteed	Guaranteed remaining power of the PSE = Guaranteed maximum power of the PSE– the sum of the maximum power of the critical PoE interfaces of the PSE
PSE CPLD Version	PSE CPLD version
PSE Software Version	PSE software version number
PSE Hardware Version	PSE hardware version number
PSE Legacy Detection	Nonstandard PD detection by the PSE: <ul style="list-style-type: none"> • Enabled • Disabled
PSE Utilization-threshold	PSE power alarm threshold
PSE Pd-policy Mode	PD power management policy mode
PSE PD Disconnect Detect Mode	PD disconnection detection mode

display poe pse interface

Syntax

display poe pse *pse-id* **interface** [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

pse *pse-id*: Specifies a PSE ID. To display PSE ID and slot mappings, use the **display poe device** command.

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

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

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

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

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

Description

Use **display poe pse interface** to display the PoE state of all PoE interfaces connected to a PSE.

Examples

Display the power state of all PoE interfaces connected to PSE 4.

```
<Sysname> display poe pse 4 interface
```

Interface	Status	Priority	CurPower (W)	Operating Status	IEEE Class	Detection Status
GE1/0/1	disabled	low	0.0	off	0	disabled
GE1/0/2	disabled	low	0.0	off	0	disabled
GE1/0/3	disabled	low	0.0	off	0	disabled
GE1/0/4	disabled	low	0.0	off	0	disabled
GE1/0/5	disabled	low	0.0	off	0	disabled
GE1/0/6	disabled	low	0.0	off	0	disabled
GE1/0/7	disabled	low	0.0	off	0	disabled
GE1/0/8	disabled	low	0.0	off	0	disabled
.....						
GE1/0/23	disabled	low	0.0	off	0	disabled
GE1/0/24	disabled	low	0.0	off	0	disabled

--- 0 port(s) on, 0.0 (W) consumed, 800.0 (W) remaining ---

Table 26 Command output

Field	Description
Interface	Shortened form of a PoE interface.
Status	PoE enabled/disabled state. For the value, see Table 21 .
Priority	Priority of a PoE interface. For the value, see Table 21 .
CurPower	Current power of a PoE interface.
Operating Status	Operating state of a PoE interface. For the value, see Table 21 .
IEEE Class	PD power class.
Detection Status	Power detection state of a PoE interface. For the value, see Table 21 .
port(s) on	Number of PoE interfaces that are supplying power.
consumed	Power consumed by PoE interfaces on the PSE.
Remaining	Remaining power that the PSE can still supply.

display poe pse interface power

Syntax

display poe pse *pse-id* **interface power** [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

pse *pse-id*: Specifies a PSE ID. To view the mapping between PSE ID and slot, use the **display poe device** command.

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

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

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

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

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

Description

Use **display poe pse interface power** to display power information for PoE interfaces connected with the PSE.

Examples

Display the power state of PoE interfaces connected with PSE 4.

```
<Sysname> display poe pse 4 interface power
```

Interface	Status	Priority	CurPower (W)	Operating Status	IEEE Class	Detection Status
GE1/0/1	disabled	low	0.0	off	0	disabled
GE1/0/2	disabled	low	0.0	off	0	disabled
GE1/0/3	disabled	low	0.0	off	0	disabled
GE1/0/4	disabled	low	0.0	off	0	disabled
GE1/0/5	enabled	low	0.0	off	0	searching
.....						
GE1/0/47	disabled	low	0.0	off	0	disabled
GE1/0/48	disabled	low	0.0	off	0	disabled
--- 0 port(s) on, 0.0 (W) consumed, 800.0 (W) remaining ---						

Table 27 Command output

Field	Description
Interface	Shortened form of a PoE interface.
CurPower	Current power of a PoE interface.
PeakPower	Peak power of a PoE interface.
MaxPower	Maximum power of a PoE interface.
PD Description	Description of the PD connected with a PoE interface. When the description contains more than 34 characters, the first 30 characters followed by four dots are displayed.
port(s) on	Number of PoE interfaces that are supplying power.
consumed	Power being consumed by all PoE interfaces.
Remaining	Remaining power that the PSE can still supply.

display poe-profile

Syntax

```
display poe-profile [ index index | name profile-name ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

index *index*: Specifies a PoE configuration file by its index number in the range of 1 to 100.

name *profile-name*: Specifies a PoE configuration file by its name, a string of 1 to 15 characters.

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

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

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

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

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

Description

Use **display poe-profile** to display information about the PoE configuration file.

If no argument is specified, all information about the configurations and applications of existing PoE configuration files is displayed.

Examples

Display information about all PoE configuration files.

```
<Sysname> display poe-profile
Poe-profile      Index  ApplyNum  Interface  Configuration
forIPphone       1      6         GE1/0/5    poe enable
                  GE1/0/6    poe priority critical
                  GE1/0/7
                  GE1/0/8
                  GE1/0/9
                  GE1/0/10
forAP             2      2         GE1/0/11    poe enable
                  GE1/0/12    poe max-power 14000
---  2 poe-profile(s) created, 8 port(s) applied  ---
```

Display information about the PoE configuration file with index number 1.

```
<Sysname> display poe-profile index 1
Poe-profile      Index  ApplyNum  Interface  Configuration
forIPphone       1      6         GE1/0/5    poe enable
                  GE1/0/6    poe priority critical
                  GE1/0/7
                  GE1/0/8
                  GE1/0/9
                  GE1/0/10
---  6 port(s) applied  ---
```

Display information about PoE configuration file forIPphone.

```
<Sysname> display poe-profile name AA
Poe-profile      Index  ApplyNum  Interface  Configuration
forIPphone       1      6         GE1/0/5    poe enable
                  GE1/0/6    poe priority critical
                  GE1/0/7
                  GE1/0/8
                  GE1/0/9
                  GE1/0/10
```

```
--- 6 port(s) applied ---
```

Table 28 Command output

Field	Description
Poe-profile	Name of the PoE configuration file
Index	Index number of the PoE configuration file
ApplyNum	Number of PoE interfaces to which a PoE configuration file is applied
Interface	Shortened form of the PoE interface to which the PoE configuration is applied
Configuration	Configurations of the PoE configuration file
poe-profile(s) created	Number of PoE configuration files
port(s) applied	Sum of the number of PoE interfaces to which all PoE configuration files are respectively applied

display poe-profile interface

Syntax

display poe-profile interface *interface-type interface-number* [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

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

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

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

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

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

Description

Use **display poe-profile interface** to display all information about the configurations and applications of the PoE configuration file that currently takes effect on the specified PoE interface.

Examples

Display all information about the configurations and applications of the current PoE configuration file applied to GigabitEthernet 1/0/1.

```
<Sysname> display poe-profile interface gigabitethernet 1/0/1
Poe-profile      Index  ApplyNum  Interface  Current Configuration
forIPphone      1      6         GE1/0/1    poe enable
                                     poe priority critical
```

Not all the configurations of a PoE configuration file can be applied successfully, so only the configurations that currently take effect on the interface are displayed. For the descriptions for other fields, see [Table 26](#).

poe enable

Syntax

poe enable

undo poe enable

View

PoE interface view, PoE-profile file view

Default level

2: System level

Parameters

None

Description

Use **poe enable** to enable PoE on a PoE interface.

Use **undo poe enable** to disable PoE on a PoE interface.

By default, PoE is disabled on a PoE interface.

If a PoE configuration file is already applied to a PoE interface, remove the application of the file to the PoE interface before configuring the interface in PoE-profile view.

If a PoE configuration file is applied to a PoE interface, remove the application of the file to the PoE interface before configuring the interface in PoE interface view.

Examples

Enable PoE on a PoE interface.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe enable
```

Enable PoE on a PoE interface through a PoE configuration file.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe enable
[Sysname-poe-profile-abc-1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] apply poe-profile name abc
```

poe legacy enable

Syntax

poe legacy enable pse *pse-id*

undo poe legacy enable pse *pse-id*

View

System view

Default level

2: System level

Parameters

pse *pse-id*: Specifies a PSE ID.

Description

Use **poe legacy enable** to enable the PSE to detect nonstandard PDs.

Use **undo poe legacy enable** to disable the PSE from detecting nonstandard PDs.

By default, the PSE is disabled from detecting nonstandard PDs.

Examples

Enable PSE 7 to detect nonstandard PDs (for a device with multiple PSEs).

```
<Sysname> system-view
```

```
[Sysname] poe legacy enable pse 7
```

poe max-power

Syntax

poe max-power *max-power*

undo poe max-power

View

PoE interface view, PoE-profile file view

Default level

2: System level

Parameters

max-power: Specifies the maximum power in milliwatts allocated to a PoE interface. It is in the range of 1000 to 30000 milliwatts.

Description

Use **poe max-power** to configure the maximum power for a PoE interface.

Use **undo poe max-power** to restore the default.

By default, the maximum power that a PoE interface can supply is 30000 milliwatts.

Examples

Set the maximum power of GigabitEthernet 1/0/1 to 12000 milliwatts.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] poe max-power 12000
```

Set the maximum power of GigabitEthernet 1/0/1 to 12000 milliwatts in the PoE configuration file **abc**.

```
<Sysname> system-view
```

```
[Sysname] poe-profile abc
```

```
[Sysname-poe-profile-abc-1] poe max-power 12000
```

```
[Sysname-poe-profile-abc-1] quit
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] apply poe-profile name abc
```

poe pd-description

Syntax

poe pd-description *text*
undo poe pd-description

View

PoE interface view

Default level

2: System level

Parameters

text: Describes of the PD connected to a PoE interface, a string of 1 to 80 characters.

Description

Use **poe pd-description** to configure a description for the PD connected to a PoE interface.

Use **undo poe pd-description** to restore the default.

By default, no description is available for the PD connected to a PoE interface.

Examples

Configure the description for the PD connected to GigabitEthernet 1/0/1 as IP Phone for Room 101.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] poe pd-description IP Phone For Room 101
```

poe pd-policy priority

Syntax

poe pd-policy priority
undo poe pd-policy priority

View

System view

Default level

2: System level

Parameters

None

Description

Use **poe pd-policy priority** to configure a power management priority policy on the PoE interface.

Use **undo poe pd-policy priority** to restore the default.

By default, no power management priority policy is configured on the PoE interface.

- If the policy is enabled, and the PoE interface needs to supply power to outside in the case that the PSE is overloaded, the system allows the PoE interface to enable the PoE function, but whether the power can be supplied depends on the PoE interface priority.

- If the policy is not enabled, and the PoE interface needs to supply power to outside in the case that the PSE is overloaded, the system will not allow the PoE interface to enable the PoE function.

Examples

Configure a PD power management priority policy

```
<Sysname> system-view
[Sysname] poe pd-policy priority
```

poe priority

Syntax

```
poe priority { critical | high | low }
undo poe priority
```

View

PoE interface view, PoE-profile file view

Default level

2: System level

Parameters

critical: Sets the power priority of a PoE interface to **critical**. The PoE interface whose power priority level is **critical** operates in guaranteed mode. In other words, power is first supplied to the PD connected to this critical PoE interface.

high: Sets the power priority of a PoE interface to **high**.

low: Sets the power priority of a PoE interface to **low**.

Description

Use **poe priority** to configure a power priority level for a PoE interface.

Use **undo poe priority** to restore the default.

By default, the power priority of a PoE interface is **low**.

When the PoE power is insufficient, power is first supplied to PoE interfaces with a higher priority level.

If a PoE configuration file is already applied to a PoE interface, remove the application of the file to the PoE interface before configuring the interface in PoE-profile view.

If a PoE configuration file is applied to a PoE interface, remove the application of the file to the PoE interface before configuring the interface in PoE interface view.

If two PoE interfaces have the same priority level, the PoE interface with a smaller ID has the higher priority level.

Examples

Set the power priority of GigabitEthernet 1/0/1 to **critical**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe priority critical
```

Set the power priority of GigabitEthernet 1/0/1 to **critical** through a PoE configuration file.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe priority critical
```

```
[Sysname-poe-profile-abc-1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] apply poe-profile name abc
```

poe update

Syntax

poe update { **full** | **refresh** } *filename* [**pse** *pse-id*]

View

System view

Default level

2: System level

Parameters

full: Specifies the upgrade of the PSE processing software in full mode when the software is unavailable.

refresh: Specifies the upgrade of the PSE processing software in refresh mode when the software is available.

filename: Specifies the name of the upgrade file, a string of 1 to 64 characters. This file must be in the root directory of the file system of the device.

pse *pse-id*: Specifies a PSE ID.

Description

Use **poe update** to upgrade the PSE processing software online.

If none of the PoE commands can be successfully executed, use the full mode to restore the PSE firmware. In any other case, use the full mode only when the refresh mode cannot work correctly.

If you do not provide the *pse-id* argument, the PSEs of all IRF member devices are upgraded.

Examples

Upgrade the processing software of PSE 7 in service.

```
<Sysname> system-view
```

```
[Sysname] poe update refresh 0400_001.S19 pse 7
```

poe utilization-threshold

Syntax

poe utilization-threshold *utilization-threshold-value* **pse** *pse-id*

undo poe utilization-threshold **pse** *pse-id*

View

System view

Default level

2: System level

Parameters

utilization-threshold-value: Specifies the power alarm threshold in percentage, in the range of 1 to 99.

pse *pse-id*: Specifies a PSE ID.

Description

Use **poe utilization-threshold** to configure a power alarm threshold for the PSE.

Use **undo poe utilization-threshold** to restore the default power alarm threshold of the PSE.

By default, the power alarm threshold for the PSE is 80%.

The system sends a trap message when the power utilization exceeds the alarm threshold. If the power utilization always stays above the alarm threshold, the system does not send any trap message. Instead, when the percentage of the power utilization drops below the alarm threshold, the system sends a trap message again.

Examples

Set the power alarm threshold to 90% for PSE 7.

```
<Sysname> system-view
```

```
[Sysname] poe utilization-threshold 90 pse 7
```

poe-profile

Syntax

poe-profile *profile-name* [*index*]

undo poe-profile { **index** *index* | **name** *profile-name* }

View

System view

Default level

2: System level

Parameters

profile-name: Specifies the name of a PoE configuration file, a string of 1 to 15 characters. A PoE configuration file name begins with a letter (a through z or A through Z) and must not contain reserved keywords such as **undo**, **all**, **name**, **interface**, **user**, **poe**, **disable**, **max-power**, **mode**, **priority** and **enable**.

index: Specifies the index number of a PoE configuration file, in the range of 1 to 100.

Description

Use **poe-profile** *profile-name* to create a PoE configuration file and enter PoE-profile view.

Use **undo poe-profile** to delete the specified PoE configuration file.

If no index is specified, the system automatically assigns an index to the PoE configuration file, starting from 1.

If a PoE configuration file is already applied to a PoE interface, you cannot delete it. To delete the file, execute the **undo apply poe-profile** command to remove the application of the PoE configuration file to the PoE interface.

Examples

Create a PoE configuration file, name it **abc**, and specify the index number as **3**.

```
<Sysname> system-view
```

```
[Sysname] poe-profile abc 3
```

New feature: Supporting automatically creating RSA key pairs or SSH

Feature change description

When an SSH client logs in, the device automatically creates RSA key pairs if no local DSA or RSA key pairs exist.

Command changes

None

Modified feature: SCP server name

Feature change description

Changed the length range for the SCP server name.

Command changes

Modified command: scp

Syntax

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

View

User view

Change description

Before modification: The *server* argument is a string of 1 to 255 case-insensitive characters.

After modification: When the specified SCP server runs IPv4, the *server* argument is a string of 1 to 20 case-insensitive characters. When the specified SCP server runs IPv6, the *server* argument is a string of 1 to 46 case-insensitive characters.

Modified feature: Configuring portal-free rules to support TCP/UDP port numbers

Feature change description

A portal-free rule allows specific users to access external network resources without portal authentication.

Besides the newly added TCP/UDP port numbers, you can also specify IP addresses, MAC address, the interface connecting the client, and VLAN for a portal-free rule. A user packet passing the portal-free rule does not trigger portal authentication, and the user can directly access network resources.

Command changes

Modified command: portal free-rule

Old syntax

```
portal free-rule rule-number { destination { any | ip { ip-address mask { mask-length | netmask } | any } | ipv6 { ipv6-address prefix-length | any } } | source { any | [ interface interface-type interface-number | ip { ip-address mask { mask-length | netmask } | any } | ipv6 { ipv6-address prefix-length | any } | mac mac-address | vlan vlan-id ] * } } *
```

New syntax

```
portal free-rule rule-number { destination { any | ip { ipv4-address mask { mask-length | mask } | any } [ tcp tcp-port-number | udp udp-port-number ] | ipv6 { ipv6-address prefix-length | any } } | source { any | [ interface interface-type interface-number | ip { ipv4-address mask { mask-length | mask } | any } [ tcp tcp-port-number | udp udp-port-number ] | ipv6 { ipv6-address prefix-length | any } | mac mac-address | vlan vlan-id ] * } } *
```

Views

System view

Default command level

2: System level

Change description

Before modification: You cannot specify TCP or UDP port numbers in the portal-free rule.

After modification: You can specify TCP or UDP port numbers in the portal-free rule. If you specify both a source port number and a destination port number for a portal-free rule, the source and destination port numbers must belong to the same transport layer protocol.

Modified feature: Setting the time to wait for a DAD NS from a DHCPv6 client

Feature change description

With SAVI enabled, the default time to wait for a DAD NS from a DHCPv6 client is 1 second. You can use the **ipv6 savi dad-preparedelay value** command to set the waiting time.

Command reference

Modified command: ipv6 savi dad-preparedelay

Old syntax

```
ipv6 savi dad-preparedelay [ value ]
```

New syntax

```
ipv6 savi dad-preparedelay value
```

Views

System view

Change description

Before modification: Argument *value* was optional. If you do not specify this argument, the default time is 0 centisecond.

After modification: Argument *value* is required.

Modified feature: Support of voice VLAN for 128 OUI addresses

Feature change description

The number of OUI addresses that the voice VLAN feature supports was modified from 16 to 128.

Command changes

Modified command: voice vlan mac-address

Syntax

```
voice vlan mac-address mac-address mask oui-mask [ description text ]
```

Views

System view

Change description

Before modification: The command can configure up to 16 OUI addresses.

After modification: The command can configure up to 128 OUI addresses.

Modified feature: Configuring CDP compatibility

Feature change description

When the switch is directly connected to a device that supports only CDP rather than LLDP, you can configure CDP compatibility to enable the switch to exchange information (CDP packets) with the directly-connected device.

[Table 2](#) shows the fields contained in CDP packets sent by the switch, and the **Addresses**, **Capabilities**, **Software Version**, **Platform**, **Duplex**, **MTU**, and **System Name** fields are newly added.

Table 2 Fields in CDP packets

Field	Description
Device ID	Bridge MAC address of the switch.
Addresses	Port IPv4 address. The port IPv4 address is the main IPv4 address of the VLAN interface that is in up state and whose corresponding VLAN ID is the lowest among the VLANs permitted on the port. If none of the VLAN interfaces of the permitted VLANs is assigned an IPv4 address or all VLAN interfaces are down, no port IPv4 address will be advertised.

Field	Description
Port ID	ID of the port connecting to the CDP neighbor.
Capabilities	Capabilities: Switch.
Software Version	Software version running on the switch.
Platform	Switch model.
Duplex	Duplex state of the port.
MTU	Maximum transmission unit.
System Name	System name of the switch.
Native VLAN	Port VLAN ID (PVID).
Voice VLAN	VLAN configured by using the lldp voice-vlan command or voice VLAN configured on the port.

To enable this feature, you only need to enable LLDP and CDP-compatible LLDP. For more information about LLDP and CDP-compatible LLDP, see "LLDP configuration" in *Layer 2—LAN Switching Configuration Guide of HP 5500 HI Switch Series Configuration Guides-Release 5101*.

Command changes

You can use the **display lldp neighbor-information** command to view information about CDP neighbors.

Modified command: display lldp neighbor-information

Syntax

```
display lldp neighbor-information [ brief | interface interface-type interface-number [ brief ] | list
[ system-name system-name ] ] [ { begin | exclude | include } regular-expression ]
```

Views

Any view

Change description

IP address information for CDP neighbors was added to the output.

Display the LLDP information sent from the neighboring devices received through all ports. (This example displays only the information about the CDP neighbor.)

```
<Sysname> display lldp neighbor-information
```

```
...
```

```
CDP neighbor-information of port 2[GigabitEthernet1/0/2]:
```

```
  CDP neighbor index : 2
```

```
  Chassis ID          : C4507
```

```
  Address             : 192.168.1.56
```

```
  Port ID             : GigabitEthernet1/0/1
```

```
  Software version    : Cisco IOS Software, Catalyst 4500 L3 Switch Software
(cat4500-ENTSERVICESK9-M), Version 12.2(31)SGA4, RELEASE SOFTWARE (fc1)
```

```
  Platform            : cisco WS-C4507R
```

```
  Duplex              : Full
```

Table 29 Command output

Field	Description
CDP neighbor-information of port 2	CDP information received through port 2.
CDP neighbor index	Index of the CDP neighboring device.
Chassis ID	Name of the CDP neighboring device.
Address	IPv4 address of the port that connects the CDP neighboring device to the local device. This field is newly added.
Port ID	ID of the port that connects the CDP neighboring device to the local device.
Software version	Software version of the CDP neighboring device.
Platform	Model of the CDP neighboring device.
Duplex	Duplex state of the port that connects the CDP neighboring device to the local device.

Modified feature: ping ipv6

Feature change description

The length of the IPv6 address or host name string that specifies the destination host in the **ping ipv6** command is changed.

Command changes

Modified command: ping ipv6

Syntax

```
ping ipv6 [ -a source-ipv6 | -c count | -m interval | -s packet-size | -t timeout | -tos tos |  
-vpn-instance vpn-instance-name ] * host [ -i interface-type interface-number ]
```

Views

Any view

Change description

The length of the *host* argument is changed from 1 to 46 characters to 1 to 255 characters.

Modified feature: Configuring the maximum number of operations that an NQA client can simultaneously perform

Feature change description

The maximum number of operations that an NQA client can simultaneously perform is modified.

Command reference

Modified command: `nqa agent max-concurrent`

Syntax

nqa agent max-concurrent *number*

Views

System view

Change description

Before modification: The value range for the *number* argument was from 1 to 5.

After modification: The value range for the *number* argument is from 1 to 30.

Modified feature: Configuring parameters for an sFlow collector

Feature change description

The option **vpn-instance** *vpn-instance-name* was added to the **sflow collector** command.

Command reference

Modified command: `sflow collector`

Syntax

sflow collector *collector-id* { [**vpn-instance** *vpn-instance-name*] { **ip** *ip-address* | **ipv6** *ipv6-address* } | **datagram-size** *size* | **description** *text* | **port** *port-number* | **time-out** *seconds* } *

Views

System view

Change description

Added the **vpn-instance** *vpn-instance-name* option.

Modified feature: Configuring load-sharing criteria for a link aggregation group

Feature change description

Added load-sharing criteria of MPLS labels in Layer 2 aggregate interface view.

Added configuration of load-sharing criteria in Layer 3 aggregate interface view.

Command changes

Modified command: link-aggregation load-sharing mode

Old syntax

```
link-aggregation global load-sharing mode { { destination-ip | destination-mac | source-ip | source-mac } * }
```

New syntax

```
link-aggregation global load-sharing mode { { destination-ip | destination-mac | mpls-label1 | mpls-label2 | source-ip | source-mac } * }
```

Old views

Layer 2 aggregate interface view

New views

Layer 2 aggregate interface view, Layer 3 aggregate interface view

Parameters

destination-ip: Performs load sharing in link aggregation groups based on destination IP address.

destination-mac: Performs load sharing in link aggregation groups based on destination MAC address.

mpls-label1: Performs load sharing for MPLS traffic based on Layer 1 label.

mpls-label2: Performs load sharing for MPLS traffic based on Layer 2 label.

source-ip: Performs load sharing in link aggregation groups based on source IP address.

source-mac: Performs load sharing in link aggregation groups based on source MAC address.

Description

In Layer 2 or Layer 3 aggregate interface view, the switch supports the following load sharing criteria and combinations:

- Load-sharing criteria automatically determined based on the packet type
- Source IP address
- Destination IP address
- Source MAC address
- Destination MAC address
- Layer 1 MPLS label
- Destination IP address and source IP address
- Destination MAC address and source MAC address
- Layer 1 MPLS label and Layer 2 MPLS label

Change description

Before modification: Load-sharing criteria for a link aggregation group could be configured only in Layer 2 aggregate interface view, and only the **destination-ip**, **destination-mac**, **source-ip**, and **source-mac** keywords were supported.

After modification: They can be configured in both Layer 2 and Layer 3 aggregate interface views, and support for the **mpls-label1** and **mpls-label2** keywords is added.

Modified feature: Implementing ACL-based IPsec

Feature change description

ACL-based IPsec can be used to protect the data flow between the local device and the peer end of the IPsec tunnel, rather than the forwarded data flow.

IKE-based IPsec tunnel for IPv4 packets configuration example

Network requirements

As shown in [Figure 11](#), configure an IPsec tunnel between Switch A and Switch B to protect data flows between Switch A and Switch B. Configure the tunnel to use the security protocol ESP, the encryption algorithm AES-CBC-128, and the authentication algorithm HMAC-SHA1-96.

Figure 18 Network diagram



Configuration procedure

1. Configure Switch A:

Assign an IP address to VLAN-interface 1.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 2.2.2.1 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

Define an ACL to identify data flows from Switch A to Switch B.

```
[SwitchA] acl number 3101
[SwitchA-acl-adv-3101] rule 0 permit ip source 2.2.2.1 0 destination 2.2.3.1 0
[SwitchA-acl-adv-3101] rule 5 permit ip source 2.2.3.1 0 destination 2.2.2.1 0
[SwitchA-acl-adv-3101] quit
```

Create an IPsec proposal named **tran1**.

```
[SwitchA] ipsec proposal tran1
```

Specify the encapsulation mode as **tunnel**.

```
[SwitchA-ipsec-proposal-tran1] encapsulation-mode tunnel
```

Specify the security protocol as **ESP**.

```
[SwitchA-ipsec-proposal-tran1] transform esp
```

Specify the algorithms for the proposal.

```
[SwitchA-ipsec-proposal-tran1] esp encryption-algorithm aes 128
[SwitchA-ipsec-proposal-tran1] esp authentication-algorithm sha1
[SwitchA-ipsec-proposal-tran1] quit
```

Configure the IKE peer.

```
[SwitchA] ike peer peer
[SwitchA-ike-peer-peer] pre-shared-key Ab12<><>
[SwitchA-ike-peer-peer] remote-address 2.2.3.1
[SwitchA-ike-peer-peer] quit
```

Create an IPsec policy that uses IKE for IPsec SA negotiation.

```
[SwitchA] ipsec policy map1 10 isakmp
```

Apply the IPsec proposal.

```
[SwitchA-ipsec-policy-isakmp-map1-10] proposal tran1
```

Apply the ACL.

```
[SwitchA-ipsec-policy-isakmp-map1-10] security acl 3101
```

Apply the IKE peer.

```
[SwitchA-ipsec-policy-isakmp-map1-10] ike-peer peer
```

```
[SwitchA-ipsec-policy-isakmp-map1-10] quit
```

Apply the IPsec policy group to VLAN-interface 1.

```
[SwitchA] interface vlan-interface 1
```

```
[SwitchA-Vlan-interface1] ipsec policy map1
```

2. Configure Switch B:

Assign an IP address to VLAN-interface 1.

```
<SwitchB> system-view
```

```
[SwitchB] interface vlan-interface 1
```

```
[SwitchB-Vlan-interface1] ip address 2.2.3.1 255.255.255.0
```

```
[SwitchB-Vlan-interface1] quit
```

Define an ACL to identify data flows from Switch B to Switch A.

```
[SwitchB] acl number 3101
```

```
[SwitchB-acl-adv-3101] rule 0 permit ip source 2.2.3.1 0 destination 2.2.2.1 0
```

```
[SwitchB-acl-adv-3101] rule 5 permit ip source 2.2.2.1 0 destination 2.2.3.1 0
```

```
[SwitchB-acl-adv-3101] quit
```

Create an IPsec proposal named **tran1**.

```
[SwitchB] ipsec proposal tran1
```

Specify the encapsulation mode as **tunnel**.

```
[SwitchB-ipsec-proposal-tran1] encapsulation-mode tunnel
```

Specify the security protocol as **ESP**.

```
[SwitchB-ipsec-proposal-tran1] transform esp
```

Specify the algorithms for the proposal.

```
[SwitchB-ipsec-proposal-tran1] esp encryption-algorithm aes 128
```

```
[SwitchB-ipsec-proposal-tran1] esp authentication-algorithm sha1
```

```
[SwitchB-ipsec-proposal-tran1] quit
```

Configure the IKE peer.

```
[SwitchB] ike peer peer
```

```
[SwitchB-ike-peer-peer] pre-shared-key Ab12<><>
```

```
[SwitchB-ike-peer-peer] remote-address 2.2.2.1
```

```
[SwitchB-ike-peer-peer] quit
```

Create an IPsec policy that uses IKE for IPsec SA negotiation.

```
[SwitchB] ipsec policy use1 10 isakmp
```

Apply the ACL.

```
[SwitchB-ipsec-policy-isakmp-use1-10] security acl 3101
```

Apply the IPsec proposal.

```
[SwitchB-ipsec-policy-isakmp-use1-10] proposal tran1
```

Apply the IKE peer.

```
[SwitchB-ipsec-policy-isakmp-use1-10] ike-peer peer
[SwitchB-ipsec-policy-isakmp-use1-10] quit
```

Apply the IPsec policy group to VLAN-interface 1.

```
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ipsec policy use1
```

3. Verifying the configuration

After the previous configuration, send traffic from Switch B to Switch A. Switch A starts IKE negotiation with Switch B when receiving the first packet. If IKE negotiation is successful and SAs are set up, the traffic between the two switches will be IPsec protected.

IKE configuration example

Network requirements

As shown in [Figure 14](#), configure an IPsec tunnel that uses IKE negotiation between Switch A and Switch B to secure the communication between the two switches.

For Switch A, configure an IKE proposal that uses the sequence number 10 and the authentication algorithm SHA1. Configure Switch B to use the default IKE proposal.

Configure the two routers to use the pre-shared key authentication method.

Figure 19 Network diagram



Configuration procedure

1. Make sure Switch A and Switch B can reach each other.
2. Configure Switch A:

Assign an IP address to VLAN-interface 1.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-vlan-interface1] ip address 1.1.1.1 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

Configure ACL 3101 to identify traffic from Switch A to Switch B..

```
[SwitchA] acl number 3101
[SwitchA-acl-adv-3101] rule 0 permit ip source 1.1.1.1 0 destination 2.2.2.2 0
[SwitchA-acl-adv-3101] rule 1 permit ip source 2.2.2.2 0 destination 1.1.1.1 0
[SwitchA-acl-adv-3101] quit
```

Create IPsec proposal tran1.

```
[SwitchA] ipsec proposal tran1
```

Set the packet encapsulation mode to tunnel.

```
[SwitchA-ipsec-proposal-tran1] encapsulation-mode tunnel
```

Use security protocol ESP.

```
[Switch-ipsec-proposal-tran1] transform esp
```

Specify encryption and authentication algorithms.

```
[SwitchA-ipsec-proposal-tran1] esp encryption-algorithm aes 128
```

```

[SwitchA-ipsec-proposal-tran1] esp authentication-algorithm sha1
[SwitchA-ipsec-proposal-tran1] quit
# Create an IKE proposal numbered 10.
[SwitchA] ike proposal 10
# Set the authentication algorithm to SHA1.
[SwitchA-ike-proposal-10] authentication-algorithm sha
# Configure the authentication method as pre-shared key.
[SwitchA-ike-proposal-10] authentication-method pre-share
# Set the ISAKMP SA lifetime to 5000 seconds.
[SwitchA-ike-proposal-10] sa duration 5000
[SwitchA-ike-proposal-10] quit
# Create IKE peer peer.
[SwitchA] ike peer peer
# Configure the IKE peer to reference IKE proposal 10.
[SwitchA-ike-peer-peer] proposal 10
# Set the pre-shared key.
[SwitchA-ike-peer-peer] pre-shared-key Ab12<><>
# Specify the IP address of the peer security gateway.
[SwitchA-ike-peer-peer] remote-address 2.2.2.2
[SwitchA-ike-peer-peer] quit
# Create an IPsec policy that uses IKE negotiation.
[SwitchA] ipsec policy map1 10 isakmp
# Reference IPsec proposal tran1.
[SwitchA-ipsec-policy-isakmp-map1-10] proposal tran1
# Reference ACL 3101 to identify the protected traffic.
[SwitchA-ipsec-policy-isakmp-map1-10] security acl 3101
# Reference IKE peer peer.
[SwitchA-ipsec-policy-isakmp-map1-10] ike-peer peer
[SwitchA-ipsec-policy-isakmp-map1-10] quit
# Apply the IPsec policy to VLAN-interface 1.
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ipsec policy map1

```

3. Configure Switch B:

```

# Assign an IP address to VLAN-interface 1.
<SwitchB> system-view
[SwitchB] interface Vlan-interface1
[SwitchB-Vlan-interface1] ip address 2.2.2.2 255.255.255.0
[SwitchB-Vlan-interface1] quit
# Configure ACL 3101 to identify traffic from Switch B to Switch A.
[SwitchB] acl number 3101
[SwitchB-acl-adv-3101] rule 0 permit ip source 2.2.2.2 0 destination 1.1.1.0 0
[SwitchB-acl-adv-3101] rule 1 permit ip source 1.1.1.1 0 destination 2.2.2.2 0
[SwitchB-acl-adv-3101] quit
# Create IPsec proposal tran1.

```

```

[SwitchB] ipsec proposal tran1

# Set the packet encapsulation mode to tunnel.
[SwitchB-ipsec-proposal-tran1] encapsulation-mode tunnel

# Use security protocol ESP.
[SwitchB-ipsec-proposal-tran1] transform esp

# Specify encryption and authentication algorithms.
[SwitchB-ipsec-proposal-tran1] esp encryption-algorithm aes 128
[SwitchB-ipsec-proposal-tran1] esp authentication-algorithm sha1
[SwitchB-ipsec-proposal-tran1] quit

# Create an IKE proposal numbered 10.
[SwitchB] ike proposal 10

# Set the authentication algorithm to SHA1.
[SwitchB-ike-proposal-10] authentication-algorithm sha

# Configure the authentication method as pre-shared key.
[SwitchB-ike-proposal-10] authentication-method pre-share

# Set the ISAKMP SA lifetime to 5000 seconds.
[SwitchB-ike-proposal-10] sa duration 5000
[SwitchB-ike-proposal-10] quit

# Create IKE peer peer.
[SwitchB] ike peer peer

# Configure the IKE peer to reference IKE proposal 10.
[SwitchB-ike-peer-peer] proposal 10

# Set the pre-shared key.
[SwitchB-ike-peer-peer] pre-shared-key Ab12<><>

# Specify the IP address of the peer security gateway.
[SwitchB-ike-peer-peer] remote-address 1.1.1.1
[SwitchB-ike-peer-peer] quit

# Create an IPsec policy that uses IKE negotiation.
[SwitchB] ipsec policy use1 10 isakmp

# Reference IPsec proposal tran1.
[SwitchB-ipsec-policy-isakmp-use1-10] proposal tran1

# Reference ACL 3101 to identify the protected traffic.
[SwitchB-ipsec-policy-isakmp-use1-10] security acl 3101

# Reference IKE peer peer.
[SwitchB-ipsec-policy-isakmp-use1-10] ike-peer peer
[SwitchB-ipsec-policy-isakmp-use1-10] quit

# Apply the IPsec policy to VLAN-interface 1.
[SwitchB-Vlan-interface1] ipsec policy use1

```

Verifying the configuration

After the above configuration, send traffic from Switch B to Switch A. Switch A starts IKE negotiation with Switch B when receiving the first packet. IKE proposal matching starts with the one having the highest priority. During the matching process, lifetime is not involved but it is determined by the IKE negotiation parties.

Command changes

None

Modified feature: Setting the IRF link down report delay

Feature change description

Changed the value range and default value of the *interval* argument.

Command changes

Modified command: `irf link-delay`

Syntax

`irf link-delay` *interval*

Views

System view

Change description

Before modification: The value range (in milliseconds) for the *interval* argument is 200 to 2000. By default, IRF link down events are immediately reported to the upper layer.

After modification: The value range (in milliseconds) for the *interval* argument is 0 to 30000. By default, IRF link down events are reported 4 seconds later after their occurrence.

Modified feature: Configuring the ABR to advertise a default route to the stub area

Feature change description

In the previous releases, before advertising a default route in a Type-3 LSA to the stub area, the ABR is required to check whether FULL-state neighbors exist in the backbone area.

In this release, you can disable the checking by executing the command.

Command changes

Modified command: `stub`

Old syntax

`stub` [**`no-summary`**]

New syntax

`stub` [**`no-summary`** | **`default-route-advertise-always`**] *

Views

OSPF area view

Change description

Before modification: The ABR is required to check whether FULL-state neighbors exist in the backbone area before advertising a default route in a Type-3 LSA to the stub area.

After modification: With the newly added **default-route-advertise-always** keyword, the ABR advertises a default route in a Type-3 LSA into the stub area regardless of whether FULL-state neighbors exist in the backbone area. This is available only when the ABR interfaces in the backbone area are in upstate.

R5105

This chapter includes following contents:

- New feature: Disabling password recovery capacity
- New feature: Configuring a port to forward 802.1X EAPOL packets untagged
- New feature: Configuring preferred tunnels in a tunneling policy
- Modified feature: Configuring NDP globally and for specific ports
- Modified feature: Configuring NTDP globally and for specific ports
- Modified feature: Configuring the cluster function
- Modified feature: Default configuration

New feature: Disabling password recovery capacity

Disabling password recovery capacity

Password recovery capability controls console user access to the device configuration and SDRAM from BootROM menus.

If password recovery capability is enabled, a console user can access the device configuration without authentication and reconfigure the console login password and user privilege level passwords.

If password recovery capability is disabled, a console user must restore the factory-default configuration before configuring new passwords. Restoring the factory-default configuration deletes the next-startup configuration files.

To enhance system security:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Disable password recovery capacity.	undo password-recovery enable	By default, password recovery capability is enabled.

For more information about BootROM menus and password recovery capacity, see appendix B in *HP 5500HI-CMW520-R5105 Release Notes Release Notes*.

Command reference

password-recovery enable

Syntax

password-recovery enable

undo password-recovery enable

View

System view

Default level

3: Manage level

Description

Use **password-recovery enable** to enable password recovery capability.

Use **undo password-recovery enable** to disable password recovery capability.

By default, password recovery capability is enabled.

To enhance system security, disable password recovery capability.

Examples

Disable password recovery capability.

```
<Sysname> system-view
```

```
[Sysname] undo password-recovery enable
```

New feature: Configuring a port to forward 802.1X EAPOL packets untagged

Configuring a port to forward 802.1X EAPOL packets untagged

After an 802.1X user passes authentication, the 802.1X server assigns authorization attributes to the access device. If the port is assigned to a VLAN as a tagged member, the port that connects the clients forwards packets tagged. 802.1X defines EAP over LAN (EAPOL) for passing EAP packets between the client and the network access device over a wired or wireless LAN. An EAPOL-format 802.1X packet cannot carry any VLAN tag in its header. To ensure the communication between the client and the network access device, you can configure the port that connects the client and the network access device to forward 802.1X EAPOL packets after removing the tag.

To configure a port to forward 802.1X EAPOL packets untagged:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the port to forward 802.1X EAPOL packets untagged.	dot1x eapol untag	Optional. By default, whether the port forwards 802.1X EAPOL packets with the VLAN tag depends on the port configuration and the server-assigned VLAN setting.

NOTE:

- An access port cannot be a tagged member of any VLAN.
- The device does not change the PVID of a hybrid or trunk port when the port is assigned to the VLAN as a tagged member.

Command reference

dot1x eapol untag

Syntax

dot1x eapol untag

undo dot1x eapol untag

View

Layer 2 Ethernet interface view

Default level

3: Manage level

Description

Use **dot1x eapol untag** to configure a port to forward 802.1X EAPOL packets untagged.

By default, whether the port forwards 802.1X EAPOL packets with the VLAN tag depends on the port configuration and the server-assigned VLAN setting.

Examples

Configure GigabitEthernet 1/0/1 to forward 802.1X EAPOL packets untagged.

```
<Sysname> system-view
[Sysname]interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x eapol untag
```

New feature: Configuring preferred tunnels in a tunneling policy

Configuring preferred tunnels in a tunneling policy

When multiple tunnels exist in an MPLS L3VPN network, you can configure a tunneling policy to specify the type and number of tunnels to be used by using the **tunnel select-seq** command or the **preferred-path** command.

With the **preferred-path** command, you can configure preferred tunnels that each correspond to a tunnel interface.

After a tunneling policy is applied on a PE, the PE selects tunnels in this order:

- The PE matches the peer PE address against the destination addresses of preferred tunnels, starting from the tunnel with the smallest number. If no match is found, the local PE selects tunnels as configured by the **tunnel select-seq** command or the default tunneling policy if the **tunnel select-seq** command is not configured. The default tunneling policy selects only one tunnel (no load balancing) in this order: LSP tunnel, CR-LSP tunnel.
- If a matching tunnel is found and the tunnel is available, the local PE stops matching other tunnels and forwards the traffic to the specified tunnel interface.
- If the matching tunnel is unavailable (for example, the tunnel is down or the tunnel's ACL does not permit the traffic) and is not specified with the **disable-fallback** keyword, the local PE continues to match other tunnels. If the tunnel is specified with the **disable-fallback** keyword, the local PE stops matching and tunnel selection fails.

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a tunneling policy and enter tunneling policy view.	tunnel-policy <i>tunnel-policy-name</i>	N/A
3. Configure a preferred tunnel and specify a tunnel interface for it.	preferred-path <i>number</i> interface tunnel <i>tunnel-number</i> [disable-fallback]	Optional. By default, no preferred tunnel is configured.

Command reference

preferred-path

Use **preferred-path interface tunnel** to configure a preferred tunnel and specify a tunnel interface for it.

Use **undo preferred-path** to remove a preferred tunnel.

Syntax

preferred-path *number* **interface tunnel** *tunnel-number* [**disable-fallback**]

undo preferred-path *number*

Default

No preferred tunnel exists.

Views

Tunneling policy view

Default command level

2: System view

Parameters

number: Specifies the number of the preferred tunnel, in the range of 0 to 63. A smaller number means a higher priority.

interface tunnel *tunnel-number*: Specifies a tunnel interface for the preferred tunnel. The *tunnel-number* argument represents the tunnel interface number. The value range for the *tunnel-number* argument is from 0 to 127.

disable-fallback: With this keyword specified, the tunneling policy does not select other paths when this preferred tunnel is matched (the tunnel's destination address and encapsulation type are both matched) but is unavailable.

Usage guidelines

In a tunneling policy, you can configure up to 64 preferred tunnels.

The tunnel interfaces specified for preferred tunnels can have the same destination address and the tunnel encapsulation type must be MPLS TE.

Examples

Tunnel interfaces Tunnel 0, Tunnel 2, and Tunnel 3 have the same destination address 1.1.1.1. Configure a tunneling policy **po1** for the device, so that the device selects tunnels for traffic destined for 1.1.1.1 in this order: Tunnel 0, Tunnel 2, Tunnel 3. If all three tunnels are unavailable, tunnel selection is stopped and traffic destined for 1.1.1.1 cannot be transmitted. For traffic going to other destinations, the device selects tunnels by type and only one CR-LSP tunnel can be selected.

```
<Sysname> system-view
[Sysname] tunnel-policy po1
[Sysname-tunnel-policy-po1] preferred-path 0 interface tunnel 0
[Sysname-tunnel-policy-po1] preferred-path 2 interface tunnel 2
[Sysname-tunnel-policy-po1] preferred-path 3 interface tunnel 3 disable-fallback
[Sysname-tunnel-policy-po1] tunnel select-seq cr-lsp load-balance-number 1
```

Modified feature: Configuring NDP globally and for specific ports

Feature change description

NDP is now disabled globally and for specific ports by default.

Command changes

Modified command: `ndp enable`

Syntax

In Layer 2 Ethernet port view or Layer 2 aggregate interface view:

`ndp enable`

`undo ndp enable`

In system view:

`ndp enable [interface interface-list]`

`undo ndp enable [interface interface-list]`

Views

System view, Layer 2 Ethernet port view, Layer 2 aggregate interface view

Change description

Before modification: NDP is enabled globally and for specific ports by default.

After modification: NDP is disabled globally and for specific ports by default.

Modified feature: Configuring NTDP globally and for specific ports

Feature change description

NTDP is now disabled globally and for specific ports by default.

Command changes

Modified command: `ntdp enable`

Syntax

`ntdp enable`

`undo ntdp enable`

Views

System view, Layer 2 Ethernet port view, Layer 2 aggregate interface view

Change description

Before modification: NTDP is enabled globally and for specific ports by default.

After modification: NTDP is disabled globally and for specific ports by default.

Modified feature: Configuring the cluster function

Feature change description

The cluster function is now disabled by default.

Command changes

Modified command: cluster enable

Syntax

cluster enable

undo cluster enable

Views

System view

Change description

Before modification: The cluster function is enabled by default.

After modification: The cluster function is disabled by default.

Modified feature: Default configuration

Feature change description

The following changes are made to the default configuration in this release:

- The **telnet server enable** command is deleted and Telnet service is disabled.
- The **interface vlan-interface1** command is deleted and VLAN-interface 1 does not exist.
- The **ip address dhcp-alloc client-identifier mac vlan-interface1** command is deleted and VLAN-interface 1 does not apply for an IP address.
- The **undo ip http enable** command is added and HTTP service is disabled.
- The **undo cwmp enable** command is added and CWMP service is disabled.
- Deleted the default RADIUS scheme system, which included the following commands: **radius scheme system**, **server-type extended**, **primary authentication** 127.0.0.1 1645, **primary accounting** 127.0.0.1 1646, and **user-name-format without-domain**.

The default configuration takes effect only when the switch starts up with no specific configuration file. Once you specify a specific startup configuration file for the switch, the switch uses the specific configuration file instead of the default configuration.

Command changes

None

F5103

This release has the following changes:

- New feature: Delaying the MAC authentication
- New feature: Specifying the source interface for DNS packets
- New feature: Configuring DHCPv6 snooping to support Option 18 and Option 37
- New feature: Setting the subnet mask length to be 31
- New feature: Setting the DSCP value for multiple types of protocol packets
- New feature: Automatic configuration file backup for software downgrading
- New feature: Configuring LLDP to advertise a specific voice VLAN
- New feature: Enabling LLDP to automatically discover IP phones
- New feature: MVRP
- New feature: Portal authentication in IPv6 networks
- New feature: SCP
- New feature: FIPS
- New feature: Configuring ACL-based IPsec
- New feature: IKE
- New feature: Configuring the log file overwrite-protection function
- New feature: Verifying the correctness and integrity of the file
- New feature: Displaying per-port queue-based traffic statistics
- Modified feature: Configuring MAC authentication timers
- Modified feature: NTP
- Modified feature: Configuring a password for the local user
- Modified feature: 802.1X critical VLAN
- Modified feature: MAC authentication critical VLAN
- Modified feature: Modifying CLI configuration commands executed in FIPS mode for CC evaluation
- Modified feature: Modifying login management commands executed in FIPS mode for CC evaluation
- Modified Feature: Modifying software upgrade commands executed in FIPS mode for CC evaluation
- Modified Feature: Modifying configuration file management commands executed in FIPS mode for CC evaluation
- Modified Feature: Modifying security commands executed in FIPS mode for CC evaluation
- Modified feature: Modifying SNMP commands executed in FIPS mode for CC evaluation
- Modified feature: Clearing all users from the password control blacklist
- Modified feature: Setting the interval for saving system information to the log file

New feature: Delaying the MAC authentication

When both 802.1X authentication and MAC authentication are enabled on a port, you can delay the MAC authentication, so that 802.1X authentication is preferentially triggered. Configure the function as needed according to the network conditions.

Configuring the MAC authentication delay

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the MAC authentication delay.	mac-authentication timer auth-delay <i>time</i>	By default, MAC authentication is not delayed.

Command reference

mac-authentication timer auth-delay

Use **mac-authentication timer auth-delay** to configure the MAC authentication delay.

Use **undo mac-authentication timer auth-delay** to restore the default.

Syntax

mac-authentication timer auth-delay *time*

undo mac-authentication timer auth-delay

Default

MAC authentication is not delayed.

Views

Layer 2 Ethernet port view

Default command level

2: System level

Parameters

time: Specifies the MAC authentication delay, which ranges from 1 to 180 seconds.

Examples

Set the MAC authentication delay to 30 seconds on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitEthernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] mac-authentication timer auth-delay 30
```

New feature: Specifying the source interface for DNS packets

Specifying the source interface for DNS packets

By default, the device uses the primary IP address of the output interface of the matching route as the source IP address of a DNS request. Therefore, the source IP address of the DNS packets may vary with DNS servers. In some scenarios, the DNS server only responds to DNS requests sourced from a specific IP address. In such cases, specify the source interface for the DNS packets so that

the device can always use the primary IP address of the specified source interface as the source IP address of DNS packets.

To specify the source interface for DNS packets:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Specify the source interface for DNS packets.	dns source-interface <i>interface-type interface-number</i>	By default, no source interface for DNS packets is specified. The device looks up its routing table for an output interface for a DNS request destined for a DNS server and uses the primary IP address of the interface as the source IP address of the packet.

Command reference

dns source-interface

Use **dns source-interface** to specify the source interface for DNS packets.

Use **undo dns source-interface** to restore the default.

Syntax

dns source-interface *interface-type interface-number*

undo dns source-interface

Default

No source interface for DNS packets is specified. The device uses the primary IP address of the output interface of the matching route as the source IP address of a DNS request.

Views

System view

Default command level

2. System level

Parameters

interface-type interface-number: Specifies the interface type and number.

Usage guidelines

The device uses the primary IP address of the specified source interface as the source IP address of a DNS request, which however is still forwarded through the output interface of the matching route.

Examples

Specify VLAN-interface 2 as the source interface of DNS requests.

```
<Sysname> system-view
```

```
[Sysname] dns source-interface vlan-interface2
```

New feature: Configuring DHCPv6 snooping to support Option 18 and Option 37

Configuring DHCPv6 snooping to support Option 18 and Option 37

Option 18 is the Interface ID option and Option 37 is the Remote ID option. Upon receiving a DHCPv6 request, the DHCPv6 snooping device adds Option 18 or Option 37 into the request message before forwarding it to the DHCPv6 server.

Figure 1 Option 18 format

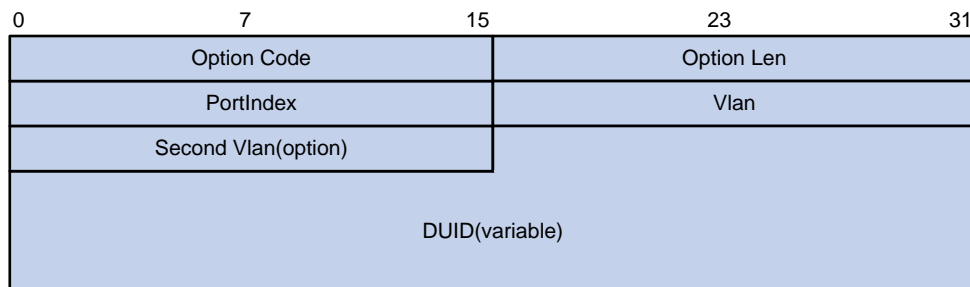
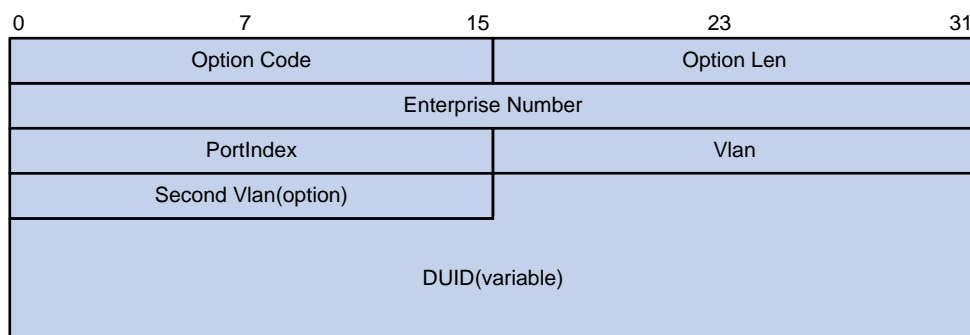


Figure 2 Option 37 format



The Second Vlan field is optional. If the received DHCPv6 request does not contain a second VLAN, Option 18 or Option 37 also does not contain it.

To configure DHCPv6 Snooping to support Option 18 and Option 37:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable DHCPv6 Snooping globally.	ipv6 dhcp snooping enable	By default, this function is disabled.
3. Enter VLAN view.	vlan <i>vlan-id</i>	N/A
4. Enable DHCPv6 snooping in the VLAN.	ipv6 dhcp snooping vlan enable	By default, this function is disabled.
5. Enter Layer 2 Ethernet port view or Layer 2 aggregate interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
6. Enable DHCPv6 snooping to support Option 18.	ipv6 dhcp snooping option interface-id enable	By default, DHCPv6 snooping does not support Option 18.

Step	Command	Remarks
7. Configure the DUID in Option 18.	ipv6 dhcp snooping option interface-id string <i>interface-id</i>	Optional. By default, the DUID in Option 18 is the DUID of the device.
8. Enable DHCPv6 snooping to support Option 37.	ipv6 dhcp snooping option remote-id enable	By default, DHCPv6 snooping does not support Option 37.
9. Configure the DUID in Option 37.	ipv6 dhcp snooping option remote-id string <i>remote-id</i>	Optional. By default, the DUID in Option 37 is the DUID of the device.

Command reference

ipv6 dhcp snooping option interface-id enable

Use **ipv6 dhcp snooping option interface-id enable** to enable DHCPv6 snooping support for Option 18.

Use **undo ipv6 dhcp snooping option interface-id enable** to restore the default.

Syntax

ipv6 dhcp snooping option interface-id enable

undo ipv6 dhcp snooping option interface-id enable

Default

By default, DHCPv6 snooping support for Option 18 is disabled.

Views

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default command level

2: System level

Usage guidelines

The **ipv6 dhcp snooping option interface-id enable** command is effective only when you enable DHCPv6 snooping globally in system view, and enable DHCPv6 snooping in VLAN view.

Examples

Enable DHCPv6 snooping support for Option 18.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping enable
[Sysname] vlan 1
[Sysname-vlan1] ipv6 dhcp snooping vlan enable
[Sysname-vlan1] quit
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet 1/0/1] ipv6 dhcp snooping option interface-id enable
```

ipv6 dhcp snooping option interface-id string

Use **ipv6 dhcp snooping option interface-id string** to configure the DUID in Option 18.

Use **undo ipv6 dhcp snooping option interface-id string** to restore the default.

Syntax

ipv6 dhcp snooping option interface-id string *interface-id*
undo ipv6 dhcp snooping option interface-id string

Default

The DUID in Option 18 is the DUID of the device.

Views

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default command level

2: System level

Parameters

interface-id: Specifies the DUID in user-defined Option 18, a string of 1 to 128 characters.

Examples

Specify company001 as the DUID in Option 18.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping enable
[Sysname] vlan 1
[Sysname-vlan1] ipv6 dhcp snooping vlan enable
[Sysname-vlan1] quit
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option interface-id enable
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option interface-id string company001
```

ipv6 dhcp snooping option remote-id enable

Use **ipv6 dhcp snooping option remote-id enable** to enable DHCPv6 snooping support for Option 37.

Use **undo ipv6 dhcp snooping option remote-id enable** to restore the default.

Syntax

ipv6 dhcp snooping option remote-id enable
undo ipv6 dhcp snooping option remote-id enable

Default

DHCPv6 snooping support for Option 37 is disabled.

Views

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default command level

2: System level

Usage guidelines

This command is effective only when you enable DHCPv6 snooping globally in system view, and enable DHCPv6 snooping in VLAN view.

Examples

Enable DHCPv6 snooping support for Option 37.

```
<Sysname> system-view
```

```
[Sysname] ipv6 dhcp snooping enable
[Sysname] vlan 1
[Sysname-vlan1] ipv6 dhcp snooping vlan enable
[Sysname-vlan1] quit
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option remote-id enable
```

ipv6 dhcp snooping option remote-id string

Use **ipv6 dhcp snooping option remote-id string** to configure the DUID in Option 37.

Use **undo ipv6 dhcp snooping option remote-id string** to restore the default.

Syntax

ipv6 dhcp snooping option remote-id string *remote-id*

undo ipv6 dhcp snooping option remote-id string

Default

The DUID in Option 37 is the DUID of the device.

Views

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default command level

2: System level

Parameters

string: Specifies the DUID value in user-defined Option 37, a string of 1 to 128 characters.

Examples

Specify device001 as the DUID in Option 37.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping enable
[Sysname] vlan 1
[Sysname-vlan1] ipv6 dhcp snooping vlan enable
[Sysname-vlan1] quit
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option remote-id enable
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option remote-id string device001
```

Examples

Configure Ethernet interface GigabitEthernet 1/0/1 as a trusted port.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping trust
```

New feature: Setting the subnet mask length to be 31

Setting the subnet mask length to be 31

The switch supports the subnet mask length of IP address to be 31 (or supports the subnet mask to be 255.255.255.254) to meet the usage requirement of saving IP addresses in the point-to-point communication.

Command reference

Modified command: ip address

Syntax

```
ip address ip-address { mask-length | mask } [ sub ]
```

views

Interface view

Change description

Before modification: The value of the *mask-length* argument cannot be 31. The value of the *mask* argument cannot be 255.255.255.254.

After modification: The value of the *mask-length* argument can be 31. The value of the *mask* argument can be 255.255.255.254.

New feature: Setting the DSCP value for multiple types of protocol packets

A field in an IPv4 or IPv6 header contains 8 bits and is used to identify the service type of an IP packet. In an IPv4 packet, this field is called "Type of Service (ToS)." In an IPv6 packet, this field is called "Traffic class." According to RFC 2474, the ToS field is redefined as the differentiated services (DS) field, where a DSCP value is represented by the first six bits (0 to 5) and is in the range 0 to 63. The remaining two bits (6 and 7) are reserved. When a packet is being transmitted, the network devices can identify its DSCP value, and determines the transmission priority of the packet according to the DSCP value.

This release allows you to set the DSCP value for multiple types of protocol packets, including VRRP, RADIUS, SSH, HTTP, Telnet, FTP, TFTP, IGMP, MLD, PIM, IPv6 PIM, NTP, NQA, SNMP, ICMP, IGMP Snooping, MLD Snooping, DHCP, DNS, IPv6 DNS, DHCPv6, RIP, OSPF, BGP, and IPv6 BGP.

When you configure the DSCP value for some types of protocol packets, you should specify the ToS field value rather than the DSCP value. Because the DSCP field is the first 6 bits of the ToS field, each four continuous ToS field values, starting from 0, correspond to one DSCP value. An easier way to convert the DSCP value to the ToS value is to multiply the expected DSCP value by four to get the ToS field value.

Setting the DSCP value for BGP protocol packets

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Enter BGP view.	<ul style="list-style-type: none"> Enter BGP view: bgp <i>as-number</i> Enter BGP-VPN instance view: <ul style="list-style-type: none"> bgp <i>as-number</i> ipv4-family vpn-instance <i>vpn-instance-name</i> 	Use either approach.
3. Set the DSCP value for BGP protocol packets sent to the specified BGP peer or BGP peer group.	peer { <i>group-name</i> <i>ip-address</i> } dscp <i>dscp-value</i>	Optional. By default, the DSCP value in BGP protocol packets is 48.

Setting the DSCP value for DHCPv6 protocol packets

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the DSCP value for DHCPv6 protocol packets sent by the DHCPv6 servers and DHCPv6 relay agents.	ipv6 dhcp dscp <i>dscp-value</i>	Optional. By default, the DSCP value in DHCPv6 protocol packets sent by the DHCPv6 servers and DHCPv6 relay agents is 56.
3. Set the DSCP value for DHCPv6 protocol packets sent by the DHCPv6 clients.	ipv6 dhcp client dscp <i>dscp-value</i>	Optional. By default, the DSCP value in DHCPv6 protocol packets sent by the DHCPv6 clients is 56.

Setting the DSCP value for DHCP protocol packets

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the DSCP value for DHCP protocol packets sent by the DHCP servers and DHCP relay agents.	dhcp dscp <i>dscp-value</i>	Optional. By default, the DSCP value in DHCP protocol packets sent by the DHCP servers and DHCP relay agents is 56.
3. Set the DSCP value for DHCP protocol packets sent by the DHCP clients.	dhcp client dscp <i>dscp-value</i>	Optional. By default, the DSCP value in DHCP protocol packets sent by the DHCP clients is 56.

Setting the DSCP value for DNS protocol packets

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the DSCP value for DNS protocol packets transmitted.	dns dscp <i>dscp-value</i>	Optional. By default, the DSCP value in DNS protocol packets transmitted is 0.

Setting the DSCP value for FTP and TFTP protocol packets

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the DSCP value for IPv4 protocol packets sent by the FTP clients.	ftp client dscp <i>dscp-value</i>	Optional. By default, the DSCP value in IPv4 protocol packets sent by the FTP clients is 0.
3. Set the DSCP value for IPv6 protocol packets sent by the FTP clients.	ftp client ipv6 dscp <i>dscp-value</i>	Optional. By default, the DSCP value in IPv6 protocol packets sent by the FTP clients is 0.
4. Set the DSCP value for IPv4 protocol packets sent by FTP servers.	ftp server dscp <i>dscp-value</i>	Optional. By default, the DSCP value in IPv4 protocol packets sent by the FTP servers is 0.
5. Set the DSCP value for IPv4 protocol packets sent by the TFTP clients.	tftp client dscp <i>dscp-value</i>	Optional. By default, the DSCP value in IPv4 protocol packets sent by the TFTP clients is 0.
6. Set the DSCP value for IPv6 protocol packets sent by the TFTP clients.	tftp client ipv6 dscp <i>dscp-value</i>	Optional. By default, the DSCP value in IPv6 protocol packets sent by the TFTP clients is 0.

Setting the DSCP value for HTTP protocol packets

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the DSCP value for IPv4 HTTP protocol packets transmitted.	ip http dscp <i>dscp-value</i>	Optional. By default, the DSCP value in IPv4 HTTP protocol packets transmitted is 16.
3. Set the DSCP value for IPv6 HTTP protocol packets transmitted.	ipv6 http dscp <i>dscp-value</i>	Optional. By default, the DSCP value in IPv6 HTTP protocol packets transmitted is 0.

Setting the DSCP value for IGMP protocol packets sent by IGMP snooping

This configuration allows you to set the DSCP value for IGMP protocol packets sent by IGMP snooping.

To set the DSCP value for IGMP protocol packets transmitted:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IGMP-snooping view.	igmp-snooping	N/A
3. Set the DSCP value for IGMP protocol packets transmitted.	dscp <i>dscp-value</i>	By default, the DSCP value in IGMP protocol packets transmitted is 48.

Setting the DSCP value for IGMP protocol packets

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network IGMP view or VPN instance IGMP view.	igmp [<i>vpn-instance vpn-instance-name</i>]	N/A
3. Set the DSCP value for IGMP protocol packets.	dscp <i>dscp-value</i>	Optional. By default, the DSCP value in IGMP protocol packets is 48.

Setting the DSCP value for IPv6 BGP protocol packets

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enter IPv6 address family view.	ipv6-family	N/A
4. Set the DSCP value for IPv6 BGP protocol packets sent to the specified IPv6 BGP peer or IPv6 BGP peer group.	peer { <i>ipv6-group-name</i> <i>ipv6-address</i> } dscp <i>dscp-value</i>	Optional. By default, the DSCP value in IPv6 BGP protocol packets is 48.

Setting the DSCP value for IPv6 DNS protocol packets

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Set the DSCP value for IPv6 DNS protocol packets transmitted.	dns ipv6 dscp <i>dscp-value</i>	Optional. By default, the DSCP value in IPv6 DNS protocol packets transmitted is 0.

Setting the DSCP value for IPv6 PIM protocol packets

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Set the DSCP value for IPv6 PIM protocol packets.	dscp <i>dscp-value</i>	Optional. By default, the DSCP value in IPv6 PIM protocol packets is 48.

Setting the DSCP value for MLD protocol packets sent by MLD snooping

This configuration allows you to set the DSCP value for MLD protocol packets sent by MLD snooping.

To set the DSCP value for MLD protocol packets transmitted:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter MLD-snooping view.	mld-snooping	N/A
3. Set the DSCP value for MLD protocol packets transmitted.	dscp <i>dscp-value</i>	By default, the DSCP value in MLD protocol packets transmitted is 48.

Setting the DSCP value for MLD protocol packets

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter MLD view.	mld	N/A
3. Set the DSCP value for MLD protocol packets.	dscp <i>dscp-value</i>	Optional. By default, the DSCP value in MLD protocol packets is 48.

Setting the ToS value for packets sent by the TCP listening service on the NQA server

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the ToS value for packets sent by the TCP listening service on the NQA server.	nqa server tcp-connect tos <i>tos</i>	Optional. By default, the ToS value in the packets sent by the TCP listening service on the NQA server is 0.

Setting the ToS value for packets sent by the UDP listening service on the NQA server

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the ToS value for packets sent by the UDP listening service on the NQA server.	nqa server udp-echo tos <i>tos</i>	Optional. By default, the ToS value in the packets sent by the UDP listening service on the NQA server is 0.

Setting the ToS value for NQA probe packets

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter NQA operation view.	nqa entry <i>admin-name</i> <i>operation-tag</i>	N/A
3. Specify the DHCP type and enter its view.	type dhcp	N/A
4. Set the ToS value for NQA probe packets.	tos <i>value</i>	Optional. By default, the ToS value in NQA probe packets is 0.

Setting the DSCP value for NTP protocol packets

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the DSCP value for NTP protocol packets.	ntp-service dscp <i>dscp-value</i>	Optional. By default, the DSCP value in NTP protocol packets is 16.

Setting the DSCP value for OSPF protocol packets

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Enable an OSPF process.	ospf [<i>process-id</i> router-id <i>router-id</i> vpn-instance <i>vpn-instance-name</i>] *	By default, no OSPF process is enabled.
3. Set the DSCP value for OSPF protocol packets.	dscp <i>dscp-value</i>	Optional. By default, the DSCP value in OSPF protocol packets is 48.

Setting the DSCP value for PIM protocol packets

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network IGMP view or VPN instance PIM view.	pim [vpn-instance <i>vpn-instance-name</i>]	N/A
3. Set the DSCP value for PIM protocol packets.	dscp <i>dscp-value</i>	Optional. By default, the DSCP value in PIM protocol packets is 48.

Setting the DSCP value for RADIUS protocol packets

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the DSCP value for IPv4 RADIUS protocol packets.	radius dscp <i>dscp-value</i>	Optional. By default, the DSCP value in IPv4 RADIUS protocol packets is 0.
3. Set the DSCP value for IPv6 RADIUS protocol packets.	radius ipv6 dscp <i>dscp-value</i>	Optional. By default, the DSCP value in IPv6 RADIUS protocol packets is 0.

Setting the DSCP value for RIP protocol packets

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a RIP process and enter RIP view.	rip [<i>process-id</i>] [vpn-instance <i>vpn-instance-name</i>]	By default, no RIP process runs.
3. Set the DSCP value for RIP protocol packets.	dscp <i>dscp-value</i>	Optional. By default, the DSCP value in RIP protocol packets is 48.

Setting the DSCP value for SNMP trap packets

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the DSCP value for SNMP trap packets.	snmp-agent target-host trap address udp-domain { <i>ip-address</i> ipv6 <i>ipv6-address</i> } [udp-port <i>port-number</i>] [dscp <i>dscp-value</i>] [vpn-instance <i>vpn-instance-name</i>] params securityname <i>security-string</i> [v1 v2c v3 [authentication privacy]]	Optional. By default, the DSCP value in SNMP trap packets is 0.

Setting the DSCP value for SNMP response packets

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the DSCP value for SNMP response packets.	snmp-agent packet response dscp <i>dscp-value</i>	Optional. By default, the DSCP value in SNMP response packets is 0.

Setting the DSCP value for SSH protocol packets

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the DSCP value for protocol packets sent by the IPv4 SSH servers.	ssh server dscp <i>dscp-value</i>	Optional. By default, the DSCP value in protocol packets sent by the IPv4 SSH servers is 16.
3. Set the DSCP value for protocol packets sent by the IPv6 SSH servers.	ssh server ipv6 dscp <i>dscp-value</i>	Optional. By default, the DSCP value in protocol packets sent by the IPv6 SSH servers is 0.
4. Set the DSCP value for protocol packets sent by the IPv4 SSH clients.	ssh client dscp <i>dscp-value</i>	Optional. By default, the DSCP value in protocol packets sent by the IPv4 SSH clients is 16.
5. Set the DSCP value for protocol packets sent by the IPv6 SSH clients.	ssh client ipv6 dscp <i>dscp-value</i>	Optional. By default, the DSCP value in protocol packets sent by the IPv6 SSH clients is 0.
6. Set the DSCP value for protocol packets sent by the IPv4 SFTP clients.	sftp client dscp <i>dscp-value</i>	Optional. By default, the DSCP value in protocol packets sent by the IPv4 SFTP clients is 16.

Step	Command	Remarks
7. Set the DSCP value for protocol packets sent by the IPv6 SFTP clients.	sftp client ipv6 dscp <i>dscp-value</i>	Optional. By default, the DSCP value in protocol packets sent by the IPv6 SFTP clients is 8.

Setting the DSCP value for Telnet protocol packets

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the DSCP value for protocol packets sent by the IPv4 Telnet clients.	telnet client dscp <i>dscp-value</i>	Optional. By default, the DSCP value in protocol packets sent by the IPv4 Telnet clients is 16.
3. Set the DSCP value for protocol packets sent by the IPv6 Telnet clients.	telnet client ipv6 dscp <i>dscp-value</i>	Optional. By default, the DSCP value in protocol packets sent by the IPv6 Telnet clients is 0.
4. Set the DSCP value for protocol packets sent by the IPv4 Telnet servers.	telnet server dscp <i>dscp-value</i>	Optional. By default, the DSCP value in protocol packets sent by the IPv4 Telnet servers is 48.
5. Set the DSCP value for protocol packets sent by the IPv6 Telnet servers.	telnet server ipv6 dscp <i>dscp-value</i>	Optional. By default, the DSCP value in protocol packets sent by the IPv6 Telnet servers is 0.

Setting the DSCP value for VRRP protocol packets

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the DSCP value for IPv4 VRRP protocol packets.	vrrp dscp <i>dscp-value</i>	Optional. By default, the DSCP value in IPv4 VRRP protocol packets is 48.
3. Set the DSCP value for IPv6 VRRP protocol packets.	vrrp ipv6 dscp <i>dscp-value</i>	Optional. By default, the DSCP value in IPv6 VRRP protocol packets is 56.

Setting the DSCP value for the protocol packets sent to the log host

To set the DSCP value for the protocol packets sent to the log host:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the DSCP value for the protocol packets sent to the log host.	info-center loghost [vpn-instance <i>vpn-instance-name</i>] { <i>host-ipv4-address</i> ipv6 <i>host-ipv6-address</i> } [port <i>port-number</i>] [dscp <i>dscp-value</i>] [channel { <i>channel-number</i> <i>channel-name</i> } facility <i>local-number</i>] *	Optional. By default, the DSCP value in the protocol packets sent to the log host is 0.

Setting the DSCP value for outgoing LDP packets

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter MPLS LDP view.	mpls ldp	N/A
3. Set the DSCP value for outgoing LDP packets.	dscp <i>dscp-value</i>	The default value is 48.

Setting the DSCP value for outgoing RSVP packets

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter MPLS view.	mpls	N/A
3. Set the DSCP value for outgoing RSVP packets.	mpls rsvp-te dscp <i>dscp-value</i>	The default value is 48.

New commands

dhcp client dscp

Use **dhcp client dscp** to set the DSCP value for DHCP protocol packets sent by the DHCP clients.

Use **undo dhcp client dscp** to restore the default.

Syntax

dhcp client dscp *dscp-value*

undo dhcp client dscp

Default

The DSCP value in DHCP protocol packets sent by the DHCP clients is 56.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the DHCP protocol packets transmitted, which ranges from 0 to 63.

Examples

Set the DSCP value to 30 for DHCP protocol packets sent by the DHCP clients.

```
<Sysname> system-view
```

```
[Sysname] dhcp client dscp 30
```

dhcp dscp

Use **dhcp dscp** to set the DSCP value for DHCP protocol packets sent by the DHCP servers and DHCP relay agents.

Use **undo dhcp dscp** to restore the default.

Syntax

dhcp dscp *dscp-value*

undo dhcp dscp

Default

The DSCP value in DHCP protocol packets sent by the DHCP servers and DHCP relay agents is 56.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the DHCP protocol packets transmitted, which ranges from 0 to 63.

Examples

Set the DSCP value to 30 for DHCP protocol packets transmitted.

```
<Sysname> system-view
```

```
[Sysname] dhcp dscp 30
```

dns dscp

Use **dns dscp** to set the DSCP value for DNS protocol packets transmitted.

Use **undo dns dscp** to restore the default.

Syntax

dns dscp *dscp-value*

undo dns dscp

Default

The DSCP value in DNS protocol packets transmitted is 0.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the DNS protocol packets transmitted, which ranges from 0 to 63.

Examples

Set the DSCP value to 30 for DNS protocol packets transmitted.

```
<Sysname> system-view
```

```
[Sysname] dns dscp 30
```

dns ipv6 dscp

Use **dns ipv6 dscp** to set the DSCP value for IPv6 DNS protocol packets transmitted.

Use **undo dns ipv6 dscp** to restore the default.

Syntax

dns ipv6 dscp *dscp-value*

undo dns ipv6 dscp

Default

The DSCP value in IPv6 DNS protocol packets transmitted is 0.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the IPv6 DNS protocol packets transmitted, which ranges from 0 to 63.

Examples

Set the DSCP value to 30 for IPv6 DNS protocol packets transmitted.

```
<Sysname> system-view
```

```
[Sysname] dns ipv6 dscp 30
```

dscp (IGMP view)

Use **dscp** to set the DSCP value for IGMP protocol packets.

Use **undo dscp** to restore the default.

Syntax

dscp *dscp-value*

undo dscp

Default

The DSCP value in IGMP protocol packets is 48.

Views

Public network IGMP view, VPN instance IGMP view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

Set the DSCP value to 63 for IGMP protocol packets in the public network.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] dscp 63
```

Set the DSCP value to 63 for IGMP protocol packets in the VPN instance named **mvpn**.

```
<Sysname> system-view
[Sysname] igmp vpn-instance mvpn
[Sysname-igmp-mvpn] dscp 63
```

dscp (IGMP-Snooping view)

Use **dscp** to set the DSCP value for IGMP protocol packets transmitted.

Use **undo dscp** to restore the default.

Syntax

dscp *dscp-value*

undo dscp

Default

The DSCP value in IGMP protocol packets transmitted is 48.

Views

IGMP-snooping view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the IGMP protocol packets transmitted, which ranges from 0 to 63.

Examples

Set the DSCP value to 63 for IGMP protocol packets transmitted.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] dscp 63
```

dscp (IPv6 PIM view)

Use **dscp** to set the DSCP value for IPv6 PIM protocol packets.

Use **undo dscp** to restore the default.

Syntax

dscp *dscp-value*

undo dscp

Default

The DSCP value in IPv6 PIM protocol packets is 48.

Views

IPv6 PIM view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

Set the DSCP value to 63 for IPv6 PIM protocol packets.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] dscp 63
```

dscp (MLD view)

Use **dscp** to set the DSCP value for MLD protocol packets.

Use **undo dscp** to restore the default.

Syntax

dscp *dscp-value*

undo dscp

Default

The DSCP value in MLD protocol packets is 48.

Views

MLD view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

Set the DSCP value to 63 for MLD protocol packets.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] dscp 63
```

dscp (MLD-Snooping view)

Use **dscp** to set the DSCP value for MLD protocol packets transmitted.

Use **undo dscp** to restore the default.

Syntax

dscp *dscp-value*

undo dscp

Default

The DSCP value in MLD protocol packets transmitted is 48.

Views

MLD-snooping view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the MLD protocol packets transmitted, which ranges from 0 to 63.

Examples

Set the DSCP value to 63 for MLD protocol packets transmitted by MLD-snooping.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] dscp 63
```

dscp (MPLS LDP view)

Use **dscp** to set the DSCP value for outgoing LDP packets.

Use **undo dscp** to restore the default.

Syntax

dscp *dscp-value*

undo dscp

Default

The DSCP value for outgoing LDP packets is 48.

Views

MPLS LDP view

Default command level

2: System level

Parameters

dscp-value: DSCP value for outgoing LDP packets, in the range of 0 to 63.

Examples

Set the DSCP for outgoing LDP packets to 56.

```
<Sysname> system-view
[Sysname] mpls lsr-id 1.1.1.1
[Sysname] mpls
[Sysname-mpls] quit
[Sysname] mpls ldp
[Sysname-mpls-ldp] dscp 56
```

dscp (OSPF view)

Use **dscp** to set the DSCP value for OSPF protocol packets.

Use **undo dscp** to restore the default.

Syntax

dscp *dscp-value*

undo dscp

Default

The DSCP value in OSPF protocol packets is 48.

Views

OSPF view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

Set the DSCP value to 63 for OSPF protocol packets sent by OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf
[Sysname-ospf-1] dscp 63
```

dscp (PIM view)

Use **dscp** to set the DSCP value for PIM protocol packets.

Use **undo dscp** to restore the default.

Syntax

dscp *dscp-value*

undo dscp

Default

The DSCP value in PIM protocol packets is 48.

Views

Public network PIM view, VPN instance PIM view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

Set the DSCP value to 63 for PIM protocol packets in the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] dscp 63
```

Set the DSCP value to 63 for PIM protocol packets in the VPN instance named **mvpn**.

```
<Sysname> system-view
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] dscp 63
```

dscp (RIP view)

Use **dscp** to set the DSCP value for RIP protocol packets.

Use **undo dscp** to restore the default.

Syntax

dscp *dscp-value*

undo dscp

Default

The DSCP value in RIP protocol packets is 48.

Views

RIP view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

Set the DSCP value to 63 for RIP protocol packets sent by RIP process 1.

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1] dscp 63
```

ftp client dscp

Use **ftp client dscp** to set the DSCP value for FTP protocol packets sent by the FTP clients.

Use **undo ftp client dscp** to restore the default.

Syntax

ftp client dscp *dscp-value*

undo ftp client dscp

Default

The DSCP value in protocol packets sent by the FTP clients is 0.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

Set the DSCP value to 30 for protocol packets sent by the FTP clients.

```
<Sysname> system-view
[Sysname] ftp client dscp 30
```

ftp client ipv6 dscp

Use **ftp client ipv6 dscp** to set the DSCP value for FTP protocol packets sent by the IPv6 FTP clients.

Use **undo ftp client ipv6 dscp** to restore the default.

Syntax

ftp client ipv6 dscp *dscp-value*

undo ftp client ipv6 dscp

Default

The DSCP value in protocol packets sent by the IPv6 FTP clients is 0.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

Set the DSCP value to 30 for protocol packets sent by the IPv6 FTP clients.

```
<Sysname> system-view
```

```
[Sysname] ftp client ipv6 dscp 30
```

ftp server dscp

Use **ftp server dscp** to set the DSCP value for FTP protocol packets sent by the FTP servers.

Use **undo ftp server dscp** to restore the default.

Syntax

ftp server dscp *dscp-value*

undo ftp server dscp

Default

The DSCP value in protocol packets sent by the FTP servers is 0.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

Set the DSCP value to 30 for protocol packets sent by the FTP servers.

```
<Sysname> system-view
```

```
[Sysname] ftp server dscp 30
```


ip http dscp

Use **ip http dscp** to set the DSCP value for HTTP protocol packets transmitted.

Use **undo ip http dscp** to restore the default.

Syntax

ip http dscp *dscp-value*

undo ip http dscp

Default

The DSCP value in HTTP protocol packets transmitted is 16.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

Set the DSCP value to 30 for HTTP protocol packets transmitted.

```
<Sysname> system-view
```

```
[Sysname] ip http dscp 30
```

ipv6 dhcp client dscp

Use **ipv6 dhcp client dscp** to set the DSCP value for DHCPv6 protocol packets sent by the DHCPv6 clients.

Use **undo ipv6 dhcp client dscp** to restore the default.

Syntax

ipv6 dhcp client dscp *dscp-value*

undo ipv6 dhcp client dscp

Default

The DSCP value in DHCPv6 protocol packets sent by the DHCPv6 clients is 56

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the DHCPv6 protocol packets transmitted, which ranges from 0 to 63.

Examples

Set the DSCP value to 30 for DHCPv6 protocol packets sent by the DHCPv6 clients.

```
<Sysname> system-view
```

```
[Sysname] ipv6 dhcp client dscp 30
```

ipv6 dhcp dscp

Use **ipv6 dhcp dscp** to set the DSCP value for DHCPv6 protocol packets sent by the DHCPv6 servers and DHCPv6 relay agents.

Use **undo ipv6 dhcp dscp** to restore the default.

Syntax

ipv6 dhcp dscp *dscp-value*

undo ipv6 dhcp dscp

Default

The DSCP value in DHCPv6 protocol packets sent by the DHCPv6 servers and DHCPv6 relay agents is 56.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the DHCPv6 protocol packets transmitted, which ranges from 0 to 63.

Examples

Set the DSCP value to 30 for the DHCPv6 protocol packets sent by the DHCPv6 servers and DHCPv6 relay agents.

```
<Sysname> system-view
```

```
[Sysname] ipv6 dhcp dscp 30
```

ipv6 http dscp

Use **ipv6 http dscp** to set the DSCP value for IPv6 HTTP protocol packets transmitted.

Use **undo ipv6 http dscp** to restore the default.

Syntax

ipv6 http dscp *dscp-value*

undo ipv6 http dscp

Default

The DSCP value in IPv6 HTTP protocol packets transmitted is 0.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

Set the DSCP value to 30 for IPv6 HTTP protocol packets transmitted.

```
<Sysname> system-view
```

```
[Sysname] ipv6 http dscp 30
```

mpls rsvp-te dscp

Use **mpls rsvp-te dscp** to set the DSCP value for outgoing RSVP packets.

Use **undo mpls rsvp-te dscp** to restore the default.

Syntax

mpls rsvp-te dscp *dscp-value*

undo mpls rsvp-te dscp

Default

The DSCP value for outgoing RSVP packets is 48.

Views

MPLS view

Default command level

2: System level

Parameters

dscp-value: DSCP value for outgoing RSVP packets, in the range of 0 to 63.

Examples

Set DSCP 56 for RSVP packets.

```
<Sysname> system-view
```

```
[Sysname] mpls
```

```
[Sysname-mpls] mpls rsvp-te dscp 56
```

nqa server tcp-connect tos

Use **nqa server tcp-connect tos** to set the ToS value for packets sent by the TCP listening service on the NQA server.

Use **undo nqa server tcp-connect tos** to restore the default.

Syntax

nqa server tcp-connect tos *tos*

undo nqa server tcp-connect tos

Default

The ToS value in the packets sent by the TCP listening service on the NQA server is 0.

Views

System view

Default command level

2: System level

Parameters

tos: Type of Service (ToS) field value in the protocol packets sent by the TCP listening service on the NQA server. This argument ranges from 0 to 255.

Examples

Set the ToS value to 30 for packets sent by the TCP listening service on the NQA server.

```
<Sysname> system-view
```

```
[Sysname] nqa server tcp-connect tos 30
```

nqa server udp-echo tos

Use **nqa server udp-echo tos** to set the ToS value for packets sent by the UDP listening service on the NQA server.

Use **undo nqa server udp-echo tos** to restore the default.

Syntax

nqa server udp-echo tos *tos*

undo nqa server udp-echo tos

Default

The ToS value in the packets sent by the UDP listening service on the NQA server is 0.

Views

System view

Default command level

2: System level

Parameters

tos: Type of Service (ToS) field value in the protocol packets sent by the UDP listening service on the NQA server. This argument ranges from 0 to 255.

Examples

Set the ToS value to 30 for packets sent by the UDP listening service on the NQA server.

```
<Sysname> system-view
```

```
[Sysname] nqa server udp-echo tos 30
```

ntp-service dscp

Use **ntp-service dscp** to set the DSCP value for NTP protocol packets.

Use **undo ntp-service dscp** to restore the default.

Syntax

ntp-service dscp *dscp-value*

undo ntp-service dscp

Default

The DSCP value in NTP protocol packets is 16.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

Set the DSCP value to 30 for NTP protocol packets.

```
<Sysname> system-view
```

```
[Sysname] ntp-service dscp 30
```

peer dscp (BGP/BGP-VPN instance view)

Use **peer dscp** to set the DSCP value for BGP protocol packets sent to the specified BGP peer or BGP peer group.

Use **undo peer dscp** to cancel the configuration.

Syntax

peer { *group-name* | *ip-address* } **dscp** *dscp-value*

undo peer { *group-name* | *ip-address* } **dscp**

Default

The DSCP value in BGP protocol packets is 48.

Views

BGP view, BGP VPN instance view

Default command level

2: System level

Parameters

group-name: Peer group name, a string of 1 to 47 characters.

ip-address: IP address of a peer.

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Usage guidelines

Make sure the specified BGP peer or BGP peer group already exists.

Examples

In BGP view, set the DSCP value to 63 for BGP protocol packets sent to the BGP peer group named **test**, which already exists.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test dscp 63
```

In BGP VPN instance view, set the DSCP value to 63 for BGP protocol packets sent to the BGP peer group named **test**, which already exists. (You must create VPN instance **vpn1** first)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer test dscp 63
```

peer dscp (IPv6 address family view)

Use **peer dscp** to set the DSCP value for IPv6 BGP protocol packets sent to the specified IPv6 peer or IPv6 peer group.

Use **undo peer dscp** to cancel the configuration.

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **dscp** *dscp-value*

undo peer { *ipv6-group-name* | *ipv6-address* } **dscp**

Default

The DSCP value in IPv6 BGP protocol packets is 48.

Views

IPv6 address family view

Default command level

2: System level

Parameters

ipv6-group-name: Peer group name, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Usage guidelines

Make sure the specified IPv6 peer or IPv6 peer group already exists.

Examples

Set the DSCP value to 63 for IPv6 BGP protocol packets sent to the EBGP peer group named **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test dscp 63
```

radius dscp

Use **radius dscp** to set the DSCP value for IPv4 RADIUS protocol packets.

Use **undo radius dscp** to restore the default.

Syntax

radius dscp *dscp-value*

undo radius dscp

Default

The DSCP value in IPv4 RADIUS protocol packets is 0.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

Set the DSCP value to 6 for IPv4 RADIUS protocol packets.

```
<Sysname> system-view
[Sysname] radius dscp 6
```

radius ipv6 dscp

Use **radius ipv6 dscp** to set the DSCP value for IPv6 RADIUS protocol packets.

Use **undo radius ipv6 dscp** to restore the default.

Syntax

```
radius ipv6 dscp dscp-value  
undo radius ipv6 dscp
```

Default

The DSCP value in IPv6 RADIUS protocol packets is 0.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

```
# Set the DSCP value to 6 for IPv6 RADIUS protocol packets.  
<Sysname> system-view  
[Sysname] radius ipv6 dscp 6
```

sftp client dscp

Use **sftp client dscp** to set the DSCP value for protocol packets sent by the IPv4 SFTP clients.
Use **undo sftp client dscp** to restore the default.

Syntax

```
sftp client dscp dscp-value  
undo sftp client dscp
```

Default

The DSCP value in protocol packets sent by the IPv4 SFTP clients is 16.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

```
# Set the DSCP value to 30 for protocol packets sent by the IPv4 SFTP clients.  
<Sysname> system-view  
[Sysname] sftp client dscp 30
```

sftp client ipv6 dscp

Use **sftp client ipv6 dscp** to set the DSCP value for protocol packets sent by the IPv6 SFTP clients.
Use **undo sftp client ipv6 dscp** to restore the default.

Syntax

sftp client ipv6 dscp *dscp-value*

undo sftp client ipv6 dscp

Default

The DSCP value in protocol packets sent by the IPv6 SFTP clients is 8.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

Set the DSCP value to 30 for protocol packets sent by the IPv6 SFTP clients.

```
<Sysname> system-view
```

```
[Sysname] sftp client ipv6 dscp 30
```

snmp-agent packet response dscp

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

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

Syntax

snmp-agent packet response dscp *dscp-value*

undo snmp-agent packet response dscp

Default

The DSCP value in SNMP response packets is 0.

Views

System view

Default command level

3: Manage level

Parameters

dscp-value: DSCP value in the SNMP response packets, which ranges from 0 to 63.

Examples

Set the DSCP value to 45 for SNMP response packets.

```
<Sysname> system-view
```

```
[Sysname] snmp-agent packet response dscp 45
```

ssh client dscp

Use **ssh client dscp** to set the DSCP value for protocol packets sent by the IPv4 SSH clients.

Use **undo ssh client dscp** to restore the default.

Syntax

```
ssh client dscp dscp-value  
undo ssh client dscp
```

Default

The DSCP value in protocol packets sent by the IPv4 SSH clients is 16.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

```
# Set the DSCP value to 30 for protocol packets sent by the IPv4 SSH clients.  
<Sysname> system-view  
[Sysname] ssh client dscp 30
```

ssh client ipv6 dscp

Use **ssh client ipv6 dscp** to set the DSCP value for protocol packets sent by the IPv6 SSH clients.

Use **undo ssh client ipv6 dscp** to restore the default.

Syntax

```
ssh client ipv6 dscp dscp-value  
undo ssh client ipv6 dscp
```

Default

The DSCP value in protocol packets sent by the IPv6 SSH clients is 0.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

```
# Set the DSCP value to 30 for protocol packets sent by the IPv6 SSH clients.  
<Sysname> system-view  
[Sysname] ssh client ipv6 dscp 30
```

ssh server dscp

Use **ssh server dscp** to set the DSCP value for protocol packets sent by the IPv4 SSH servers.

Use **undo ssh server dscp** to restore the default.

Syntax

```
ssh server dscp dscp-value  
undo ssh server dscp
```

Default

The DSCP value in protocol packets sent by the IPv4 SSH servers is 16.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

```
# Set the DSCP value to 30 for protocol packets sent by the IPv4 SSH servers.  
<Sysname> system-view  
[Sysname] ssh server dscp 30
```

ssh server ipv6 dscp

Use **ssh server ipv6 dscp** to set the DSCP value for protocol packets sent by the IPv6 SSH servers.

Use **undo ssh server ipv6 dscp** to restore the default.

Syntax

```
ssh server ipv6 dscp dscp-value  
undo ssh server ipv6 dscp
```

Default

The DSCP value in protocol packets sent by the IPv6 SSH servers is 0.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

```
# Set the DSCP value to 30 for protocol packets sent by the IPv6 SSH servers.  
<Sysname> system-view  
[Sysname] ssh server ipv6 dscp 30
```

telnet client dscp

Use **telnet client dscp** to set the DSCP value for protocol packets sent by the Telnet clients.

Use **undo telnet client dscp** to restore the default.

Syntax

telnet client dscp *dscp-value*

undo telnet client dscp

Default

The DSCP value in protocol packets sent by the Telnet clients is 16.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

Set the DSCP value to 30 for protocol packets sent by the Telnet clients.

```
<Sysname> system-view
```

```
[Sysname] telnet client dscp 30
```

telnet client ipv6 dscp

Use **telnet client ipv6 dscp** to set the DSCP value for protocol packets sent by the IPv6 Telnet clients.

Use **undo telnet client ipv6 dscp** to restore the default.

Syntax

telnet client ipv6 dscp *dscp-value*

undo telnet client ipv6 dscp

Default

The DSCP value in protocol packets sent by the IPv6 Telnet clients is 0.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

Set the DSCP value to 0 for protocol packets sent by the IPv6 Telnet clients.

```
<Sysname> system-view
```

```
[Sysname] telnet client ipv6 dscp 30
```

telnet server dscp

Use **telnet server dscp** to set the DSCP value for protocol packets sent by the Telnet servers.

Use **undo telnet server dscp** to restore the default.

Syntax

telnet server dscp *dscp-value*

undo telnet server dscp

Default

The DSCP value in protocol packets sent by the Telnet servers is 48.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

Set the DSCP value to 30 for protocol packets sent by the Telnet servers.

```
<Sysname> system-view
```

```
[Sysname] telnet server dscp 30
```

telnet server ipv6 dscp

Use **telnet server ipv6 dscp** to set the DSCP value for protocol packets sent by the IPv6 Telnet servers.

Use **undo telnet server ipv6 dscp** to restore the default.

Syntax

telnet server ipv6 dscp *dscp-value*

undo telnet server ipv6 dscp

Default

The DSCP value in protocol packets sent by the IPv6 Telnet servers is 0.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

Set the DSCP value to 30 for protocol packets sent by the IPv6 Telnet servers.

```
<Sysname> system-view
```

```
[Sysname] telnet server ipv6 dscp 30
```

tftp client dscp

Use **tftp client dscp** to set the DSCP value for protocol packets sent by the TFTP clients.

Use **undo tftp client dscp** to restore the default.

Syntax

tftp client dscp *dscp-value*

undo tftp client dscp

Default

The DSCP value in protocol packets sent by the TFTP clients is 0.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

Set the DSCP value to 30 for protocol packets sent by the TFTP clients.

```
<Sysname> system-view
```

```
[Sysname] tftp client dscp 30
```

tftp client ipv6 dscp

Use **tftp client ipv6 dscp** to set the DSCP value for protocol packets sent by the IPv6 TFTP clients.

Use **undo tftp client ipv6 dscp** to restore the default.

Syntax

tftp client ipv6 dscp *dscp-value*

undo tftp client ipv6 dscp

Default

The DSCP value in protocol packets sent by the IPv6 TFTP clients is 0.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

Set the DSCP value to 30 for protocol packets sent by the IPv6 TFTP clients.

```
<Sysname> system-view
```

```
[Sysname] tftp client ipv6 dscp 30
```

tos (DHCP operation type view)

Use **tos** to set the ToS value for NQA probe packets.

Use **undo tos** to restore the default.

Syntax

tos *value*

undo tos

Default

The ToS value in NQA probe packets is 0.

Views

DHCP operation type view

Default command level

2: System level

Parameters

value: ToS value in the NQA probe packets, which ranges from 0 to 255.

Examples

Set the ToS value to 1 for NQA probe packets.

```
<Sysname> system-view
```

```
[Sysname] nqa entry admin test
```

```
[Sysname-nqa-admin-test] type dhcp
```

```
[Sysname-nqa-admin-test-dhcp] tos 1
```

vrrp dscp

Use **vrrp dscp** to set the DSCP value for IPv4 VRRP protocol packets.

Use **undo vrrp dscp** to restore the default.

Syntax

vrrp dscp *dscp-value*

undo vrrp dscp

Default

The DSCP value in IPv4 VRRP protocol packets is 48.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

Set the DSCP value to 30 for IPv4 VRRP protocol packets transmitted.

```
<Sysname> system-view
```

```
[Sysname] vrrp dscp 30
```

vrrp ipv6 dscp

Use **vrrp ipv6 dscp** to set the DSCP value for IPv6 VRRP protocol packets.

Use **undo vrrp ipv6 dscp** to restore the default.

Syntax

```
vrrp ipv6 dscp dscp-value  
undo vrrp ipv6 dscp
```

Default

The DSCP value in IPv6 VRRP protocol packets is 56.

Views

System view

Default command level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Examples

Set the DSCP value to 30 for IPv6 VRRP protocol packets transmitted.

```
<Sysname> system-view
```

```
[Sysname] vrrp ipv6 dscp 30
```

Modified commands

Modified command: info-center loghost

Old syntax

```
info-center loghost [ vpn-instance vpn-instance-name ] { host-ipv4-address | ipv6  
host-ipv6-address } [ port port-number ] [ channel { channel-number | channel-name } | facility  
local-number ] *
```

New syntax

```
info-center loghost [ vpn-instance vpn-instance-name ] { host-ipv4-address | ipv6  
host-ipv6-address } [ port port-number ] [ dscp dscp-value ] [ channel { channel-number |  
channel-name } | facility local-number ] *
```

Views

System view

Change description

The **dscp** *dscp-value* option is added.

dscp *dscp-value*: Sets the DSCP value in the packets sent to the log host, which ranges from 0 to 63 and defaults to 0.

Modified command: ping ipv6

Old syntax

```
ping ipv6 [ -a source-ipv6 | -c count | -m interval | -s packet-size | -t timeout | -vpn-instance  
vpn-instance-name ] * host [ -i interface-type interface-number ]
```

New syntax

```
ping ipv6 [ -a source-ipv6 | -c count | -m interval | -s packet-size | -t timeout | -vpn-instance  
vpn-instance-name | -tos tos ] * host [ -i interface-type interface-number ]
```

Views

Any view

Change description

The **-tos** *tos* option is added.

-tos *tos*: Sets the Traffic Class field value in the ICMPv6 echo request. The *tos* argument ranges from 0 to 255 and defaults to 0.

Modified command: snmp-agent target-host

Old syntax

```
snmp-agent target-host trap address udp-domain { ip-address | ipv6 ipv6-address } [ udp-port
port-number ] [ vpn-instance vpn-instance-name ] params securityname security-string [ v1 | v2c
| v3 [ authentication | privacy ] ]
```

New syntax

```
snmp-agent target-host trap address udp-domain { ip-address | ipv6 ipv6-address } [ udp-port
port-number ] [ dscp dscp-value ] [ vpn-instance vpn-instance-name ] params securityname
security-string [ v1 | v2c | v3 [ authentication | privacy ] ]
```

Views

System view

Change description

The **dscp** *dscp-value* option is added.

dscp *dscp-value*: Sets the DSCP value for the SNMP traps, which ranges from 0 to 63 and defaults to 0.

Modified command: tracer

Old syntax

```
tracer [ -a source-ip | -f first-ttl | -m max-ttl | -p port | -q packet-number | -vpn-instance
vpn-instance-name | -w timeout ] * host
```

New syntax

```
tracer [ -a source-ip | -f first-ttl | -m max-ttl | -p port | -q packet-number | -vpn-instance
vpn-instance-name | -w timeout | -tos tos ] * host
```

Views

Any view

Change description

The **-tos** *tos* option is added.

-tos *tos*: Sets the ToS field value in the tracer request. The *tos* argument ranges from 0 to 255 and defaults to 0.

Modified command: tracer ipv6

Old syntax

```
tracer ipv6 [ -f first-ttl | -m max-ttl | -p port | -q packet-number | -vpn-instance vpn-instance-name |
-w timeout ] * host
```


New syntax

tracert ipv6 [**-f** *first-ttl* | **-m** *max-ttl* | **-p** *port* | **-q** *packet-number* | **-vpn-instance** *vpn-instance-name* | **-w** *timeout* | **-tos** *tos*] * *host*

Views

Any view

Change description

The **-tos** *tos* option is added.

-tos *tos*: Sets the Traffic Class field value in the tracert request. The *tos* argument ranges from 0 to 255 and defaults to 0.

New feature: Automatic configuration file backup for software downgrading

Configuring automatic configuration file backup for software downgrading

After a software upgrade, the first time you use the **save** [**safely**] [**backup** | **main**] [**force**] command to save configuration to a configuration file that was created before the upgrade, the system verifies the compatibility of the configuration file with the software version.

If any incompatibility is found, the system uses the running configuration to overwrite the configuration file after backing up the file to the Flash memory on each member device for future rollback. The backup file is named in the *old-filename_bak.cfg* format. For example, if the old configuration file is named *config.cfg*, the backup file is named *config_bak.cfg*.

If the backup attempt fails on an IRF member device, choose one of the following failure handling actions at prompt:

- **Give up saving the configuration**—In this approach, the system does not save the configuration on any member device.
- **Overwrite the configuration file**—In this approach, the system uses the running configuration to overwrite the configuration file on the member device without backing up the file. You can copy the backup configuration file from the master device to this member device for future rollback.

To load the backup configuration file after a software downgrade, specify the file as the next-startup configuration file before performing the downgrade.

Command reference

None.

New feature: Configuring LLDP to advertise a specific voice VLAN

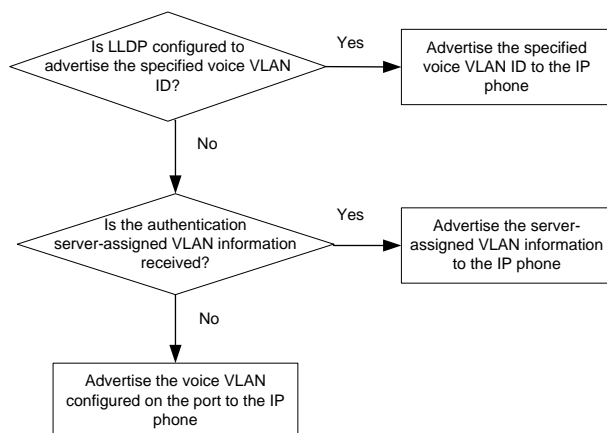
Voice VLAN advertisement through LLDP is available only for LLDP-enabled IP phones. If CDP-compatibility is enabled, this feature is also available for CDP-enabled IP phones. For more information about LLDP, CDP compatibility, and voice VLANs, see *Layer 2—LAN Switching Configuration Guide*.

Configuration guidelines

By default, if the voice VLAN feature is configured on an LLDP-enabled port, LLDP advertises this voice VLAN to the IP phone connected to the port. This feature allows you to specify the voice VLAN information that LLDP will advertise to IP phones through network policy TLVs.

Figure 3 shows the procedure of voice VLAN advertisement through LLDP.

Figure 3 Voice VLAN advertisement through LLDP



With the received voice VLAN information, the IP phone automatically completes the voice VLAN configuration, including the voice VLAN ID, tagging status, and priority. This voice VLAN can be the voice VLAN directly specified for LLDP advertisement, the voice VLAN configured on the port, or the voice VLAN assigned by a server, depending on your configuration.

To identify the voice VLAN advertised by LLDP, execute the **display lldp local-information** command, and examine the MED information fields in the command output.

Configuration procedure

To configure LLDP to advertise a specific voice VLAN:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view or port group view.	<ul style="list-style-type: none">Enter Layer 2 Ethernet interface view: interface <i>interface-type</i> <i>interface-number</i>Enter port group view: port-group manual <i>port-group-name</i>	Use one of the commands.
3. Configure LLDP to advertise a specific voice VLAN.	lldp voice-vlan <i>vlan-id</i>	By default, LLDP advertises the voice VLAN configured on the port.

Dynamically advertising server-assigned VLANs through LLDP

Dynamic advertisement of server-assigned VLANs through LLDP must work with 802.1X or MAC authentication, and is available only for LLDP-enabled IP phones. If 802.1X authentication is used, make sure the IP phones also support 802.1X authentication.

To implement this function for an IP phone, perform the following configuration tasks:

- Enable LLDP globally and on the port connected to the IP phone.
- Configure 802.1X or MAC authentication to make sure the IP phone can pass security authentication. For more information about 802.1X authentication, MAC authentication, and VLAN assignment by servers, see *Security Configuration Guide*.
- Configure VLAN authorization for the IP phone on the authentication server.

After the IP phone passes authentication, LLDP advertises the server-assigned VLAN in the Network Policy TLV to the IP phone. The IP phone will send its traffic tagged with the assigned VLAN.

Command reference

lldp voice-vlan

Syntax

```
lldp voice-vlan vlan-id
undo lldp voice-vlan
```

Views

Layer 2 Ethernet interface view, port group view

Default command level

2: System level

Parameters

vlan-id: Specifies a voice VLAN by its ID, which ranges from 1 to 4094.

Usage guidelines

Use **lldp voice-vlan** *vlan-id* to configure a port to advertise a specific voice VLAN ID to the connected IP phone through LLDP. If CDP compatibility is enabled, LLDP also includes the specified voice VLAN ID in the CDP packets sent to the IP phone.

Use **undo lldp voice-vlan** to restore the default.

By default, if a voice VLAN is configured on an LLDP-enabled port, LLDP advertises this voice VLAN to the IP phone connected to the port.

Examples

```
# Configure port GigabitEthernet 1/0/1 to advertise voice VLAN 4094.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp voice-vlan 4094
```

New feature: Enabling LLDP to automatically discover IP phones

Overview

In a traditional voice VLAN network, the switch maps the source MAC addresses of IP phones to a limited number of OUI addresses to allow them to access the network. This method restricts the types of IP phones on the network, if the IP phones with the source MAC addresses match the same OUI address are categorized as a type.

To break the restriction, you can enable the switch to automatically discover IP phones through LLDP. With this function, the switch can automatically discover the peer, and exchange LLDP TLVs with the

peer. If the LLDP System Capabilities TLV received on a port shows that the peer is phone capable, the switch determines that the peer is an IP phone and sends an LLDP TLV carrying the voice VLAN configuration to the peer.

When the IP phone discovery process is complete, the port will automatically join the voice VLAN and improve the transmission priority of the voice traffic for the IP phone. To ensure that the IP phone can pass authentication, the switch will add the MAC address of the IP phone to the MAC address table.

For more information about voice VLANs, see the chapter "Voice VLAN configuration."

NOTE:

This function is available only when your IP phone supports LLDP. Identify whether your IP phone supports LLDP by checking its usage guide.

Configuration procedure

Before you enable the switch to automatically discover IP phones through LLDP, complete the following tasks:

- Enable LLDP globally and on ports.
- Configure voice VLANs.

To enable LLDP to automatically discover IP phones:

Step	Command	Remarks
1. Enter system view	system-view	N/A
2. Enable LLDP to automatically discover IP phones	voice vlan track lldp	Disabled by default.

! IMPORTANT:

- When the switch is enabled to automatically discover IP phones through LLDP, you can connect at most five IP phones to each port of the switch.
 - You cannot use this function together with CDP compatibility.
-

Command reference

voice vlan track lldp

Use **voice vlan track lldp** to enable LLDP to automatically discover IP phones.

Use **undo voice vlan track lldp** to disable LLDP from automatically discovering IP phones.

Syntax

voice vlan track lldp

undo voice vlan track lldp

Default

LLDP is disabled from automatically discovering IP phones.

Views

System view

Default command level

2: System level

Examples

Enable the switch to automatically discover IP phones through LLDP.

```
<Sysname> system-view
```

```
[Sysname] voice vlan track lldp
```

New feature: MVRP

Overview

Multiple Registration Protocol (MRP) is an attribute registration protocol and transmits attribute messages. Multiple VLAN Registration Protocol (MVRP) is a typical MRP application. MVRP propagates and learns VLAN configuration among devices. MVRP enables a device to propagate the local VLAN configuration to the other devices, receive VLAN configuration from other devices, and dynamically update the local VLAN configuration (including the active VLANs and the ports through which a VLAN can be reached). MVRP makes sure that all MVRP-enabled devices in a LAN maintain the same VLAN configuration, and reduces the VLAN configuration workload. When the network topology changes, MVRP can propagate and learn VLAN configuration information again according to the new topology, and real-time synchronize the network topology.

MRP is an enhanced version of Generic Attribute Registration Protocol (GARP) and improves the declaration efficiency. MVRP is an enhanced version of GARP VLAN Registration Protocol (GVRP). MVRP delivers the following benefits over GVRP:

- GVRP does not support the multiple spanning tree instance (MSTI). MVRP runs on a per-MSTI basis, and implements per-VLAN redundant link calculation and load sharing.
- MVRP decreases the number of packets transmitted for the same amount of VLAN configuration, and improves the declaration efficiency.

For more information about GVRP or MSTI, see "*Layer 2—LAN Switching Configuration Guide*."

MRP

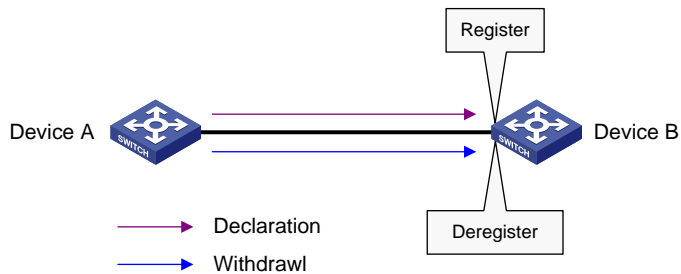
MRP allows participants in the same LAN to declare, propagate, and register information (for example, VLAN information) on a per Multiple Spanning Tree Instance (MSTI) basis.

MRP implementation

Each port that participates in an MRP application (for example, MVRP) is called an "MRP participant." Similarly, a port that participates in an MVRP application is called an "MVRP participant."

As shown in [Figure 4](#), an MRP participant registers and deregisters its attribute values on other MRP participants by sending declarations and withdrawals, and registers and deregisters the attribute values of other participants according to the received declarations and withdrawals. MRP rapidly propagates the configuration information of an MRP participant throughout the LAN.

Figure 4 MRP implementation



MVRP registers and deregisters VLAN attributes as follows:

- When a port receives the declaration of a VLAN attribute, the port registers the VLAN and joins the VLAN.
- When a port receives the withdrawal of a VLAN attribute, the port deregisters the VLAN and leaves the VLAN.

Figure 4 shows a simple MVRP implementation on an MSTI. In a network with multiple MSTIs, VLAN registration and deregistration are performed on a per-MSTI basis.

MRP messages

MRP exchanges information among MRP participants by advertising MRP messages, including Join, New, Leave, and LeaveAll. Join and New messages are declarations, and Leave and LeaveAll messages are withdrawals.

- Join message
 - An MRP participant sends Join messages when it wishes to declare the attribute values configured on it and receives Join messages from other MRP participants.
 - When receiving a Join message, an MRP participant sends a Join message to all participants except the sender.

Join messages fall into the following types:

- **JoinEmpty**—An MRP participant sends JoinEmpty messages to declare attribute values that it has not registered. For example, when a static VLAN exists on a device, the attribute of the VLAN on the device is not changed even if the device learns the VLAN again through MRP. In this case, the Join message for the VLAN attribute is a JoinEmpty message, because the VLAN attribute is not registered.
- **JoinIn**—An MRP participant sends JoinIn messages to declare attribute values that it has registered. For example, when the device learns a VLAN through MRP messages, and dynamically creates the VLAN, the Join message for the VLAN attribute is a JoinIn message.
- New message

Similar to a Join message, a New message enables MRP participants to register attributes.

 - When the Multiple Spanning Tree Protocol (MSTP) topology changes, an MRP participant sends New messages to declare the topology change.
 - On receiving a New message, an MRP participant sends a New message out of each port except the receiving port.
- Leave message
 - An MRP participant sends Leave messages when it wishes other participants to deregister the attributes that it has deregistered.
 - When receiving a Leave message, an MRP participant sends a Leave message to all participants except the sender.
- LeaveAll message

- Each MRP participant is configured with an individual LeaveAll timer. When the timer expires, the MRP participant sends LeaveAll messages to the remote participants, so that the local participant and the remote participants deregister all attributes and re-register all attributes. This process periodically clears the useless attributes in the network.
- On receiving a LeaveAll message, MRP determines whether to send a Join message to request the sender to re-register these attributes according to attribute status.

MRP timers

The implementation of MRP uses the following timers to control MRP message transmission.

- Periodic timer

On startup, an MRP participant starts its own Periodic timer to control MRP message transmission. The MRP participant collects the MRP messages to be sent before the Periodic timer expires, and sends the MRP messages in as few packets as possible when the Periodic timer expires and meanwhile restarts the Periodic timer. This mechanism reduces the number of MRP protocol packets periodically sent.

You can enable or disable the Periodic timer at the CLI. When you disable the Periodic timer, MRP will not periodically send MRP messages, and MRP messages are sent only when the LeaveAll timer expires or the local participant receives LeaveAll messages from a remote participant.

- Join timer

The Join timer controls the transmission of Join messages. To make sure Join messages can be reliably transmitted to other participants, an MRP participant waits for a period of the Join timer after sending a Join message. If the participant receives JoinIn messages from other participants and the attributes in the JoinIn messages are the same as the sent Join messages before the Join timer expires, the participant does not re-send the Join message. When both the Join timer and the Periodic timer expire, the participant re-sends the Join message.

- Leave timer

The Leave timer controls the deregistration of attributes. When an MRP participant wishes other participants to deregister its attributes, it sends a Leave message. On receiving a Leave message, MRP starts the Leave timer, and deregisters the attributes if it does not receive any Join message for the attributes before the Leave timer expires. When an MRP participant sends or receives LeaveAll messages, it starts the Leave timer. MRP deregisters the attributes in the LeaveAll messages if it does not receive any Join message for the attributes before the Leave timer expires.

- LeaveAll timer

On startup, an MRP participant starts its own LeaveAll timer. When the LeaveAll timer expires, MRP sends out a LeaveAll message and restarts the LeaveAll timer. On receiving the LeaveAll message, other participants re-register all the attributes and re-start their LeaveAll timer.

When you configure the MRP timers, follow these guidelines:

- When the LeaveAll timer of an MRP participant expires, the MRP participant sends LeaveAll messages to the remote participants. On receiving a LeaveAll message, a remote participant restarts its LeaveAll timer, and stops sending out LeaveAll messages. This mechanism effectively reduces the number of LeaveAll messages in the network.
- To avoid the case that the LeaveAll timer of a fixed participant always first expires, the switch randomly changes the LeaveAll timer within a certain range when the MRP participant restarts its LeaveAll timer.

MVRP registration modes

The VLAN information propagated by MVRP includes not only locally, manually configured static VLAN information but also dynamic VLAN information from other devices.

VLANs created manually, locally are called "static VLANs", and VLANs learned through MVRP are called "dynamic VLANs." The following MVRP registration modes are available.

- **Normal**
An MVRP participant in normal registration mode performs dynamic VLAN registrations and deregistrations, and sends declarations and withdrawals for dynamic and static VLANs.
- **Fixed**
An MVRP participant in fixed registration mode disables deregistering dynamic VLANs, sends declarations for dynamic VLANs and static VLANs, and drops received MVRP protocol packets. As a result, an MVRP participant port in fixed registration mode does not deregister or register dynamic VLANs.
- **Forbidden**
An MVRP participant in forbidden registration mode disables registering dynamic VLANs, sends declarations for dynamic VLANs and static VLANs, and drops received MVRP protocol packets. As a result, an MVRP participant in forbidden registration mode does not register dynamic VLANs, and does not re-register a dynamic VLAN when the VLAN is deregistered.

Protocols and standards

IEEE 802.1ak *IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks – Amendment 07: Multiple Registration Protocol*

MVRP configuration task list

Task	Remarks
Enabling MVRP	Required.
Configuring the MVRP registration mode	Optional.
Configuring MRP timers	Optional.
Enabling GVRP compatibility	Optional.

Configuration prerequisites

Before configuring MVRP, perform the following tasks:

- Make sure that all MSTIs in the network are effective and each MSTI is mapped to an existing VLAN on each device in the network, because MVRP runs on a per-MSTI basis.
- Configure the involved ports as trunk ports, because MVRP is available only on trunk ports.

Enabling MVRP

This section describes how to enable MVRP.

Configuration restrictions and guidelines

- MVRP can work with STP, RSTP, or MSTP, but not other link layer topology protocols, including PVST, RRPP, and Smart Link. Ports blocked by STP, RSTP, or MSTP can receive and send MVRP protocol packets. For more information about STP, RSTP, MSTP, and PVST, see " *Layer 2—LAN Switching Configuration Guide*." For more information about RRPP and Smart Link, see *High Availability Configuration Guide*.
- Do not enable both MVRP and remote port mirroring on a port. Otherwise, MVRP may register the remote probe VLAN to incorrect ports, which would cause the monitor port to receive

undesired duplicates. For more information about port mirroring, see *Network Management and Monitoring Configuration Guide*.

- Enabling MVRP on a Layer 2 aggregate interface enables both the aggregate interface and all Selected member ports in the link aggregation group to participate in dynamic VLAN registration and deregistration.

Configuration procedure

To enable MVRP:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable MVRP globally.	mvrp global enable	By default, MVRP is globally disabled. To enable MVRP on a port, first enable MVRP globally.
3. Enter interface view.	<ul style="list-style-type: none"> • Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: interface <i>interface-type interface-number</i> • Enter port group view: port-group manual <i>port-group-name</i> 	Use one of the commands.
4. Configure the port to permit the specified VLANs.	port trunk permit vlan { <i>vlan-list</i> all }	By default, a trunk port permits only VLAN 1. Make sure that the trunk port permits all registered VLANs. For more information about the port trunk permit vlan command, see <i>Layer 2—LAN Switching Command Reference</i> .
5. Enable MVRP on the port.	mvrp enable	By default, MVRP is disabled on a port.

Configuring the MVRP registration mode

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	<ul style="list-style-type: none"> • Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: interface <i>interface-type interface-number</i> • Enter port group view: port-group manual <i>port-group-name</i> 	Use one of the commands.
3. Configure the MVRP registration mode.	mvrp registration { fixed forbidden normal }	Optional. The default setting is normal registration mode.

Configuring MRP timers

⚠ CAUTION:

The MRP timers apply to all MRP applications, for example, MVRP, on a port. To avoid frequent VLAN registrations and deregistrations, use the same MRP timers throughout the network.

Each port maintains its own Periodic, Join, and LeaveAll timers, and each attribute of a port maintains a Leave timer.

To configure MRP timers:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter proper view.	<ul style="list-style-type: none">Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: interface <i>interface-type interface-number</i>Enter port group view: port-group manual <i>port-group-name</i>	Use one of the commands.
3. Configure the LeaveAll timer.	mrp timer leaveall <i>timer-value</i>	Optional. The default setting is 1000 centiseconds.
4. Configure the Join timer.	mrp timer join <i>timer-value</i>	Optional. The default setting is 20 centiseconds.
5. Configure the Leave timer.	mrp timer leave <i>timer-value</i>	Optional. The default setting is 60 centiseconds.
6. Configure the Periodic timer.	mrp timer periodic <i>timer-value</i>	Optional. The default setting is 100 centiseconds.

Table 1 shows the value ranges for Join, Leave, and LeaveAll timers and their dependencies.

- If you set a timer to a value beyond the allowed value range, your configuration will fail. To do that, you can change the allowed value range by tuning the value of another related timer.
- To restore the default settings of the timers, restore the Join timer first, followed by the Leave and LeaveAll timers.

Table 1 Dependencies of the Join, Leave, and LeaveAll timers

Timer	Lower limit	Upper limit
Join	20 centiseconds	Half the Leave timer
Leave	Twice the Join timer	LeaveAll timer
LeaveAll	Leave timer on each port	32760 centiseconds

You can restore the Periodic timer to the default at any time.

Enabling GVRP compatibility

⚠ CAUTION:

- MVRP with GVRP compatibility enabled can work together with STP or RSTP, but cannot work together with MSTP. When MVRP with GVRP compatibility enabled works with MSTP, the network might operate improperly.
- When GVRP compatibility is enabled for MVRP, HP recommends disabling the Period timer. Otherwise, the VLAN status might frequently change when the system is busy.

MVRP can be compatible with GVRP. When the peer device supports GVRP, you can enable GVRP compatibility on the local end, so that the local end can receive and send MVRP and GVRP protocol packets at the same time.

To enable GVRP compatibility:

Step	Command	Remarks
1. Enter system view	system-view	N/A
2. Enable GVRP compatibility	mvrp gvrp-compliance enable	By default, GVRP compatibility is disabled.

Displaying and maintaining MVRP

Task	Command	Remarks
Display the MVRP status of the specified port and each MVRP interface in the specified VLAN.	display mvrp state interface <i>interface-type interface-number vlan</i> <i>vlan-id [{ begin exclude include } regular-expression]</i>	Available in any view.
Display the MVRP running status.	display mvrp running-status [interface <i>interface-list] [{ begin exclude include } regular-expression]</i>	Available in any view.
Display the MVRP statistics.	display mvrp statistics [interface <i>interface-list] [{ begin exclude include } regular-expression]</i>	Available in any view.
Display the dynamic VLAN operation information of the specified port.	display mvrp vlan-operation interface <i>interface-type interface-number [{ begin exclude include } regular-expression]</i>	Available in any view.
Clear the MVRP statistics of the specified ports.	reset mvrp statistics [interface <i>interface-list]</i>	Available in user view.

Configuration example for MVRP in normal registration mode

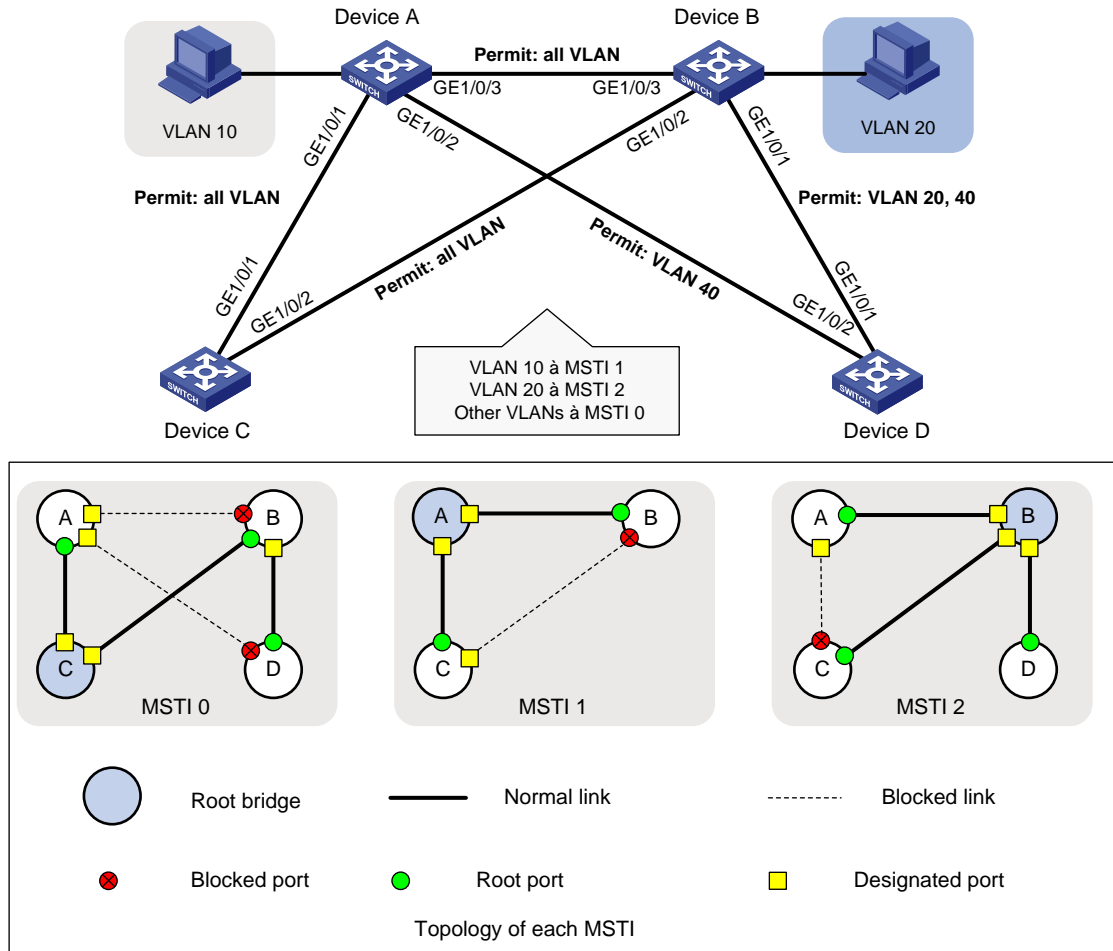
Network requirements

As shown in [Figure 5](#), configure MSTP, map VLAN 10 to MSTI 1, map VLAN 20 MST 2, and map the other VLANs to MSTI 0.

Configure MVRP and set the MVRP registration mode to normal, so that Device A, Device B, Device C, and Device D can register and deregister dynamic and static VLANs and keep identical VLAN configuration for each MSTI.

When the network is stable, set the MVRP registration mode to fixed on the port that connecting Device B to Device A, so that the dynamic VLANs on Device B are not de-registered.

Figure 5 Network diagram



Configuration procedure

Configuring Device A

Enter MST region view.

```
<DeviceA> system-view
[DeviceA] stp region-configuration
```

Configure the MST region name, VLAN-to-instance mappings, and revision level.

```
[DeviceA-mst-region] region-name example
[DeviceA-mst-region] instance 1 vlan 10
[DeviceA-mst-region] instance 2 vlan 20
[DeviceA-mst-region] revision-level 0
```

Manually activate the MST region configuration.

```
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

```

# Configure Device A as the primary root bridge of MSTI 1.
[DeviceA] stp instance 1 root primary

# Globally enable the spanning tree feature.
[DeviceA] stp enable

# Globally enable MVRP.
[DeviceA] mvrp global enable

# Configure port GigabitEthernet 1/0/1 as a trunk port, and configure it to permit all VLANs.
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan all

# Enable MVRP on port GigabitEthernet 1/0/1.
[DeviceA-GigabitEthernet1/0/1] mvrp enable
[DeviceA-GigabitEthernet1/0/1] quit

# Configure port GigabitEthernet1/0/2 as a trunk port, and configure it to permit VLAN 40.
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 40

# Enable MVRP on port GigabitEthernet1/0/2.
[DeviceA-GigabitEthernet1/0/2] mvrp enable
[DeviceA-GigabitEthernet1/0/2] quit

# Configure port GigabitEthernet 1/0/3 as a trunk port, and configure it to permit all VLANs.
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan all

# Enable MVRP on port GigabitEthernet 1/0/3.
[DeviceA-GigabitEthernet1/0/3] mvrp enable
[DeviceA-GigabitEthernet1/0/3] quit

# Create VLAN 10.
[DeviceA] vlan 10
[DeviceA-vlan10] quit

```

Configuring Device B

```

# Enter MST region view.
<DeviceB> system-view
[DeviceB] stp region-configuration

# Configure the MST region name, VLAN-to-instance mappings, and revision level.
[DeviceB-mst-region] region-name example
[DeviceB-mst-region] instance 1 vlan 10
[DeviceB-mst-region] instance 2 vlan 20
[DeviceB-mst-region] revision-level 0

# Manually activate the MST region configuration.
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit

# Configure Device B as the primary root bridge of MSTI 2.
[DeviceB] stp instance 2 root primary

# Globally enable the spanning tree feature.

```

```

[DeviceB] stp enable
# Globally enable MVRP.
[DeviceB] mvrp global enable
# Configure port GigabitEthernet 1/0/1 as a trunk port, and configure it to permit VLANs 20 and 40.
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 20 40
# Enable MVRP on port GigabitEthernet 1/0/1.
[DeviceB-GigabitEthernet1/0/1] mvrp enable
[DeviceB-GigabitEthernet1/0/1] quit
# Configure port GigabitEthernet1/0/2 as a trunk port, and configure it to permit all VLANs.
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan all
# Enable MVRP on port GigabitEthernet1/0/2.
[DeviceB-GigabitEthernet1/0/2] mvrp enable
[DeviceB-GigabitEthernet1/0/2] quit
# Configure port GigabitEthernet 1/0/3 as a trunk port, and configure it to permit all VLANs.
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan all
# Enable MVRP on port GigabitEthernet 1/0/3.
[DeviceB-GigabitEthernet1/0/3] mvrp enable
[DeviceB-GigabitEthernet1/0/3] quit
# Create VLAN 20.
[DeviceB] vlan 20
[DeviceB-vlan20] quit

```

Configuring Device C

```

# Enter MST region view.
<DeviceC> system-view
[DeviceC] stp region-configuration
# Configure the MST region name, VLAN-to-instance mappings, and revision level.
[DeviceC-mst-region] region-name example
[DeviceC-mst-region] instance 1 vlan 10
[DeviceC-mst-region] instance 2 vlan 20
[DeviceC-mst-region] revision-level 0
# Manually activate the MST region configuration.
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
# Configure Device C as the root bridge of MSTI 0.
[DeviceC] stp instance 0 root primary
# Globally enable the spanning tree feature.
[DeviceC] stp enable
# Globally enable MVRP.
[DeviceC] mvrp global enable

```

Configure port GigabitEthernet 1/0/1 as a trunk port, and configure it to permit all VLANs.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan all
```

Enable MVRP on port GigabitEthernet 1/0/1.

```
[DeviceC-GigabitEthernet1/0/1] mvrp enable
[DeviceC-GigabitEthernet1/0/1] quit
```

Configure port GigabitEthernet1/0/2 as a trunk port, and configure it to permit all VLANs.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan all
```

Enable MVRP on port GigabitEthernet1/0/2.

```
[DeviceC-GigabitEthernet1/0/2] mvrp enable
[DeviceC-GigabitEthernet1/0/2] quit
```

Configuring Device D

Enter MST region view.

```
<DeviceD> system-view
[DeviceD] stp region-configuration
```

Configure the MST region name, VLAN-to-instance mappings, and revision level.

```
[DeviceD-mst-region] region-name example
[DeviceD-mst-region] instance 1 vlan 10
[DeviceD-mst-region] instance 2 vlan 20
[DeviceD-mst-region] revision-level 0
```

Manually activate the MST region configuration.

```
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

Globally enable the spanning tree feature.

```
[DeviceD] stp enable
```

Globally enable MVRP.

```
[DeviceD] mvrp global enable
```

Configure port GigabitEthernet 1/0/1 as a trunk port, and configure it to permit VLANs 20 and 40.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 20 40
```

Enable MVRP on port GigabitEthernet 1/0/1.

```
[DeviceD-GigabitEthernet1/0/1] mvrp enable
[DeviceD-GigabitEthernet1/0/1] quit
```

Configure port GigabitEthernet1/0/2 as a trunk port, and configure it to permit VLAN 40.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 40
```

Enable MVRP on port GigabitEthernet1/0/2.

```
[DeviceD-GigabitEthernet1/0/2] mvrp enable[DeviceD-GigabitEthernet1/0/2] quit
```

Verifying the configuration

1. Verify the normal registration mode configuration.

Use the **display mvrp running-status** command to display the local MVRP VLAN information to verify whether the configuration takes effect.

Check the local VLAN information on Device A.

```
[DeviceA] display mvrp running-status
-----[MVRP Global Info]-----
Global Status      : Enabled
Compliance-GVRP    : False

----[GigabitEthernet1/0/1]----
Config Status      : Enabled
Running Status     : Enabled
Join Timer         : 20 (centiseconds)
Leave Timer         : 60 (centiseconds)
Periodic Timer     : 100 (centiseconds)
LeaveAll Timer      : 1000 (centiseconds)
Registration Type   : Normal
Local VLANs :
  1(default),

----[GigabitEthernet1/0/2]----
Config Status      : Enabled
Running Status     : Enabled
Join Timer         : 20 (centiseconds)
Leave Timer         : 60 (centiseconds)
Periodic Timer     : 100 (centiseconds)
LeaveAll Timer      : 1000 (centiseconds)
Registration Type   : Normal
Local VLANs :
  1(default),

----[GigabitEthernet1/0/3]----
Config Status      : Enabled
Running Status     : Enabled
Join Timer         : 20 (centiseconds)
Leave Timer         : 60 (centiseconds)
Periodic Timer     : 100 (centiseconds)
LeaveAll Timer      : 1000 (centiseconds)
Registration Type   : Normal
Local VLANs :
  1(default), 20,
```

The output shows that: ports GigabitEthernet 1/0/1 and GigabitEthernet1/0/2 have learned only VLAN 1 through MVRP; port GigabitEthernet 1/0/3 has learned VLAN 1 and dynamic VLAN 20 created on Device B through MVRP.

Check the local VLAN information on Device B.

```
[DeviceB] display mvrp running-status
-----[MVRP Global Info]-----
```



```
Global Status      : Enabled
Compliance-GVRP   : False
```

```
----[GigabitEthernet1/0/1]----
```

```
Config Status      : Enabled
Running Status     : Enabled
Join Timer         : 20 (centiseconds)
Leave Timer         : 60 (centiseconds)
Periodic Timer     : 100 (centiseconds)
LeaveAll Timer      : 1000 (centiseconds)
Registration Type   : Normal
Local VLANs :
  1(default),
```

```
----[GigabitEthernet1/0/2]----
```

```
Config Status      : Enabled
Running Status     : Enabled
Join Timer         : 20 (centiseconds)
Leave Timer         : 60 (centiseconds)
Periodic Timer     : 100 (centiseconds)
LeaveAll Timer      : 1000 (centiseconds)
Registration Type   : Normal
Local VLANs :
  1(default), 10,
```

```
----[GigabitEthernet1/0/3]----
```

```
Config Status      : Enabled
Running Status     : Enabled
Join Timer         : 20 (centiseconds)
Leave Timer         : 60 (centiseconds)
Periodic Timer     : 100 (centiseconds)
LeaveAll Timer      : 1000 (centiseconds)
Registration Type   : Normal
Local VLANs :
  1(default), 10,
```

The output shows that: port GigabitEthernet 1/0/1 has learned only VLAN 1 through MVRP; ports GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 have learned VLAN 1 and dynamic VLAN 10 created on Device A through MVRP.

Check the local VLAN information on Device C.

```
[DeviceC] display mvrp running-status
```

```
-----[MVRP Global Info]-----
```

```
Global Status      : Enabled
Compliance-GVRP   : False
```

```
----[GigabitEthernet1/0/1]----
```

```
Config Status      : Enabled
Running Status     : Enabled
Join Timer         : 20 (centiseconds)
Leave Timer         : 60 (centiseconds)
```

```

Periodic Timer                : 100 (centiseconds)
LeaveAll Timer                 : 1000 (centiseconds)
Registration Type              : Normal
Local VLANs :
    1(default), 10, 20,

```

```

----[GigabitEthernet1/0/2]----

```

```

Config Status                 : Enabled
Running Status                 : Enabled
Join Timer                     : 20 (centiseconds)
Leave Timer                     : 60 (centiseconds)
Periodic Timer                 : 100 (centiseconds)
LeaveAll Timer                  : 1000 (centiseconds)
Registration Type              : Normal
Local VLANs :
    1(default), 20,

```

The output shows that: port GigabitEthernet 1/0/1 has learned VLAN 1, dynamic VLAN 10 created on Device A, and dynamic VLAN 20 created on Device B through MVRP; port GigabitEthernet1/0/2 has learned VLAN 1 and dynamic VLAN 20 created on Device B through MVRP.

Check the local VLAN information on Device D.

```

[DeviceD] display mvrp running-status

```

```

-----[MVRP Global Info]-----

```

```

Global Status      : Enabled
Compliance-GVRP    : False

```

```

----[GigabitEthernet1/0/1]----

```

```

Config Status                 : Enabled
Running Status                 : Enabled
Join Timer                     : 20 (centiseconds)
Leave Timer                     : 60 (centiseconds)
Periodic Timer                 : 100 (centiseconds)
LeaveAll Timer                  : 1000 (centiseconds)
Registration Type              : Normal
Local VLANs :
    1(default), 20,

```

```

----[GigabitEthernet1/0/2]----

```

```

Config Status                 : Enabled
Running Status                 : Enabled
Join Timer                     : 20 (centiseconds)
Leave Timer                     : 60 (centiseconds)
Periodic Timer                 : 100 (centiseconds)
LeaveAll Timer                  : 1000 (centiseconds)
Registration Type              : Normal
Local VLANs :
    1(default),

```

The output shows that: port GigabitEthernet 1/0/1 has learned VLAN 1 and dynamic VLAN 20 created on Device B through MVRP; port GigabitEthernet1/0/2 has learned only VLAN 1 through MVRP.

2. Change the registration mode and verify the configuration.

Set the MVRP registration mode to fixed on GigabitEthernet 1/0/3 of Device B, so that the dynamic VLANs that Device B learns in VLAN 1 are not de-registered.

Set the MVRP registration mode to fixed on GigabitEthernet 1/0/3.

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] mvrp registration fixed
[DeviceB-GigabitEthernet1/0/3] quit
```

Display the local MVRP VLAN information on GigabitEthernet 1/0/3.

```
[DeviceB] display mvrp running-status interface gigabitethernet 1/0/3
-----[MVRP Global Info]-----
Global Status      : Enabled
Compliance-GVRP    : False

----[GigabitEthernet1/0/3]----
Config Status      : Enabled
Running Status     : Enabled
Join Timer         : 20 (centiseconds)
Leave Timer         : 60 (centiseconds)
Periodic Timer     : 100 (centiseconds)
LeaveAll Timer      : 1000 (centiseconds)
Registration Type   : Fixed
Local VLANs :
  1(default), 10,
```

The output shows that the VLAN information on GigabitEthernet 1/0/3 is not changed after you set the MVRP registration mode to fixed on GigabitEthernet 1/0/3.

Delete VLAN 10 on Device A.

```
[DeviceA] undo vlan 10
```

Display the local MVRP VLAN information on GigabitEthernet 1/0/3.

```
[DeviceB] display mvrp running-status interface gigabitethernet 1/0/3
-----[MVRP Global Info]-----
Global Status      : Enabled
Compliance-GVRP    : False

----[GigabitEthernet1/0/3]----
Config Status      : Enabled
Running Status     : Enabled
Join Timer         : 20 (centiseconds)
Leave Timer         : 60 (centiseconds)
Periodic Timer     : 100 (centiseconds)
LeaveAll Timer      : 1000 (centiseconds)
Registration Type   : Fixed
Local VLANs :
  1(default), 10,
```

The output shows that the dynamic VLAN information on GigabitEthernet 1/0/3 is not changed after you set the MVRP registration mode to fixed on GigabitEthernet 1/0/3.

Command reference

display mvrp running-status

Use **display mvrp running-status** to display the MVRP running status.

Syntax

display mvrp running-status [**interface** *interface-list*] [| { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

interface *interface-list*: Specifies an Ethernet interface list in the form of *interface-list* = { *interface-type interface-number1* [**to** *interface-type interface-number2*] }&<1-10>, where *interface-type interface-number* specifies an interface by its type and number and &<1-10> indicates that you can specify up to 10 *interface-type interface-number1* [**to** *interface-type interface-number2*] parameters. If this option is not specified, this command displays MVRP running status of all MVRP-enabled trunk ports.

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

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

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

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

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

Examples

Display the MVRP running status of all ports.

```
<Sysname> display mvrp running-status
-----[MVRP Global Info]-----
Global Status      : Enabled
Compliance-GVRP   : False

----[GigabitEthernet1/0/1]----
Config Status      : Enabled
Running Status     : Enabled
Join Timer         : 20 (centiseconds)
Leave Timer         : 60 (centiseconds)
Periodic Timer     : 100 (centiseconds)
LeaveAll Timer      : 1000 (centiseconds)
Registration Type   : Normal
Local VLANs :
  1(default), 2-10,
```

Table 2 Command output

Field	Description
MVRP Global Info	Global MVRP information.
Global Status	Global MVRP status: <ul style="list-style-type: none"> Enabled. Disabled.
Compliance-GVRP	GVRP compatibility status: <ul style="list-style-type: none"> True—Compatible. False—Incompatible.
---[GigabitEthernet1/0/1] ---	Interface prompt. The information between the current interface prompt and the next interface prompt is information about the current interface.
Config Status	Whether MVRP is enabled on the port: <ul style="list-style-type: none"> Enabled. Disabled.
Running Status	Whether MVRP takes effect on the port (determined by the link state and MVRP enabling status of the port): <ul style="list-style-type: none"> Enabled. Disabled.
Join Timer	Join timer, in centiseconds.
Leave Timer	Leave timer, in centiseconds.
Periodic Timer	Periodic timer, in centiseconds.
LeaveAll Timer	LeaveAll timer, in centiseconds.
Registration Type	MVRP registration mode: <ul style="list-style-type: none"> Fixed. Forbidden. Normal.
Local VLANs	VLAN information in the local database, which displays the VLANs learned through MVRP.

display mvrp state

Use **display mvrp state** to display the MVRP state of an interface in a VLAN.

Syntax

display mvrp state interface *interface-type interface-number* **vlan** *vlan-id* [| { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

0: Visit level

Parameters

interface *interface-type interface-number*: Displays the MVRP state of an interface specified by its type and number.

vlan *vlan-id*: Displays the MVRP state of an interface in an VLAN specified by its VLAN ID, which ranges from 1 to 4094.

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

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

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

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

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

Examples

Display the MVRP state of port GigabitEthernet 1/0/1 in VLAN 2.

```
<Sysname> display mvrp state interface gigabitethernet 1/0/1 vlan 2
```

MVRP state of VLAN 2 on port GE1/0/1

Port	VLAN	App-state	Reg-state
GE1/0/1	2	VP	IN

Table 3 Command output

Field	Description
MVRP state of VLAN 2 on port GE1/0/1	MVRP state of GigabitEthernet 1/0/1 in VLAN 2.
App-state	<p>Declaration state, which indicates the state of the attribute that the local participant declares to the remote participant. The state can be VO, VP, VN, AN, AA, QA, LA, AO, QO, AP, QP, or LO. Each state consists of two letters.</p> <p>The first letter indicates the state:</p> <ul style="list-style-type: none">• V—Very anxious, which means that the local participant has not declared the attribute or has not received any Join message containing the attribute.• A—Anxious, which means that the local participant has declared the attribute once or has received one Join message containing the attribute.• Q—Quiet, which means that the local participant has declared the attribute two times, the local participant has declared the attribute once and has received one Join message containing the attribute, or the local participant has received two Join messages containing the attribute.• L—Leaving, which means that the local participant is deregistering the attribute. <p>The second letter indicates the membership state:</p> <ul style="list-style-type: none">• A—Active member, which means that the local participant is declaring the attribute, has sent at least one Join message containing the attribute, and may receive Join messages.• P—Passive member, which means that the local participant is declaring the attribute, has received Join messages containing the attribute, but has not sent Join messages containing the attribute.• O—Observer, which means that the local participant is not declaring the attribute but is monitoring the attribute.• N—New, which means that the local participant is declaring the attribute, is receiving the Join message containing the attribute, but is not sending Join messages for the attribute. <p>For example, VP indicates "Very anxious, Passive member."</p>

Field	Description
Reg-state	<p>Registration state of attributes declared by remote participants on the local end. The state can be IN, LV, or MT:</p> <ul style="list-style-type: none"> • IN—Registered. • LV—Previously registered, but now being timed out. • MT—Not registered.

display mvrp statistics

Use **display mvrp statistics** to display MVRP statistics.

Syntax

```
display mvrp statistics [ interface interface-list ] [ | { begin | exclude | include } regular-expression ]
```

Views

Any view

Default command level

1: Monitor level

Parameters

interface *interface-list*: Specifies an Ethernet interface list in the form of *interface-list* = { *interface-type interface-number1* [**to** *interface-type interface-number2*] }&<1-10>, where *interface-type interface-number* specifies an interface by its type and number and &<1-10> indicates that you can specify up to 10 interfaces or interface ranges. If this option is not specified, this command displays MVRP statistics of all MVRP-enabled trunk ports.

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

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

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

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

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

Examples

Display MVRP statistics of all MVRP-enabled ports.

```
<Sysname> display mvrp statistics
```

```

----[GigabitEthernet1/0/1]----
Failed Registrations           : 1
Last PDU Origin                : 000f-e200-0010
Frames Received                 : 201
  New Event Received           : 0
  JoinIn Event Received        : 1167
  In Event Received            : 0
  JoinMt Event Received        : 22387
  Mt Event Received            : 31
  Leave Event Received         : 210
  LeaveAll Event Received      : 63
Frames Transmitted              : 47

```

```

New Event Transmitted           : 0
JoinIn Event Transmitted        : 311
In Event Transmitted            : 0
JoinMt Event Transmitted        : 873
Mt Event Transmitted            : 11065
Leave Event Transmitted          : 167
LeaveAll Event Transmitted       : 4
Frames Discarded                : 0

----[GigabitEthernet1/0/2]----
Failed Registrations           : 0
Last PDU Origin                : 0000-0000-0000
Frames Received                : 0
  New Event Received           : 0
  JoinIn Event Received        : 0
  In Event Received            : 0
  JoinMt Event Received        : 0
  Mt Event Received            : 0
  Leave Event Received         : 0
  LeaveAll Event Received      : 0
Frames Transmitted             : 0
  New Event Transmitted        : 0
  JoinIn Event Transmitted     : 0
  In Event Transmitted         : 0
  JoinMt Event Transmitted     : 0
  Mt Event Transmitted         : 0
  Leave Event Transmitted      : 0
  LeaveAll Event Transmitted   : 0
Frames Discarded               : 0

```

Table 4 Command output

Field	Description
----[GigabitEthernet1/0/1]----	Interface prompt. The statistics between the current interface prompt and the next interface prompt are statistics of the current interface.
Failed Registrations	Number of VLAN registration failures through MVRP on the local end.
Last PDU Origin	Source MAC address of the last MVRP PDU.
Frames Received	Number of MVRP protocol packets received.
New Event Received	Number of New attribute events received.
JoinIn Event Received	Number of JoinIn attribute events received.
In Event Received	Number of In attribute events received.
JoinMt Event Received	Number of JoinMt attribute events received.
Mt Event Received	Number of Mt attribute events received.
Leave Event Received	Number of Leave attribute events received.
LeaveAll Event Received	Number of LeaveAll attribute events received.

Field	Description
Frames Transmitted	Number of MVRP protocol packets sent.
New Event Transmitted	Number of New attribute events sent.
JoinIn Event Transmitted	Number of JoinIn attribute events sent.
In Event Transmitted	Number of In attribute events sent.
JoinMt Event Transmitted	Number of JoinMt attribute events sent.
Mt Event Transmitted	Number of Mt attribute events sent.
Leave Event Transmitted	Number of Leave attribute events sent.
LeaveAll Event Transmitted	Number of LeaveAll attribute events sent.
Frames Discarded	Number of MVRP protocol packets dropped.

display mvrp vlan-operation

Use **display mvrp vlan-operation** to display the dynamic VLAN operations of an interface.

Syntax

display mvrp vlan-operation interface *interface-type interface-number* [| { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

0: Visit level

Parameters

interface *interface-type interface-number*: Displays the dynamic VLAN operations of an interface specified its type and number.

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

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

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

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

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

Usage guidelines

These dynamic VLANs refer to the VLANs that are dynamically learned through MVRP and have not taken effect on the local device.

If a dynamic VLAN learned through MVRP is an existing static VLAN on the device or a VLAN reserved for a protocol, the dynamic VLAN does not take effect on the local device.

Examples

Display the dynamic VLAN operations of GigabitEthernet 1/0/1.

```
<Sysname> display mvrp vlan-operation interface gigabitethernet 1/0/1
Dynamic VLAN operations on port GigabitEthernet1/0/1
Operations of creating VLAN: 2-100
Operations of deleting VLAN: none
```

Operations of adding VLAN to Trunk: 2-100
Operations of deleting VLAN from Trunk: none

Table 5 Command output

Field	Description
Operations of adding VLAN to Trunk	Operations of adding VLANs to trunk ports.
Operations of deleting VLAN from Trunk	Operations of removing VLAN from trunk ports.

mrp timer join

Use **mrp timer join** to set the Join timer.

Use **undo mrp timer join** to restore the default.

Syntax

mrp timer join *timer-value*

undo mrp timer join

Default

The Join timer is 20 centiseconds.

Views

Layer 2 Ethernet port view, Layer 2 aggregate interface view, port group view

Default command level

2: System level

Parameters

timer-value: Specifies the Join timer value (in centiseconds). The Join timer must be less than half the Leave timer, and must be a multiple of 20.

Usage guidelines

You will fail to restore the default Join timer if the default Join timer is not less than half the Leave timer.

Examples

Set the Join timer to 40 centiseconds. (Suppose the Leave timer is 100 centiseconds)

```
<Sysname> system-view
```

```
[Sysname] interface ethernet 1/1
```

```
[Sysname-GigabitEthernet1/0/1] mrp timer join 40
```

Related commands

- **display mvrp running-status**
- **mrp timer leave**

mrp timer leave

Use **mrp timer leave** to set the Leave timer.

Use **undo mrp timer leave** to restore the default.

Syntax

mrp timer leave *timer-value*

undo mrp timer leave

Default

The Leave timer is 60 centiseconds.

Views

Layer 2 Ethernet port view, Layer 2 aggregate interface view, port group view

Default command level

2: System level

Parameters

timer-value: Specifies the Leave timer value (in centiseconds). The Leave timer must be greater than two times the Join timer, less than the LeaveAll timer, and a multiple of 20.

Usage guidelines

You will fail to restore the default Leave timer if the default Leave timer is not greater than two times the Join timer or not less than the LeaveAll timer.

Examples

Set the Leave timer to 100 centiseconds. (Suppose the Join and LeaveAll timer use their default settings)

```
<Sysname> system-view
```

```
[Sysname] interface ethernet 1/1
```

```
[Sysname-GigabitEthernet1/0/1] mrp timer leave 100
```

Related commands

- **display mvrp running-status**
- **mrp timer join**
- **mrp timer leaveall**

mrp timer leaveall

Use **mrp timer leaveall** to set the LeaveAll timer.

Use **undo mrp timer leaveall** to restore the default.

Syntax

mrp timer leaveall *timer-value*

undo mrp timer leaveall

Default

The LeaveAll timer is 1000 centiseconds.

Views

Layer 2 Ethernet port view, Layer 2 aggregate interface view, port group view

Default command level

2: System level

Parameter

timer-value: Specifies the LeaveAll timer value (in centiseconds). The LeaveAll timer must be greater than any Leave timer on each port, no greater than 32760, and a multiple of 20.

Usage guidelines

You will fail to restore the default LeaveAll timer if the default LeaveAll timer is not greater than any Leave timer on each port.

Each time when the LeaveAll timer of a port expires, all attributes of the MSTIs on the port are deregistered throughout the network, and such a deregistration affects a large portion of the network. Do not set too small a value for the LeaveAll timer, and make sure the LeaveAll timer is greater than any Leave timer on each port.

To keep the dynamic VLANs learned through MVRP stable, do not set the LeaveAll timer smaller than its default value (1000 centiseconds).

To avoid the case that the LeaveAll timer of a fixed participant always first expires, the switch randomly changes the LeaveAll timer within a certain range when the MRP participant restarts its LeaveAll timer.

Examples

Set the LeaveAll timer to 1500 centiseconds. (Suppose the Leave timer is restored to the default)

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-GigabitEthernet1/0/1] mrp timer leaveall 1500
```

Related commands

- **display mvrp running-status**
- **mrp timer leave**

mrp timer periodic

Use **mrp timer periodic** to set the Periodic timer.

Use **undo mrp timer periodic** to restore the default.

Syntax

mrp timer periodic *timer-value*

undo mrp timer periodic

Default

The Periodic timer is 100 centiseconds.

Views

Layer 2 Ethernet port view, Layer 2 aggregate interface view, port group view

Default command level

2: System level

Parameters

timer-value: Specifies the Periodic timer (in centiseconds), which can be 0 or 100.

Usage guidelines

Setting the Periodic timer to 0 centiseconds disables the Periodic timer.

Setting the Periodic timer to 100 centiseconds enables the Periodic timer.

Examples

Set the Periodic timer to 0 centiseconds.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
```

```
[Sysname-GigabitEthernet1/0/1] mvrp timer periodic 0
```

Related commands

display mvrp running-status

mvrp global enable

Use **mvrp global enable** to enable MVRP globally.

Use **undo mvrp global enable** to restore the default.

Syntax

mvrp global enable

undo mvrp global enable

Default

MVRP is disabled globally.

Views

System view

Default command level

2: System level

Usage guidelines

Disabling MVRP globally also disables MVRP on all ports.

Examples

```
# Enable MVRP globally.
```

```
<Sysname> system-view
```

```
[Sysname] mvrp global enable
```

Related commands

- **display mvrp running-status**
- **mvrp enable**

mvrp enable

Use **mvrp enable** to enable MVRP on a port.

Use **undo mvrp enable** to disable MVRP on a port.

Syntax

mvrp enable

undo mvrp enable

Default

MVRP is disabled on a port.

Views

Layer 2 Ethernet port view, Layer 2 aggregate interface view, port group view

Default command level

2: System level

Usage guidelines

To enable MVRP on a port, first enable MVRP globally.

Disabling MVRP globally also disables MVRP on each port.

This command is available only on trunk ports.

You cannot change the link type of MVRP-enabled trunk port.

Examples

Configure GigabitEthernet 1/0/1 as a trunk port, and enable MVRP on it.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk permit vlan all
[Sysname-GigabitEthernet1/0/1] mvrp enable
```

Related commands

- **display mvrp running-status**
- **mvrp global enable**

mvrp gvrp-compliance

Use **mvrp gvrp-compliance enable** to enable GVRP compatibility, so that the device can process both MVRP protocol packets and GVRP protocol packets.

Use **undo mvrp gvrp-compliance enable** to restore the default.

Syntax

mvrp gvrp-compliance enable
undo mvrp gvrp-compliance enable

Default

GVRP compatibility is disabled.

Views

System view

Default command level

2: System level

Examples

Enable GVRP compatibility.

```
<Sysname> system-view
[Sysname] mvrp gvrp-compliance enable
```

mvrp registration

Use **mvrp registration** to set the MVRP registration mode on the port.

Use **undo mvrp registration** to restore the default.

Syntax

mvrp registration { fixed | forbidden | normal }
undo mvrp registration

Default

The MVRP registration mode is normal.

Views

Layer 2 Ethernet port view, Layer 2 aggregate interface view, port group view

Default command level

2: System level

Parameters

fixed: Specifies the fixed registration mode.

forbidden: Specifies the forbidden registration mode.

normal: Specifies the normal registration mode.

Usage guidelines

This command is available only on trunk ports.

Examples

Configure GigabitEthernet 1/0/1 as a trunk port, and set the MVRP registration mode to fixed on the port.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk permit vlan all
[Sysname-GigabitEthernet1/0/1] mvrp registration fixed
```

Related commands

display mvrp running-status

reset mvrp statistics

Use **reset mvrp statistics** to clear the MVRP statistics of ports.

Syntax

reset mvrp statistics [**interface** *interface-list*]

Views

User view

Default command level

2: System level

Parameters

interface *interface-list*: Specifies an Ethernet interface list in the form of *interface-list* = { *interface-type interface-number1* [**to** *interface-type interface-number2*] }&<1-10>, where *interface-type interface-number* specifies an interface by its type and number and &<1-10> indicates that you can specify up to 10 interfaces or interface ranges. If this option is not specified, the command clears MVRP statistics of all ports.

Examples

Clear the MVRP statistics of all ports.

```
<Sysname> reset mvrp statistics
```

Related commands

display mvrp statistics

New feature: Portal authentication in IPv6 networks

Configuring portal authentication for an IPv6 network

The following portal authentication features are supported in an IPv6 network:

Tasks at a glance
Specifying an IPv6 portal server for portal authentication
Configuring an IPv6 portal-free rule
Specifying a source IPv6 subnet for portal authentication
Specifying an authentication domain for IPv6 portal users
Specifying a source IPv6 address for outgoing IPv6 portal packets
Logging off an IPv6 portal user

Specifying an IPv6 portal server for portal authentication

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Specify an IPv6 portal server.	portal server <i>server-name</i> ipv6 <i>ipv6-address</i> [key [cipher simple] <i>key-string</i> port <i>port-id</i> url <i>url-string</i>] *	By default, no IPv6 portal server is specified.

Configuring an IPv6 portal-free rule

Step	Command
1. Enter system view.	system-view
2. Configure an IPv6 portal-free rule.	portal free-rule <i>rule-number</i> { destination { any ipv6 { <i>ipv6-address</i> <i>prefix-length</i> any } } source { any [interface <i>interface-type</i> <i>interface-number</i> ipv6 { <i>ipv6-address</i> <i>prefix-length</i> any } mac <i>mac-address</i> vlan <i>vlan-id</i>] * } } *

Specifying a source IPv6 subnet for portal authentication

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Specify a source IPv6 subnet.	portal auth-network ipv6 <i>ipv6-network-address</i> <i>prefix-length</i>	Optional. By default, the source IPv6 subnet is ::/0, which means that users from any IPv6 subnet must pass portal authentication to access network resources.

Specifying an authentication domain for IPv6 portal users

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Specify an authentication domain for IPv6 portal users on the interface.	portal domain ipv6 <i>domain-name</i>	By default, no authentication domain is specified for IPv6 portal users.

Specifying a source IPv6 address for outgoing IPv6 portal packets

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Specify a source IPv6 address for outgoing IPv6 portal packets on the interface.	portal nas-ip ipv6 <i>ipv6-address</i>	By default, no source IPv6 address is specified and the IPv6 address of the user logon interface is used as the source IPv6 address for outgoing IPv6 portal packets.

Logging off an IPv6 portal user

Step	Command
1. Enter system view.	system-view
2. Log off an IPv6 portal user.	portal delete-user ipv6 <i>ipv6-address</i>

IPv6 portal authentication commands

portal auth-network ipv6

Use **portal auth-network ipv6** to configure a source IPv6 subnet for portal authentication on an interface. You can use this command to configure multiple source IPv6 subnets on an interface. Then, only HTTP packets from these IPv6 subnets can trigger portal authentication on the interface. If an unauthenticated user is not on any authentication source IPv6 subnet, the access device discards all the user's HTTP packets that do not match any portal-free rule.

Use **undo portal auth-network ipv6** to remove a specific source IPv6 subnet for portal authentication.

Syntax

portal auth-network ipv6 *ipv6-network-address prefix-length*

undo portal auth-network ipv6 *ipv6-network-address*

Default

The source IPv6 subnet for portal authentication is `::/0`, meaning that users in all IPv6 subnets must pass portal authentication.

Views

Interface view

Default command level

2: System level

Parameters

ipv6 *ipv6-network-address*: Specifies an authentication source IPv6 subnet address.

prefix-length: IPv6 address prefix length, in the range of 0 to 128.

Examples

Configure a portal authentication source subnet of 2011::1/64 on interface VLAN-interface 2 to allow only users from subnet 2011::1/64 to trigger portal authentication.

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 2
```

```
[Sysname-Vlan-interface2] portal auth-network ipv6 2011::1 64
```

portal delete-user ipv6

Use **portal delete-user** to log off an IPv6 portal user.

Syntax

portal delete-user ipv6 *ipv6-address*

Views

System view

Default command level

2: System level

Parameters

ipv6 *ipv6-address*: Logs off the portal user with the specified IPv6 address.

Examples

```
# Log off the portal user whose IPv6 address is 2011::1.
<Sysname> system-view
[Sysname] portal delete-user ipv6 2011::1
```

portal domain ipv6

Use **portal domain ipv6** to specify an authentication domain for IPv6 portal users on an interface. Then, the switch uses the authentication domain for authentication, authorization and accounting (AAA) of the IPv6 portal users on the interface.

Use **undo portal domain ipv6** to delete the authentication domain specified for IPv6 portal users.

Syntax

portal domain ipv6 *domain-name*

undo portal domain ipv6

Default

No authentication domain is specified for IPv6 portal users on an interface.

Views

Interface view

Default command level

2: System level

Parameters

ipv6: Specifies IPv6 portal users.

domain-name: Specifies an authentication domain name, a case-insensitive string of 1 to 24 characters. The domain specified by this argument must already exist.

Examples

```
# Configure the authentication domain for IPv6 portal users on VLAN-interface 100 as my-domain.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal domain ipv6 my-domain
```

portal free-rule ipv6

Use **portal free-rule ipv6** to configure an IPv6 portal-free rule and specify the source filtering criteria, destination filtering criteria, or both.

Use **undo portal free-rule** to remove a specific portal-free rule or all portal-free rules.

Syntax

portal free-rule *rule-number* { **destination** { **any** | **ipv6** { *ipv6-address* *prefix-length* | **any** } } | **source** { **any** | [**interface** *interface-type* *interface-number* | **ipv6** { *ipv6-address* *prefix-length* | **any** } | **mac** *mac-address* | **vlan** *vlan-id*] * } } *

undo portal free-rule { *rule-number* | **all** }

Views

System view

Default command level

2: System level

Parameters

rule-number: Number for the portal-free rule.

any: Imposes no limitation on the previous keyword.

ipv6 *ipv6-address*: Specifies an IPv6 address for the portal-free rule.

prefix-length: Specifies the prefix length of the IPv6 address, in the range of 0 to 128.

interface *interface-type interface-number*: Specifies a source interface.

mac *mac-address*: Specifies a source MAC address in the format H-H-H.

vlan *vlan-id*: Specifies a source VLAN ID.

all: Specifies all portal-free rules.

Usage guidelines

If you specify both a source IPv6 address and a source MAC address in a portal-free rule, the IPv6 address must be a host address with a 128-bit prefix. Otherwise, the specified MAC address does not take effect.

Examples

Configure a portal-free rule, allowing any packet whose source IPv6 address is 2011::1/64 to bypass portal authentication.

```
<Sysname> system-view
```

```
[Sysname] portal free-rule 15 source ipv6 2011::1 64 destination ipv6 any
```

portal nas-ip ipv6

Use **portal nas-ip ipv6** to configure an interface to use a specific source IPv6 address for outgoing IPv6 portal packets.

Use **undo portal nas-ip ipv6** to delete the specified source IPv6 address.

Syntax

portal nas-ip ipv6 *ipv6-address*

undo portal nas-ip ipv6

Default

No source IPv6 address is specified for outgoing IPv6 portal packets on an interface. The switch uses the IP address of the user logon interface as the source IPv6 address for outgoing IPv6 portal packets.

Views

Interface view

Default command level

2: System level

Parameters

ipv6 *ipv6-address*: Specifies a source IPv6 address for outgoing portal packets. This IPv6 address must be a local IPv6 address, but cannot be a multicast address, an all 0 address, or a link-local address.

Examples

Configure interface VLAN-interface 5 to use 2011::2 as the source IPv6 address for outgoing portal packets.

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 5
```

```
[Sysname-Vlan-interface5] portal nas-ip ipv6 2011::2
```

portal server ipv6

Use **portal server** *server-name* **ipv6** to configure an IPv6 portal server for portal authentication.

Use **undo portal server** to remove an portal server, restore the default destination port and default URL address, or delete the shared key.

Syntax

portal server *server-name* **ipv6** *ipv6-address* [**key** [**cipher** | **simple**] *key-string* | **port** *port-id* | **url** *url-string*] *

undo portal server *server-name* [**key** | **port** | **url**]

Default

No IPv6 portal server is configured for portal authentication.

Views

System view

Default command level

2: System level

Parameters

server-name: Configures a name for the specified portal server, a case-sensitive string of 1 to 32 characters.

ipv6 *ipv6-address*: Specifies a portal server by its IPv6 address.

key: Specifies a shared key for communication with the portal server. Portal packets exchanged between the access device and the portal server carry an authenticator, which is generated with the shared key. The receiver uses the authenticator to check the correctness of the received portal packets.

cipher: Sets a ciphertext shared key.

simple: Sets a plaintext shared key.

key-string: Specifies the shared key. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **simple** nor **cipher** is specified, you set a plaintext shared key.

port *port-id*: Specifies the destination port number used when the device sends an unsolicited message to the portal server, in the range of 1 to 65534. The default is 50100.

url *url-string*: Specifies the uniform resource locator (URL) to which HTTP packets are to be redirected. The default URL is in the `http://ip-address` format, where *ip-address* is the IP address of the portal server. You can also specify the domain name of the portal server, in which case you must use the **portal free-rule** command to configure the IP address of the DNS server as a portal authentication-free destination IP address.

Examples

Configure portal server **pts**, setting the IPv6 address to **2011::1**, the key to plaintext string **portal**, and the redirection URL to **http://2011::1/portal**.

```
<Sysname> system-view
```

```
[Sysname] portal server pts ipv6 2011::1 key simple portal url http://[2011::1]portal
```

New feature: SCP

Overview

Secure copy (SCP) is based on SSH2.0 and offers a secure approach to copying files.

SCP uses SSH connections for copying files. The switch can act as the SCP server, allowing a user to log in to the switch for file upload and download. The switch can also act as an SCP client, enabling a user to log in from the switch to a remote server for secure file transfer.

NOTE:

When the switch acts as an SCP server, only one of all the FTP, SFTP and SCP users can access the switch.

Configuring the switch as an SCP server

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the SSH server.	For more information, see the security guide for your switch.	N/A
3. Create an SSH user for a SCP client, set the service type to all or scp , and specify the authentication method.	ssh user <i>username</i> service-type { all scp } authentication-type { password { any password-publickey publickey } assign publickey <i>keyname</i> work-directory <i>directory-name</i> }	N/A
4. Create a user account and assign a working directory for the SSH user on the switch or a remote server if password authentication is used.	<ul style="list-style-type: none">On the remote server (details not shown)On the switch:<ul style="list-style-type: none">a. local-userb. passwordc. service-type sshd. authorization-attribute work-directory <i>directory-name</i>	<p>Skip this step if publickey authentication, whether with password authentication or not, is used.</p> <p>Make sure that the local user account has the name <i>username</i> as the username specified in the ssh user command.</p>

When you set the working directory for the user, follow these guidelines:

- If only password authentication is used, the working directory specified in the **ssh user** command does not take effect. You must set the working directory on the remote server or in the local user account for the SSH user.
- If publickey authentication, whether with password authentication or not, is used, you must set the working directory in the **ssh user** command.

Configuring the switch as the SCP client

To upload or download files to or from an SCP server, perform the following tasks in any view:

Task	Command
Upload a file to an SCP server.	<ul style="list-style-type: none"> Upload a file to the IPv4 SCP server: <code>scp server [port-number] put source-file-path [destination-file-path] [identity-key { dsa rsa } prefer-ctos-cipher { 3des aes128 des } prefer-ctos-hmac { md5 md5-96 sha1 sha1-96 } prefer-kex { dh-group-exchange dh-group1 dh-group14 } prefer-stoc-cipher { 3des aes128 des } prefer-stoc-hmac { md5 md5-96 sha1 sha1-96 }] *</code> Upload a file to the IPv6 SCP server: <code>scp ipv6 server [port-number] put source-file-path [destination-file-path] [identity-key { dsa rsa } prefer-ctos-cipher { 3des aes128 des } prefer-ctos-hmac { md5 md5-96 sha1 sha1-96 } prefer-kex { dh-group-exchange dh-group1 dh-group14 } prefer-stoc-cipher { 3des aes128 des } prefer-stoc-hmac { md5 md5-96 sha1 sha1-96 }] *</code>
Download a file from an SCP server.	<ul style="list-style-type: none"> Download a file from the remote IPv4 SCP server: <code>scp server [port-number] get source-file-path [destination-file-path] [identity-key { dsa rsa } prefer-ctos-cipher { 3des aes128 des } prefer-ctos-hmac { md5 md5-96 sha1 sha1-96 } prefer-kex { dh-group-exchange dh-group1 dh-group14 } prefer-stoc-cipher { 3des aes128 des } prefer-stoc-hmac { md5 md5-96 sha1 sha1-96 }] *</code> Download a file from the remote IPv6 SCP server: <code>scp ipv6 server [port-number] get source-file-path [destination-file-path] [identity-key { dsa rsa } prefer-ctos-cipher { 3des aes128 des } prefer-ctos-hmac { md5 md5-96 sha1 sha1-96 } prefer-kex { dh-group-exchange dh-group1 dh-group14 } prefer-stoc-cipher { 3des aes128 des } prefer-stoc-hmac { md5 md5-96 sha1 sha1-96 }] *</code>

NOTE:

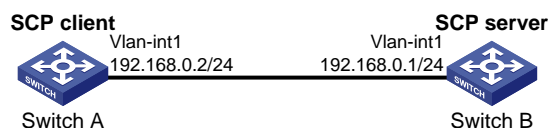
File transfer interruption during a downloading process can result in file fragments on the switch. You must manually delete them.

SCP client configuration example

Network requirements

As shown in Figure 6, switch A acts as a client and download the file **remote.bin** from switch B. The user has the username **test** and uses the password authentication method.

Figure 6 Network diagram



Configuration procedure

Create VLAN-interface 1 and assign an IP address to it.

```

<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 192.168.0.2 255.255.255.0
[SwitchA-Vlan-interface1] quit

```

Download the file **remote.bin** from the SCP server, and save it with the file name **local.bin**.

```

<SwitchA> scp 192.168.0.1 get remote.bin local.bin
Username: test
Trying 192.168.0.1 ...

```

```
The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
Enter password:
18471 bytes transfered in 0.001 seconds.
```


Configure an IP address for VLAN-interface 1, which the client will use as the destination for SSH connection.

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.1.45 255.255.255.0
[Switch-Vlan-interface1] quit
```

Set the authentication mode of the user interfaces to AAA.

```
[Switch] user-interface vty 0 15
[Switch-ui-vty0-15] authentication-mode scheme
```

Enable the user interfaces to support all protocols including SSH.

```
[Switch-ui-vty0-15] protocol inbound all
[Switch-ui-vty0-15] quit
```

Create the local user **test** and specify a working directory for the user.

```
[Switch] local-user test
[Switch-luser-test] password simple aabbcc
[Switch-luser-test] service-type ssh
[Switch-luser-test] authorization-attribute work-directory flash:/
[Switch-luser-test] quit
```

Configure the SSH user authentication method as **password** and service type as **scp**.

```
[Switch] ssh user test service-type scp authentication-type password
```

Command reference

scp

Use **scp** to transfer files with an SCP server.

Syntax

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

Views

User view

Default command level

3: Manage level

Parameters

ipv6: Specifies the type of the server as IPv6. If this keyword is not specified, the server is an IPv4 server.

server: Specifies an IPv4 or IPv6 address or host name of the server. For an IPv4 server, it is a case-insensitive string of 1 to 20 characters. For an IPv6 server, it is a case-insensitive string of 1 to 46 characters.

port-number: Specifies the port number of the server, in the range of 0 to 65535. The default is 22.

identity-key: Specifies the algorithm for publickey authentication, either **dsa** or **rsa**. The default is **dsa**.

- **dsa**: Specifies the publickey algorithm **dsa**.
- **rsa**: Specifies the publickey algorithm **rsa**.

prefer-ctos-cipher: Preferred encryption algorithm from client to server, defaulted to **aes128**.

- **3des**: Encryption algorithm 3des-cbc.
- **aes128**: Encryption algorithm aes128-cbc.
- **des**: Encryption algorithm des-cbc.

prefer-ctos-hmac: Preferred HMAC algorithm from client to server, defaulted to **sha1-96**.

- **md5**: HMAC algorithm hmac-md5.
- **md5-96**: HMAC algorithm hmac-md5-96.
- **sha1**: HMAC algorithm hmac-sha1.
- **sha1-96**: HMAC algorithm hmac-sha1-96.

prefer-kex: Preferred key exchange algorithm, defaulted to **dh-group-exchange**.

- **dh-group-exchange**: Key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1**: Key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14**: Key exchange algorithm diffie-hellman-group14-sha1.

prefer-stoc-cipher: Preferred encryption algorithm from server to client, defaulted to **aes128**.

prefer-stoc-hmac: Preferred HMAC algorithm from server to client, defaulted to **sha1-96**.

Usage guidelines

When the client's authentication method is **publickey**, the client needs to get the local private key for digital signature. As the **publickey** authentication includes RSA and DSA algorithms, you must specify an algorithm (by using the **identity-key** keyword) in order to get the correct data for the local private key. By default, the **publickey** algorithm is DSA.

Examples

Download the file **remote.bin** from the SCP server, save it locally and change the file name to **local.bin**

```
<Sysname> scp 192.168.0.1 get remote.bin local.bin
```

ssh user

Use **ssh user** to create an SSH user and specify the service type and authentication method.

Use **undo ssh user** to delete an SSH user.

Syntax

```
ssh user username service-type stelnet authentication-type { password | { any | password-publickey | publickey } assign publickey keyname }
```

```
ssh user username service-type { all | scp | sftp } authentication-type { password | { any | password-publickey | publickey } assign publickey keyname work-directory directory-name }
```

```
undo ssh user username
```

Views

System view

Default command level

3: Manage level

Parameters

username: SSH username, a case-sensitive string of 1 to 80 characters.

service-type: Specifies the service type of an SSH user, which can be one of the following:

- **all**: Specifies Stelnet, SFTP, and SCP.
- **scp**: Specifies the service type as secure copy.

- **sftp**: Specifies the service type as secure FTP.
- **stelnet**: Specifies the service type of secure Telnet.

authentication-type: Specifies the authentication method of an SSH user, which can be one of the following:

- **password**: Performs password authentication. This authentication method features easy and fast encryption, but it is vulnerable. It can work with AAA to implement user authentication, authorization, and accounting.
- **any**: Performs either password authentication or publickey authentication.
- **password-publickey**: Performs both password authentication and publickey authentication (featuring higher security) if the client runs SSH2, and performs either type of authentication if the client runs SSH1.
- **publickey**: Performs publickey authentication. This authentication method has the downside of complicated and slow encryption, but it provides strong authentication that can defend against brute-force attacks. This authentication method is easy to use. Once it is configured, the authentication process completes automatically without the need of remembering or entering any password.

assign publickey keyname: Assigns an existing public key to an SSH user. The *keyname* argument indicates the name of the client public key and is a string of 1 to 64 characters.

work-directory directory-name: Specifies the working directory for an SCP or SFTP user. The *directory-name* argument indicates the name of the working directory and is a string of 1 to 135 characters.

Usage guidelines

For a publickey authentication user, you must configure the username and the public key on the switch. For a password authentication user, you can configure the account information on either the switch or the remote authentication server, such as a RADIUS server.

If you use the **ssh user** command to configure a public key for a user who has already had a public key, the new one overwrites the old one.

You can change the authentication method and public key of an SSH user when the user is communicating with the SSH server. However, your changes take effect only after the user logs out and logs in again.

If an SCP or SFTP user has been assigned a public key, it is necessary to set a working folder for the user.

The working folder of an SCP or SFTP user depends on the user authentication method. For a user using only password authentication, the working folder is the AAA authorized one. For a user using only publickey authentication or using both publickey authentication and password authentication, the working folder is the one set by using the **ssh user** command.

Examples

Create an SSH user named **user1**, setting the service type as **scp**, the authentication method as **publickey**, the working directory of the SCP server as **flash:/**, and assigning a public key named **key1** to the user.

```
<Sysname> system-view
```

```
[Sysname] ssh user user1 service-type scp authentication-type publickey assign publickey key1 work-directory flash:/
```

Related commands

display ssh user-information

New feature: FIPS

Overview

Federal Information Processing Standards (FIPS), developed by the National Institute of Standard and Technology (NIST) of the United States, specify the requirements for cryptography modules. FIPS 140-2 defines four levels of security, simply named "Level 1" to "Level 4" from low to high. Currently, the switch supports Level 2.

Unless otherwise noted, *FIPS* in the document refers to FIPS 140-2.

FIPS self-tests

When the device operates in FIPS mode, it has self-test mechanisms, including the power-up self-test and conditional self-tests, to ensure the normal operation of cryptography modules. You can also trigger a self-test. If a self-test fails, the device restarts.



CAUTION:

If the switch reboots repeatedly, it might be caused by software failures or hardware damages. Contact technical support engineers to upgrade the software or repair the damaged hardware.

Power-up self-test

The power-up self-test, also called "known-answer test", examines the availability of FIPS-allowed cryptographic algorithms. A cryptographic algorithm is run on data for which the correct output is already known. The calculated output is compared with the known answer. If they are not identical, the known-answer test fails.

Conditional self-tests

A conditional self-test runs when an asymmetrical cryptographic module or a random number generator module is invoked. Conditional self-tests include the following types:

- **Pair-wise consistency test**—This test is run when a DSA/RSA asymmetrical key-pair is generated. It uses the public key to encrypt a plain text, and uses the private key to decrypt the encrypted text. If the decryption is successful, the test succeeds. Otherwise, the test fails.
- **Continuous random number generator test**—This test is run when a random number is generated in FIPS mode. If two consecutive random numbers are different, the test succeeds. Otherwise, the test fails.

Triggering a self-test

To examine whether the cryptography modules operate normally, you can use a command to trigger a self-test on the cryptographic algorithms. The triggered self-test is the same as the power-up self-test.

If the self-test fails, the device automatically reboots.

Configuring FIPS

To configure FIPS, complete the following tasks:

1. Remove the existing key pairs and certificates.
2. Enable the FIPS mode.

3. Enable the password control function.
4. Configure local user attributes (including local username, service type, password, and so on) on the switch.
5. Save the configuration.

After you finish the above configurations, reboot the switch. The switch works in FIPS mode that complies with the FIPS 140-2 standard after it starts up. For Common Criteria (CC) evaluation in FIPS mode, the switch also works in a operating mode that complies with the CC standard.

The switch does not support an upgrade from a FIPS-incompatible version to a FIPS-compatible version.

Enabling the FIPS mode

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the FIPS mode.	fips mode enable	Disabled by default.

After you enable the FIPS mode and reboot the switch, the switch works in FIPS mode after it starts up and the following changes occur.

- FTP/TFTP is disabled.
- Telnet is disabled.
- The HTTP server is disabled.
- SNMPv1 and SNMPv2c are disabled. Only SNMPv3 is available.
- The SSL server only supports TLS1.0.
- The SSH server does not support SSHv1 clients
- SSH only supports RSA.
- The generated RSA key pairs must have a modulus length of 2048 bits. The generated DSA key pair must have a modulus of at least 1024 bits.
- SSH, SNMPv3, IPsec and SSL do not support DES, 3DES, RC4, or MD5.

Triggering a self-test

To examine whether the cryptography modules operate normally, you can use a command to trigger a self-test on the cryptographic algorithms. The triggered self-test is the same as the power-up self-test.

If the self-test fails, the device automatically reboots.

To trigger a self-test:

Task	Command
1. Enter system view.	system-view
2. Trigger a self-test.	fips self-test

Displaying and maintaining FIPS

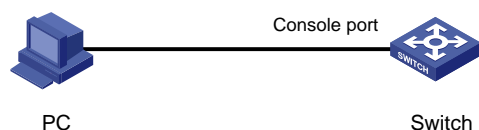
Task	Command	Remarks
Display FIPS mode state	display fips status	Available in any view.

FIPS configuration example

Network requirements

PC connects to Switch through a console port. Configure Switch to operate in FIPS mode and create a local user for PC so that PC can log in to the switch.

Figure 8 Network diagram



Configuration procedure

1. Configure Switch:

Enable the FIPS mode.

```
<Sysname> system-view
```

```
[Sysname] fips mode enable
```

Enable the password control function.

```
[Sysname] password-control enable
```

Create a local user named **test**, and set its service type as **terminal**, privilege level as **3**, and password as **AAbbcc1234%**. The password is a string of at least 10 characters by default and must contain both uppercase and lowercase letters, digits, and special characters.

```
[Sysname] local-user test
```

```
[Sysname-luser-test] service-type terminal
```

```
[Sysname-luser-test] authorization-attribute level 3
```

```
[Sysname-luser-test] password
```

```
Password:*****
```

```
Confirm :*****
```

```
Updating user(s) information, please wait.....
```

```
[Sysname-luser-test] quit
```

Save the configuration.

```
[Sysname] save
```

```
The current configuration will be written to the device. Are you sure? [Y/N]:y
```

```
Please input the file name(*.cfg)[flash:/startup.cfg]
```

```
(To leave the existing filename unchanged, press the enter key):
```

```
flash:/startup.cfg exists, overwrite? [Y/N]:y
```

```
Validating file. Please wait.....
```

```
Saved the current configuration to mainboard device successfully.
```

```
Configuration is saved to device successfully.
```

```
[Sysname] quit
```

Reboot the switch.

```
<Sysname> reboot
```

CAUTION:

After you enable the FIPS mode, be sure to create a local user and its password before you reboot the switch. Otherwise, you cannot log in to the switch. If you cannot log in to the switch, reboot the switch without the configuration file (by ignoring or removing the configuration file) so that the switch works in non-FIPS mode, and then make correct configurations.

2. Verify the configuration:

After the switch reboots, enter the username (test) and password (AAbbcc1234%). The system prompts that your first login is successful, and asks you to enter a new password. Enter a new password which has at least four characters different than the previous one and confirm the password. Then, the system displays the <Sysname> prompt.

User interface aux0 is available.

Please press ENTER.

Login authentication

Username:test

Password:

Info: First logged in. For security reasons you will need to change your password.

Please enter your new password.

Password:*****

Confirm :*****

Updating user(s) information, please wait.....

<Sysname>

Display the current FIPS mode. You can see that the FIPS mode is enabled.

<Sysname> display fips status

FIPS mode is enabled

Command reference

fips mode enable

Use **fips mode enable** to enable the FIPS mode.

Use **undo fips mode enable** to disable the FIPS mode.

Syntax

fips mode enable

undo fips mode enable

Default

The FIPS mode is disabled.

Views

System view

Default command level

2: System level

Parameters

None

Usage guidelines

After you enable the FIPS mode, reboot the switch to make your configuration effective. After the switch starts up, the switch works in FIPS mode. The FIPS mode complies with the FIPS 140-2 standard.

Examples

```
# Enable the FIPS mode.
<Sysname> system-view
[Sysname] fips mode enable
```

Related commands

display fips status

display fips status

Use **display fips status** to display the current FIPS mode.

Syntax

display fips status

Views

Any view

Default command level

1: Monitor level

Examples

```
# Display the current FIPS mode.
<Sysname> display fips status
FIPS mode is enabled
```

Related commands

fips mode enable

fips self-test

Use **fips self-test** to trigger a self-test on the password algorithms.

Syntax

fips self-test

Views

System view

Default command level

3: Manage level

Usage guidelines

To examine whether the cryptography modules operate normally, you can use a command to trigger a self-test on the cryptographic algorithms. The triggered self-test is the same as the power-up self-test.

If the self-test fails, the device automatically reboots.

Examples

```
# Trigger a self-test on the cryptographic algorithms.
```



```
<Sysname> fips self-test
Self-tests are running. Please wait...
Self-tests succeeded.
```

New feature: Configuring ACL-based IPsec

NOTE:

- The term *router* in this document refers to both routers and switches.
 - IKE configuration is available for only the switches in FIPS mode. For information about the FIPS mode, see [New feature: FIPS](#).
 - A switch in IRF mode does not support IPsec automatic negotiation.
-

Configuring ACL-based IPsec

ACL-based IPsec configuration task list

The following is the generic configuration procedure for implementing ACL-based IPsec:

1. Configure ACLs for identifying data flows to be protected.
2. Configure IPsec proposals to specify the security protocols, authentication and encryption algorithms, and encapsulation mode.
3. Configure IPsec policies to associate data flows with IPsec proposals and specify the SA negotiation mode, the peer IP addresses (the start and end points of the IPsec tunnel), the required keys, and the SA lifetime.
4. Apply the IPsec policies to interfaces to finish IPsec configuration.

To configure ACL-based IPsec:

Task	Remarks
Configuring ACLs	Required. Basic IPsec configuration.
Configuring an IPsec proposal	
Configuring an IPsec policy	
Applying an IPsec policy group to an interface	
Configuring the IPsec session idle timeout	Optional.
Enabling ACL checking of de-encapsulated IPsec packets	Optional.
Configuring the IPsec anti-replay function	Optional.
Configuring packet information pre-extraction	Optional.

CAUTION:

Typically, IKE uses UDP port 500 for communication, and AH and ESP use the protocol numbers 51 and 50 respectively. Make sure that flows of these protocols are not denied on the interfaces with IKE or IPsec configured.

Configuring ACLs

ACLs can be used to identify traffic. They are widely used in scenarios where traffic identification is desired, such as QoS and IPsec.

Keywords in ACL rules

IPsec uses ACLs to identify data flows. An ACL is a collection of ACL rules. Each ACL rule is a deny or permit statement. A permit statement identifies a data flow protected by IPsec, and a deny statement identifies a data flow that is not protected by IPsec. With IPsec, a packet is matched against the referenced ACL rules and processed according to the first rule that it matches:

- Each ACL rule matches both the outbound traffic and the returned inbound traffic. Suppose there is a rule **rule 0 permit ip source 1.1.1.0 0.0.0.255 destination 2.2.2.0 0.0.0.255**. This rule matches both traffic from 1.1.1.0 to 2.2.2.0 and traffic from 2.2.2.0 to 1.1.1.0.
- In the outbound direction, if a permit statement is matched, IPsec considers that the packet requires protection and continues to process it. If a deny statement is matched or no match is found, IPsec considers that the packet does not require protection and delivers it to the next function module.
- In the inbound direction:
 - Normal IP packets that match a permit statement are dropped.
 - IPsec packets that match a permit statement and are destined for the device itself are de-encapsulated and matched against the rule again. Only those that match a permit statement are processed by IPsec.

When you configure an ACL for IPsec, follow these guidelines:

- Permit only data flows that need to be protected and use the **any** keyword with caution. With the **any** keyword specified in a permit statement, all outbound traffic matching the permit statement will be protected by IPsec and all inbound IPsec packets matching the permit statement will be received and processed, but all inbound non-IPsec packets will be dropped. This will cause the inbound traffic that does not need IPsec protection to be all dropped.
- Avoid statement conflicts in the scope of IPsec policy groups. When creating a deny statement, be careful with its matching scope and matching order relative to permit statements. The policies in an IPsec policy group have different match priorities. ACL rule conflicts between them are prone to cause mistreatment of packets. For example, when configuring a permit statement for an IPsec policy to protect an outbound traffic flow, you must avoid the situation that the traffic flow matches a deny statement in a higher priority IPsec policy. Otherwise, the packets will be sent out as normal packets; if they match a permit statement at the receiving end, they will be dropped by IPsec.
- An ACL can be specified for only one IPsec policy. ACLs referenced by IPsec policies cannot be used by other services.
- You must create a mirror image ACL rule at the remote end for each ACL rule created at the local end. Otherwise, IPsec may protect traffic in only one direction.

The following configuration example shows how an improper statement causes unexpected packet dropping. Only the ACL-related configurations are presented.

Router A connects the segment 1.1.2.0/24 and Router B connects the segment 3.3.3.0/24. On Router A, apply the IPsec policy group **test** to the outbound interface of Router A. The IPsec policy group contains two policies, **test 1** and **test 2**. The ACLs referenced by the two policies each contain a rule that matches traffic from 1.1.2.0/24 to 3.3.3.0/24. The one referenced in policy **test 1** is a deny statement and the one referenced in policy **test 2** is a permit statement. Because **test 1** is matched prior to **test 2**, traffic from 1.1.2.0/24 to 3.3.3.0/24 will match the deny statement and sent as normal traffic. When the traffic arrives at Router B, it will be dropped if it matches a permit statement in the ACL referenced in the applied IPsec policy.

- Configurations on Router A:

```
acl number 3000
 rule 0 permit ip source 1.1.1.0 0.0.0.255 destination 2.2.2.0 0.0.0.255
 rule 1 deny ip
acl number 3001
 rule 0 permit ip source 1.1.2.0 0.0.0.255 destination 3.3.3.0 0.0.0.255
```

```

rule 1 deny ip
#
ipsec policy test 1 isakmp
security acl 3000
ike-peer aa
proposal 1
#
ipsec policy test 2 isakmp
security acl 3001
ike-peer bb
proposal 1

```

- **Configurations on Router B:**

```

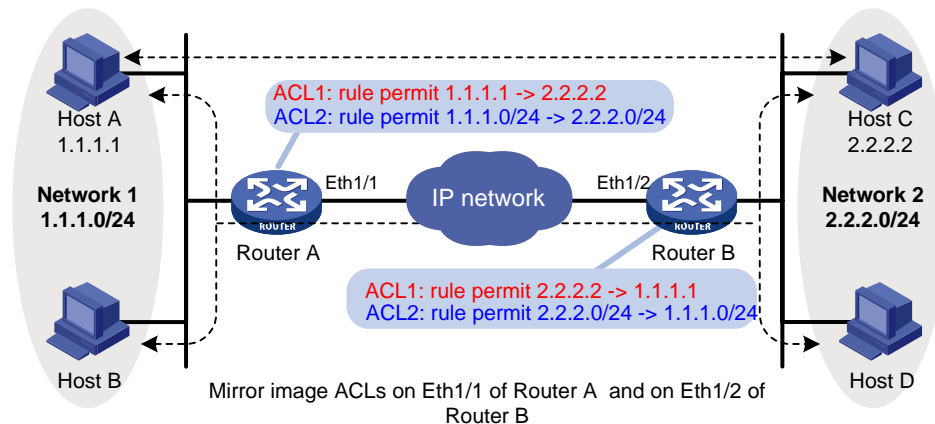
acl number 3001
rule 0 permit ip source 3.3.3.0 0.0.0.255 destination 1.1.2.0 0.0.0.255
rule 1 deny ip
#
ipsec policy test 1 isakmp
security acl 3001
ike-peer aa
proposal 1

```

Mirror image ACLs

To make sure SAs can be set up and the traffic protected by IPsec can be processed correctly at the remote peer, on the remote peer, create a mirror image ACL rule for each ACL rule created at the local peer. As shown in [Figure 9](#), ACL rules on Router B are mirror images of the rules on Router A. This makes sure that SAs can be created successfully for the traffic between Host A and Host C and the traffic between Network 1 and Network 2.

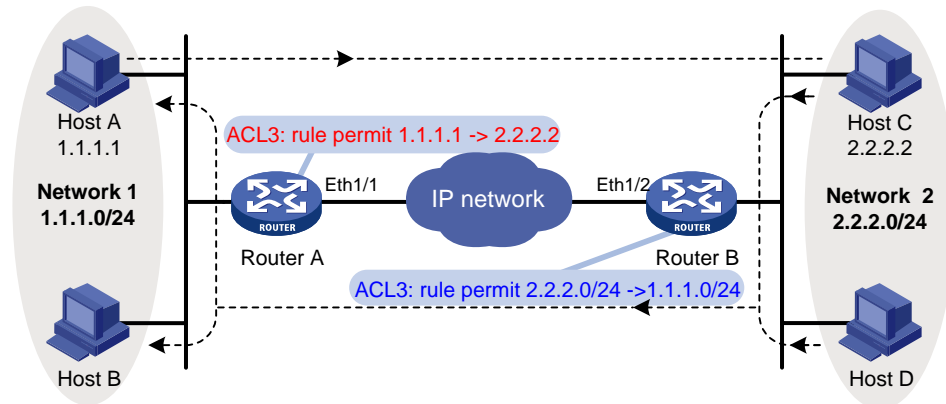
Figure 9 Mirror image ACLs



If the ACL rules on peers do not form mirror images of each other, SAs can be set up only when both of the following requirements are met:

- The range specified by an ACL rule on one peer is covered by its counterpart ACL rule on the other peer. As shown in [Figure 10](#), the range specified by the ACL rule configured on Router A is covered by its counterpart on Router B.
- The peer with the narrower rule initiates SA negotiation. If a wider ACL rule is used by the SA initiator, the negotiation request may be rejected because the matching traffic is beyond the scope of the responder. As shown in [Figure 10](#), the SA negotiation initiated by Host A to Host C is accepted but the SA negotiations from Host C to Host B or from Host D to Host A is rejected.

Figure 10 Non-mirror image ACLs



Protection modes

The switch supports IPsec for data flows in standard mode. In standard mode, one tunnel protects one data flow. The data flow permitted by an ACL rule is protected by one tunnel that is established solely for it.

For more information about ACL configuration, see *ACL and QoS Configuration Guide*.

NOTE:

To use IPsec in combination with QoS, make sure IPsec's ACL classification rules match the QoS classification rules. If the rules do not match, QoS may classify the packets of one IPsec SA to different queues, causing packets to be sent out of order. When the anti-replay function is enabled, IPsec will discard the packets beyond the anti-replay window in the inbound direction, resulting in packet loss. For more information about QoS classification rules, see *ACL and QoS Configuration Guide*.

Configuring an IPsec proposal

This section is not newly added. In this version, related commands that are executed in FIPS mode were modified.

An IPsec proposal, part of an IPsec policy or an IPsec profile, defines the security parameters for IPsec SA negotiation, including the security protocol, the encryption and authentication algorithms, and the encapsulation mode.

To configure an IPsec proposal:

Step	Command	Remarks
1. Enter system view	system-view	N/A
2. Create an IPsec proposal and enter its view	ipsec proposal <i>proposal-name</i>	By default, no IPsec proposal exists.
3. Specify the security protocol for the proposal	transform { <i>ah</i> <i>ah-esp</i> <i>esp</i> }	Optional. ESP by default.

Step	Command	Remarks
4. Specify the security algorithms	<ul style="list-style-type: none"> Specify the encryption algorithm for ESP: <ul style="list-style-type: none"> In non-FIPS mode: esp encryption-algorithm { 3des aes [key-length] des } In FIPS mode: esp encryption-algorithm aes [key-length] Specify the authentication algorithm for ESP: <ul style="list-style-type: none"> In non-FIPS mode: esp authentication-algorithm { md5 sha1 } In FIPS mode: esp authentication-algorithm sha1 Specify the authentication algorithm for AH: <ul style="list-style-type: none"> In non-FIPS mode: ah authentication-algorithm { md5 sha1 } In FIPS mode: ah authentication-algorithm sha1 	<p>Optional.</p> <p>For ESP, the default encryption algorithm is DES in non-FIPS mode and is AES-128 in FIPS mode.</p> <p>For ESP and AH, the default authentication algorithm is MD5 in non-FIPS mode and is SHA1 in FIPS mode.</p>
5. Specify the IP packet encapsulation mode for the IPsec proposal	encapsulation-mode { transport tunnel }	<p>Optional.</p> <p>Tunnel mode by default.</p> <p>Transport mode applies only when the source and destination IP addresses of data flows match those of the IPsec tunnel.</p> <p>IPsec for IPv6 routing protocols supports only the transport mode.</p>

NOTE:

- Changes to an IPsec proposal affect only SAs negotiated after the changes. To apply the changes to existing SAs, execute the **reset ipsec sa** command to clear the SAs so that they can be set up using the updated parameters.
- Only when a security protocol is selected, can you configure security algorithms for it. For example, you can specify the ESP-specific security algorithms only when you select ESP as the security protocol. ESP supports three IP packet protection schemes: encryption only, authentication only, or both encryption and authentication. For the CC evaluation in FIPS mode, you must use both ESP encryption and authentication.

Configuring an IPsec policy

IPsec policies define which IPsec proposals should be used to protect which data flows. An IPsec policy is uniquely identified by its name and sequence number.

IPsec policies fall into two categories:

- Manual IPsec policy**—The parameters are configured manually, such as the keys, the SPIs, and the IP addresses of the two ends in tunnel mode.
- IPsec policy that uses IKE**—The parameters are automatically negotiated through IKE.

This section is not newly added. In this version, IKE negotiation was added and related commands that are executed in FIPS mode were modified. For more information, see "[Command reference](#)."

Configuring a manual IPsec policy

To guarantee successful SA negotiations, follow these guidelines when configuring manual IPsec policies at the two ends of an IPsec tunnel:

- The IPsec policies at the two ends must have IPsec proposals that use the same security protocols, security algorithms, and encapsulation mode.
- The remote IP address configured on the local end must be the same as the IP address of the remote end.
- At each end, configure parameters for both the inbound SA and the outbound SA and make sure that different SAs use different SPIs.
- The local inbound SA must use the same SPI and keys as the remote outbound SA. The same is true of the local outbound SA and remote inbound SA.
- The keys for the local and remote inbound and outbound SAs must be in the same format. For example, if the local inbound SA uses a key in characters, the local outbound SA and remote inbound and outbound SAs must use keys in characters.

Follow these guidelines when you configure an IPsec policy for an IPv6 routing protocol:

- You do not need to configure ACLs or IPsec tunnel addresses.
- Within a certain routed network scope, the IPsec proposal referenced by the IPsec policies on all devices must use the same security protocol, security algorithm, and packet encapsulation, and the SAs on all devices must use the same SPI and keys. For OSPFv3, the scope can be directly connected neighbors or an OSPFv3 area. For RIPng, the scope can be directly connected neighbors or a RIPng process. For IPv6 BGP, the scope can be directly connected neighbors or a peer group.
- All SAs (both inbound and outbound) within the routed network scope must use the same SPI and keys.
- Configure the keys on all routers within the routed network scope in the same format. For example, if you enter the keys in hexadecimal format on one router, do so across the routed network scope.

Before you configure a manual IPsec policy, configure ACLs used for identifying protected traffic and IPsec proposals. ACLs are not required for IPsec policies for an IPv6 protocol.

When you configure a manual IPsec policy, follow these guidelines:

- An IPsec policy can reference only one ACL. If you apply multiple ACLs to an IPsec policy, only the last one takes effect.
- A manual IPsec policy can reference only one IPsec proposal. To change an IPsec proposal for an IPsec policy, you must remove the proposal reference first.
- At each end, configure parameters for both the inbound and the outbound SAs, and make sure different SAs use different SPIs.
- If you configure a key in two modes: string and hexadecimal, the last configured one is used.
- You cannot change the creation mode of an IPsec policy from manual to through IKE, or vice versa. To create an IPsec policy that uses IKE, delete the manual IPsec policy, and then use IKE to configure an IPsec policy.

To configure a manual IPsec policy:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a manual IPsec policy and enter its view.	ipsec policy <i>policy-name seq-number manual</i>	By default, no IPsec policy exists.

Step	Command	Remarks
3. Assign an ACL to the IPsec policy.	security acl <i>acl-number</i>	Not needed for IPsec policies to be applied to IPv6 routing protocols and required for other applications. By default, an IPsec policy references no ACL. The ACL supports match criteria of the VPN attribute.
4. Assign an IPsec proposal to the IPsec policy.	proposal <i>proposal-name</i>	By default, an IPsec policy references no IPsec proposal.
5. Configure the two ends of the IPsec tunnel.	<ul style="list-style-type: none"> Configure the local address of the tunnel: tunnel local <i>ip-address</i> Configure the remote address of the tunnel: tunnel remote <i>ip-address</i> 	Configuring the local address of the tunnel is not needed for IPsec policies to be applied to IPv6 routing protocols and required for other applications. Configuring the remote address of the tunnel is required. Both the local and remote addresses are not configured by default.
6. Configure the SPIs for the SAs.	sa spi { inbound outbound } { ah esp } <i>spi-number</i>	By default, SPIs for the SAs do not exist.
7. Configure keys for the SAs.	<ul style="list-style-type: none"> Configure an authentication key in hexadecimal: sa authentication-hex { inbound outbound } { ah esp } [cipher simple] <i>hex-key</i> Configure an authentication key in characters: sa string-key { inbound outbound } { ah esp } [cipher simple] <i>string-key</i> Configure a key in characters for ESP: sa string-key { inbound outbound } esp <i>string-key</i> Configure an encryption key in hexadecimal for ESP: sa encryption-hex { inbound outbound } esp [cipher simple] <i>hex-key</i> 	Use either command. For ESP, if you configure an authentication key, the system automatically generates an authentication key and an encryption key. If you configure an encryption key in characters for ESP, the system automatically generates an authentication key and an encryption key for ESP. The sa string-key command is not supported in FIPS mode.

Configuring an IPsec policy that uses IKE (only in FIPS mode)

To configure an IPsec policy that uses IKE, directly configure it by configuring the parameters in IPsec policy view.

Before you configure an IPsec policy that uses IKE, configure the ACLs and the IKE peer for the IPsec policy. For more information about IKE configuration, see the chapter "IKE configuration."

The parameters for the local and remote ends must match.

When you configure an IPsec policy that uses IKE, follow these guidelines:

- An IPsec policy can reference only one ACL. If you apply multiple ACLs to an IPsec policy, only the last one takes effect.
- With SAs to be established through IKE negotiation, an IPsec policy can reference up to six IPsec proposals. During negotiation, IKE searches for a fully matched IPsec proposal at the two ends of the expected IPsec tunnel. If no match is found, no SA can be set up and the packets expecting to be protected will be dropped.
- During IKE negotiation for an IPsec policy with PFS enabled, an additional key exchange is performed. If the local end uses PFS, the remote end must also use PFS for negotiation and both ends must use the same Diffie-Hellman (DH) group; otherwise, the negotiation will fail.
- An SA uses the global lifetime settings when it is not configured with lifetime settings in IPsec policy view. When negotiating to set up SAs, IKE uses the local lifetime settings or those proposed by the peer, whichever are smaller.
- You cannot change the creation mode of an IPsec policy directly. To create an IPsec policy in another creation mode, delete the current one and then configure a new IPsec policy.

To directly configure an IPsec policy that uses IKE:

Step	Command	Remark
1. Enter system view.	system-view	N/A
2. Create an IPsec policy that uses IKE and enter its view.	ipsec policy <i>policy-name</i> <i>seq-number isakmp</i>	By default, no IPsec policy exists.
3. Configure an IPsec connection name.	connection-name <i>name</i>	Optional. By default, no IPsec connection name is configured.
4. Assign an ACL to the IPsec policy.	security acl <i>acl-number</i>	By default, an IPsec policy references no ACL.
5. Assign IPsec proposals to the IPsec policy.	proposal <i>proposal-name</i> &<1-6>	By default, an IPsec policy references no IPsec proposal.
6. Specify an IKE peer for the IPsec policy.	ike-peer <i>peer-name</i>	An IPsec policy cannot reference any IKE peer that is already referenced by an IPsec profile, and vice versa.
7. Enable and configure the perfect forward secrecy feature for the IPsec policy.	pfs { dh-group2 dh-group5 dh-group14 }	Optional. By default, the PFS feature is not used for negotiation. For more information about PFS, see the chapter "IKE configuration."
8. Set the SA lifetime.	sa duration { time-based seconds traffic-based kilobytes }	Optional. By default, the global SA lifetime is used.
9. Enable the IPsec policy.	policy enable	Optional. Enabled by default.
10. Return to system view.	quit	N/A

Step	Command	Remark
11. Set the global SA lifetime.	ipsec sa global-duration { time-based <i>seconds</i> traffic-based <i>kilobytes</i> }	Optional. 3600 seconds for time-based SA lifetime by default. 1843200 kilobytes for traffic-based SA lifetime by default.

Applying an IPsec policy group to an interface

This feature is supported only in FIPS mode.

An IPsec policy group is a collection of IPsec policies with the same name but different sequence numbers. In an IPsec policy group, an IPsec policy with a smaller sequence number has a higher priority.

You can apply an IPsec policy group to a logical or physical interface to protect certain data flows. To cancel the IPsec protection, remove the application of the IPsec policy group.

For each packet to be sent out an IPsec protected interface, the system looks through the IPsec policies in the IPsec policy group in ascending order of sequence numbers. If an IPsec policy matches the packet, the system uses the IPsec policy to protect the packet. If no match is found, the system sends the packet out without IPsec protection.

To apply an IPsec policy group to an interface:

Step	Command
1. Enter system view.	system-view
2. Enter interface view.	interface <i>interface-type interface-number</i>
3. Apply an IPsec policy group to the interface.	ipsec policy <i>policy-name</i>

NOTE:

- IPsec policies can be applied only to VLAN interfaces and Layer 3 Ethernet interfaces on the switch.
- An interface can reference only one IPsec policy group. An IPsec policy can be applied to only one interface.

Configuring the IPsec session idle timeout

This feature is supported only in FIPS mode.

An IPsec session is created when the first packet matching an IPsec policy arrives. Also created is an IPsec session entry, which records the quintuplet (source IP address, destination IP address, protocol number, source port, and destination port) and the matched IPsec tunnel.

An IPsec session is automatically deleted after the idle timeout expires.

Subsequent data flows search the session entries according to the quintuplet to find a matched item. If found, the data flows are processed according to the tunnel information; otherwise, they are processed according to the original IPsec process: search the policy group or policy at the interface, and then the matched tunnel.

The session processing mechanism of IPsec saves intermediate matching procedures, improving the IPsec forwarding efficiency.

To set the IPsec session idle timeout:

Step	Command	Remark
1. Enter system view.	system-view	N/A
2. Set the IPsec session idle timeout.	ipsec session idle-time <i>seconds</i>	Optional. 300 seconds by default.

Enabling ACL checking of de-encapsulated IPsec packets

This feature is supported only in FIPS mode.

In tunnel mode, the IP packet that was encapsulated in an inbound IPsec packet may not be an object that is specified by an ACL to be protected. For example, a forged packet is not an object to be protected. If you enable ACL checking of de-encapsulated IPsec packets, all packets failing the checking will be discarded, improving the network security.

To enable ACL checking of de-encapsulated IPsec packets:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable ACL checking of de-encapsulated IPsec packets.	ipsec decrypt check	Optional. Enabled by default.

Configuring the IPsec anti-replay function

This feature is supported only in FIPS mode.

The IPsec anti-replay function protects networks against anti-replay attacks by using a sliding window mechanism called anti-replay window. This function checks the sequence number of each received IPsec packet against the current IPsec packet sequence number range of the sliding window. If the sequence number is not in the current sequence number range, the packet is considered a replayed packet and is discarded.

IPsec packet de-encapsulation involves complicated calculation. De-encapsulation of replayed packets not only makes no sense, but also consumes large amounts of resources and degrades performance, resulting in DoS. IPsec anti-replay checking, when enabled, is performed before the de-encapsulation process, reducing resource waste.

In some cases, however, the sequence numbers of some normal service data packets may be out of the current sequence number range, and the IPsec anti-replay function may drop them as well, affecting the normal communications. If this happens, disable IPsec anti-replay checking or adjust the size of the anti-replay window as required.

To configure IPsec anti-replay checking:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable IPsec anti-replay checking.	ipsec anti-replay check	Optional. Enabled by default.
3. Set the size of the IPsec anti-replay window.	ipsec anti-replay window <i>width</i>	Optional. 32 by default.

⚠ CAUTION:

- IPsec anti-replay checking is enabled by default. Do not disable it unless it needs to be disabled.
- A wider anti-replay window results in higher resource cost and more system performance degradation, which is against the original intention of the IPsec anti-replay function. Specify an anti-replay window size that is as small as possible.

NOTE:

IPsec anti-replay checking does not affect manually created IPsec SAs. According to the IPsec protocol, only IPsec SAs negotiated by IKE support anti-replay checking.

Configuring packet information pre-extraction

This feature is supported only in FIPS mode.

If you apply both an IPsec policy and QoS policy to an interface, by default, the interface first uses IPsec and then QoS to process IP packets, and QoS classifies packets by the headers of IPsec-encapsulated packets. If you want QoS to classify packets by the headers of the original IP packets, enable the packet information pre-extraction feature.

For more information about QoS policy and classification, see *ACL and QoS Configuration Guide*.

To configure packet information pre-extraction:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPsec policy view.	ipsec policy <i>policy-name</i> <i>seq-number</i> [isakmp manual]	Configure either command.
3. Enable packet information pre-extraction.	qos pre-classify	Disabled by default.

Displaying and maintaining IPsec

To do...	Use the command...	Remarks
Display IPsec policy information	display ipsec policy [brief name <i>policy-name</i> [<i>seq-number</i>]] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display IPsec proposal information	display ipsec proposal [<i>proposal-name</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display IPsec SA information	display ipsec sa [brief policy <i>policy-name</i> [<i>seq-number</i>] remote <i>ip-address</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display IPsec session information	display ipsec session [tunnel-id <i>integer</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view Only supported in FIPS mode.
Display IPsec packet statistics	display ipsec statistics [tunnel-id <i>integer</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view

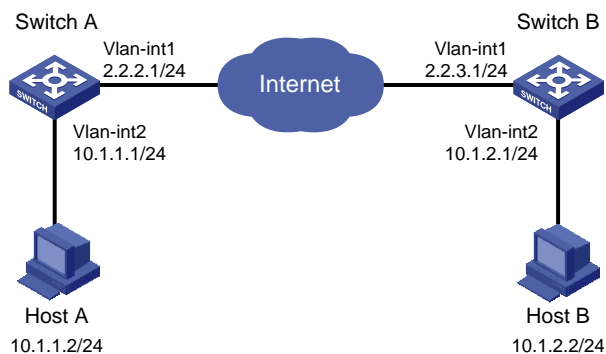
To do...	Use the command...	Remarks
Display IPsec tunnel information	display ipsec tunnel [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Clear SAs	reset ipsec sa [parameters <i>dest-address protocol spi</i> policy <i>policy-name [seq-number]</i> remote <i>ip-address</i>]	Available in user view
Clear IPsec sessions	reset ipsec session [tunnel-id <i>integer</i>]	Available in user view Only supported in FIPS mode.
Clear IPsec statistics	reset ipsec statistics	Available in user view

IKE-based IPsec tunnel for IPv4 packets configuration example

Network requirements

As shown in Figure 11, configure an IPsec tunnel between Switch A and Switch B to protect data flows between subnet 10.1.1.0/24 and subnet 10.1.2.0/24. Configure the tunnel to use the security protocol ESP, the encryption algorithm AES-CBC-128, and the authentication algorithm HMAC-SHA1-96.

Figure 11 Network diagram



Configuration procedure

1. Configure Switch A:

Assign IP addresses to VLAN-interface 1 and VLAN-interface 2.

```
<SwitchA> system-view
```

```
[SwitchA] interface vlan-interface 1
```

```
[SwitchA-Vlan-interface1] ip address 2.2.2.1 255.255.255.0
```

```
[SwitchA-Vlan-interface1] quit
```

```
[SwitchA] interface vlan-interface 2
```

```
[SwitchA-Vlan-interface2] ip address 10.1.1.1 255.255.255.0
```

```
[SwitchA-Vlan-interface2] quit
```

Configure a static route to Host B.

```
[SwitchA] ip route-static 10.1.2.0 255.255.255.0 vlan-interface 1
```

Define an ACL to identify data flows from subnet 10.1.1.0/24 to subnet 10.1.2.0/24.

```
[SwitchA] acl number 3101
```

```
[SwitchA-acl-adv-3101] rule 0 permit ip source 10.1.1.0 0.0.0.255 destination  
10.1.2.0 0.0.0.255
```

```

[SwitchA-acl-adv-3101] rule 5 permit ip source 10.1.2.0 0.0.0.255 destination
10.1.1.0 0.0.0.255
[SwitchA-acl-adv-3101] quit
# Create an IPsec proposal named tran1.
[SwitchA] ipsec proposal tran1
# Specify the encapsulation mode as tunnel.
[SwitchA-ipsec-proposal-tran1] encapsulation-mode tunnel
# Specify the security protocol as ESP.
[SwitchA-ipsec-proposal-tran1] transform esp
# Specify the algorithms for the proposal.
[SwitchA-ipsec-proposal-tran1] esp encryption-algorithm aes 128
[SwitchA-ipsec-proposal-tran1] esp authentication-algorithm sha1
[SwitchA-ipsec-proposal-tran1] quit
# Configure the IKE peer.
[SwitchA] ike peer peer
[SwitchA-ike-peer-peer] pre-shared-key Ab12<><>
[SwitchA-ike-peer-peer] remote-address 2.2.3.1
[SwitchA-ike-peer-peer] quit
# Create an IPsec policy that uses IKE for IPsec SA negotiation.
[SwitchA] ipsec policy map1 10 isakmp
# Apply the IPsec proposal.
[SwitchA-ipsec-policy-isakmp-map1-10] proposal tran1
# Apply the ACL.
[SwitchA-ipsec-policy-isakmp-map1-10] security acl 3101
# Apply the IKE peer.
[SwitchA-ipsec-policy-isakmp-map1-10] ike-peer peer
[SwitchA-ipsec-policy-isakmp-map1-10] quit
# Apply the IPsec policy group to VLAN-interface 1.
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ipsec policy map1

```

2. Configure Switch B:

```

# Assign IP addresses to VLAN-interface 1 and VLAN-interface 2.
<SwitchB> system-view
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 2.2.3.1 255.255.255.0
[SwitchB-Vlan-interface1] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 10.1.2.1 255.255.255.0
[SwitchB-Vlan-interface2] quit
# Configure a static route to Host A.
[SwitchB] ip route-static 10.1.1.0 255.255.255.0 vlan-interface 1
# Define an ACL to identify data flows from subnet 10.1.2.0/24 to subnet 10.1.1.0/24.
[SwitchB] acl number 3101
[SwitchB-acl-adv-3101] rule 0 permit ip source 10.1.2.0 0.0.0.255 destination
10.1.1.0 0.0.0.255
[SwitchB-acl-adv-3101] rule 5 permit ip source 10.1.1.0 0.0.0.255 destination
10.1.2.0 0.0.0.255

```

```

[SwitchB-acl-adv-3101] quit
# Configure a static route to Host A.
[SwitchB] ip route-static 10.1.1.0 255.255.255.0 vlan-interface 1
# Create an IPsec proposal named tran1.
[SwitchB] ipsec proposal tran1
# Specify the encapsulation mode as tunnel.
[SwitchB-ipsec-proposal-tran1] encapsulation-mode tunnel
# Specify the security protocol as ESP.
[SwitchB-ipsec-proposal-tran1] transform esp
# Specify the algorithms for the proposal.
[SwitchB-ipsec-proposal-tran1] esp encryption-algorithm aes 128
[SwitchB-ipsec-proposal-tran1] esp authentication-algorithm sha1
[SwitchB-ipsec-proposal-tran1] quit
# Configure the IKE peer.
[SwitchB] ike peer peer
[SwitchB-ike-peer-peer] pre-shared-key Ab12<><>
[SwitchB-ike-peer-peer] remote-address 2.2.2.1
[SwitchB-ike-peer-peer] quit
# Create an IPsec policy that uses IKE for IPsec SA negotiation.
[SwitchB] ipsec policy usel 10 isakmp
# Apply the ACL.
[SwitchB-ipsec-policy-isakmp-usel-10] security acl 3101
# Apply the IPsec proposal.
[SwitchB-ipsec-policy-isakmp-usel-10] proposal tran1
# Apply the IKE peer.
[SwitchB-ipsec-policy-isakmp-usel-10] ike-peer peer
[SwitchB-ipsec-policy-isakmp-usel-10] quit
# Apply the IPsec policy group to VLAN-interface 1.
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ipsec policy usel

```

Verifying the configuration

After the configuration, IKE negotiation will be triggered to set up SAs when there is traffic between subnet 10.1.1.0/24 and subnet 10.1.2.0/24. If IKE negotiation is successful and SAs are set up, the traffic between the two subnets will be IPsec protected.

Command reference

Modified command: ah authentication-algorithm

Old syntax

```

ah authentication-algorithm { md5 | sha1 }
undo ah authentication-algorithm

```

New syntax

In non-FIPS mode:

```

ah authentication-algorithm { md5 | sha1 }
undo ah authentication-algorithm

```

In FIPS mode:

```
ah authentication-algorithm sha1
undo ah authentication-algorithm
```

Views

IPsec proposal view

Default command level

2: System level

Parameters

md5: Uses MD5 algorithm. This keyword is not available for FIPS mode.

sha1: Uses SHA1.

Change description

After modification: In FIPS mode, MD5 algorithm is not supported. By default, AH uses SHA1 algorithm.

New command: connection-name

Use **connection-name** to configure an IPsec connection name. This name functions only as a description of the IPsec policy.

Use **undo connection-name** to restore the default.

Syntax

```
connection-name name
undo connection-name
```

Default

No IPsec connection name is configured.

Views

IPsec policy view

Default command level

2: System level

Parameters

name: IPsec connection name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

This command is supported only in FIPS mode.

Example

```
# Set IPsec connection name to aaa.
<Sysname> system-view
[Sysname] ipsec policy policy1 1 isakmp
[Sysname-ipsec-policy-isakmp-policy1-1] connection-name aaa
```

Modified command: display ipsec sa

Old syntax

display ipsec sa [**brief** | **policy** *policy-name* [*seq-number*]] [| { **begin** | **exclude** | **include** } *regular-expression*]

New syntax

display ipsec sa [**brief** | **policy** *policy-name* [*seq-number*] | **remote** *ip-address*] [| { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

brief: Displays brief information about all IPsec SAs.

policy: Displays detailed information about IPsec SAs created by using a specified IPsec policy.

policy-name: Name of the IPsec policy, a string 1 to 15 characters.

seq-number: Sequence number of the IPsec policy, in the range 1 to 65535.

remote *ip-address*: Displays detailed information about the IPsec SA with a specified remote address. This option is supported only in FIPS mode.

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

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

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

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

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

Change description

After modification: This command displays information about the IPsec SA with a specified remote address.

New command: display ipsec session

Use **display ipsec session** to display information about IPsec sessions.

Syntax

display ipsec session [**tunnel-id** *integer*] [| { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

integer: ID of the IPsec tunnel, in the range 1 to 2000000000.

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

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

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

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

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

Usage guidelines

This command is supported only in FIPS mode.

If you do not specify any parameters, the command displays information about all IPsec sessions.

IPsec can find matched tunnels directly by session, reducing the intermediate matching procedures and improving the forwarding efficiency. A session is identified by the quintuplet of protocol, source IP address, source port, destination IP address, and destination port.

Examples

Display information about all IPsec sessions.

```
<Sysname> display ipsec session

-----
total sessions : 2
-----

tunnel-id : 3
session idle time/total duration (sec) : 36/300

session flow :      (8 times matched)
    Sour Addr : 15.15.15.1          Sour Port:    0  Protocol : 1
    Dest Addr : 15.15.15.2          Dest Port:    0  Protocol : 1

-----

tunnel-id : 4
session idle duration/total duration (sec) : 7/300

session flow :      (3 times matched)
    Sour Addr : 12.12.12.1          Sour Port:    0  Protocol : 1
    Dest Addr : 13.13.13.1          Dest Port:    0  Protocol : 1
```

Display information about the session with an IPsec tunnel ID of 5.

```
<Sysname> display ipsec session tunnel-id 5

-----
total sessions : 1
-----

tunnel-id : 5
session idle time/total duration (sec) : 30/300

session flow :      (4 times matched)
    Sour Addr : 12.12.12.2          Sour Port:    0  Protocol : 1
    Dest Addr : 13.13.13.2          Dest Port:    0  Protocol : 1
```

Table 6 Command output

Field	Description
total sessions	Total number of IPsec sessions.
tunnel-id	IPsec tunnel ID, same as the connection-id of the IPsec SA.

Field	Description
session idle time	Idle duration of the IPsec session in seconds.
total duration	Lifetime of the IPsec session in seconds, defaulted to 300 seconds.
session flow	Flow information of the IPsec session.
times matched	Total number of packets matching the IPsec session.
Sour Addr	Source IP address of the IPsec session.
Dest Addr	Destination IP address of the IPsec session.
Sour Port	Source port number of the IPsec session.
Dest Port	Destination port number of the IPsec session.
Protocol	Protocol number of the IPsec protected data flow, for example, 1 for ICMP.

Related commands

reset ipsec session

Modified command: **esp authentication-algorithm**

Old syntax

```
esp authentication-algorithm { md5 | sha1 }
undo esp authentication-algorithm
```

New syntax

In non-FIPS mode:

```
esp authentication-algorithm { md5 | sha1 }
undo esp authentication-algorithm
```

In FIPS mode:

```
esp authentication-algorithm sha1
undo esp authentication-algorithm
```

Views

IPsec proposal view

Default command level

2: System level

Parameters

md5: Uses the MD5 algorithm, which uses a 128-bit key. The FIPS mode does not support MD5.

sha1: Uses the SHA1 algorithm, which uses a 160-bit key.

Change description

After modification: In FIPS mode, the MD5 algorithm is not supported. By default, ESP uses SHA1 authentication algorithm.

Modified command: **esp encryption-algorithm**

Old syntax

```
esp encryption-algorithm { 3des | aes [ key-length ] | des }
```

undo esp encryption-algorithm

New syntax

In non-FIPS mode:

esp encryption-algorithm { **3des** | **aes** [*key-length*] | **des** }

undo esp encryption-algorithm

In FIPS mode:

esp encryption-algorithm **aes** [*key-length*]

undo esp encryption-algorithm

Views

IPsec proposal view

Default command level

2: System level

Parameters

3des: Uses triple DES (3DES) in cipher block chaining (CBC) mode as the encryption algorithm. The 3DES algorithm uses a 168-bit key for encryption. The FIPS mode does not support this algorithm.

aes: Uses the Advanced Encryption Standard (AES) in CBC mode as the encryption algorithm. The AES algorithm uses a 128-bit, 192-bit, or 256-bit key for encryption.

key-length: Key length for the AES algorithm, which can be 128, 192, and 256 and defaults to 128. This argument is for AES only.

des: Uses the Data Encryption Standard (DES) in CBC mode as the encryption algorithm. The DES algorithm uses a 56-bit key for encryption. This keyword is not available for FIPS mode.

Change description

After modification: In FIPS mode, the 3DES and DES algorithms are not supported. By default, ESP uses AES-128 encryption algorithm.

New command: ike-peer (IPsec policy view)

Use **ike-peer** to reference an IKE peer in an IPsec policy configured through IKE negotiation.

Use **undo ike-peer** to remove the reference.

Syntax

ike-peer *peer-name*

undo ike-peer *peer-name*

Views

IPsec policy view

Default command level

2: System level

Parameters

peer-name: IKE peer name, a string of 1 to 32 characters.

Usage guidelines

This command is supported only in FIPS mode.

This command applies to only IKE negotiation mode.

Examples

```
# Configure a reference to an IKE peer in an IPsec policy.
<Sysname> system-view
[Sysname] ipsec policy policy1 10 isakmp
[Sysname-ipsec-policy-isakmp-policy1-10] ike-peer peer1
```

Related commands

ipsec policy

New command: ipsec anti-replay check

Use **ipsec anti-replay check** to enable IPsec anti-replay checking.

Use **undo ipsec anti-replay check** to disable IPsec anti-replay checking.

Syntax

```
ipsec anti-replay check
undo ipsec anti-replay check
```

Default

IPsec anti-replay checking is enabled.

Views

System view

Default command level

2: System level

Usage guidelines

This command is supported only in FIPS mode.

Examples

```
# Enable IPsec anti-replay checking.
<Sysname> system-view
[Sysname] ipsec anti-replay check
```

New command: ipsec anti-replay window

Use **ipsec anti-replay window** to set the size of the anti-replay window.

Use **undo ipsec anti-replay window** to restore the default.

Syntax

```
ipsec anti-replay window width
undo ipsec anti-replay window
```

Default

The size of the anti-replay window is 32.

Views

System view

Default command level

2: System level

Parameters

width: Size of the anti-replay window. It can be 32, 64, 128, 256, 512, or 1024.

Usage guidelines

This command is supported only in FIPS mode.

Your configuration affects only IPsec SAs negotiated later.

Examples

Set the size of the anti-replay window to 64.

```
<Sysname> system-view
```

```
[Sysname] ipsec anti-replay window 64
```

New command: ipsec decrypt check

Use **ipsec decrypt check** to enable ACL checking of de-encapsulated IPsec packets.

Use **undo ipsec decrypt check** to disable ACL checking of de-encapsulated IPsec packets.

Syntax

ipsec decrypt check

undo ipsec decrypt check

Default

ACL checking of de-encapsulated IPsec packets is enabled.

Views

System view

Default command level

2: System level

Usage guidelines

This command is supported only in FIPS mode.

Examples

Enable ACL checking of de-encapsulated IPsec packets.

```
<Sysname> system-view
```

```
[Sysname] ipsec decrypt check
```

New command: ipsec policy (interface view)

Use **ipsec policy** to apply an IPsec policy group to an interface.

Use **undo ipsec policy** to remove the application.

Syntax

ipsec policy *policy-name*

undo ipsec policy [*policy-name*]

Views

Interface view

Default command level

2: System level

Parameters

policy-name: Name of the existing IPsec policy group to be applied to the interface, a string of 1 to 15 characters.

Usage guidelines

This command is supported only in FIPS mode.

IPsec policies can be applied only to VLAN interfaces and Layer 3 Ethernet interfaces on the switch.

Only one IPsec policy group can be applied to an interface. To apply another IPsec policy group to the interface, remove the original application first. An IPsec policy can be applied to only one interface.

With an IPsec policy group applied to an interface, the system uses each IPsec policy in the group to protect certain data flows.

For each packet to be sent out an IPsec protected interface, the system checks the IPsec policies of the IPsec policy group in the ascending order of sequence numbers. If it finds an IPsec policy whose ACL matches the packet, it uses the IPsec policy to protect the packet. If it finds no ACL of the IPsec policies matches the packet, it does not provide IPsec protection for the packet and sends the packet out directly.

Examples

Apply IPsec policy group **pg1** to interface VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ipsec policy pg1
```

Related commands

ipsec policy (system view)

Modified command: ipsec policy (system view)

Old syntax

```
ipsec policy policy-name seq-number [ manual ]
undo ipsec policy policy-name [ seq-number ]
```

New syntax

```
ipsec policy policy-name seq-number [ isakmp | manual ]
undo ipsec policy policy-name [ seq-number ]
```

Views

System view

Default command level

2: System level

Parameters

policy-name: Name for the IPsec policy, a case-insensitive string of 1 to 15 characters, including letters and digits. No minus sign (-) can be included.

seq-number: Sequence number for the IPsec policy, in the range of 1 to 65535.

isakmp: Sets up SAs through IKE negotiation. This keyword is supported only in FIPS mode.

manual: Sets up SAs manually.

Change description

After modification: This command can create an IPsec policy through IKE negotiation and enter its view.

Modified command: ipsec proposal

Syntax

ipsec proposal *proposal-name*

undo ipsec proposal *proposal-name*

Views

System view

Default command level

2: System level

Parameters

proposal-name: Name for the proposal, a case-insensitive string of 1 to 32 characters .

Change description

After modification: In FIPS mode, this command can create a new IPsec proposal, with default protocol as ESP, encryption algorithm AES-128, and authentication algorithm SHA1.

New command: ipsec sa global-duration

Use **ipsec sa global-duration** to configure the global SA lifetime.

Use **undo ipsec sa global-duration** to restore the default.

Syntax

ipsec sa global-duration { **time-based** *seconds* | **traffic-based** *kilobytes* }

undo ipsec sa global-duration { **time-based** | **traffic-based** }

Default

The time-based global SA lifetime is 3,600 seconds, and the traffic-based global SA lifetime is 1843200 kilobytes.

Views

System view

Default command level

2: System level

Parameters

seconds: Time-based global SA lifetime in seconds, in the range 180 to 604800.

kilobytes: Traffic-based global SA lifetime in kilobytes, in the range 2560 to 4294967295.

Usage guidelines

This command is supported only in FIPS mode.

When negotiating to set up an SA, IKE prefers the lifetime of the IPsec policy that it uses. If the IPsec policy is not configured with its own lifetime, IKE uses the global SA lifetime.

When negotiating to set up an SA, IKE prefers the shorter one of the local lifetime and that proposed by the remote.

You can configure both a time-based and a traffic-based global SA lifetime. An SA is aged out when it has existed for the specified time period or has processed the specified volume of traffic.

The SA lifetime applies to only IKE negotiated SAs. It is not effective for manually configured SAs.

For CC evaluation in FIPS mode, if IPsec uses IKE automatic negotiation, when IPsec SAs reach the traffic-based lifetime, IPsec notifies IKE to re-perform phase 1 and phase 2 negotiations.

Examples

Set the time-based global SA lifetime to 7200 seconds (2 hours).

```
<Sysname> system-view
```

```
[Sysname] ipsec sa global-duration time-based 7200
```

Set the traffic-based global SA lifetime to 10240 kilobytes (10 Mbytes).

```
[Sysname] ipsec sa global-duration traffic-based 10240
```

Related commands

sa duration

New command: ipsec session idle-time

Use **ipsec session idle-time** to set the idle timeout for IPsec sessions.

Use **undo ipsec session idle-time** to restore the default.

Syntax

ipsec session idle-time *seconds*

undo ipsec session idle-time

Default

The IPsec session idle timeout is 300 seconds.

Views

System view

Default command level

2: System level

Parameters

Seconds: IPsec session idle timeout in seconds, in the range of 60 to 3,600.

Usage guidelines

This command is supported only in FIPS mode.

Examples

Set the IPsec session idle timeout to 600 seconds.

```
<Sysname> system-view
```

```
[Sysname] ipsec session idle-time 600
```

New command: pfs

Use **pfs** to enable and configure the perfect forward secrecy (PFS) feature so that the system uses the feature when employing the IPsec policy to initiate a negotiation.

Use **undo pfs** to remove the configuration.

Syntax

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

undo pfs

Default

The PFS feature is not used for negotiation

Views

IPsec policy view

Default command level

2: System level

Parameters

dh-group2: Uses 1024-bit Diffie-Hellman group.

dh-group5: Uses 1536-bit Diffie-Hellman group.

dh-group14: Uses 2048-bit Diffie-Hellman group.

Usage guidelines

This command is supported only in FIPS mode.

In terms of security and necessary calculation time, the following four groups are in the descending order: 2048-bit Diffie-Hellman group (**dh-group14**), 1536-bit Diffie-Hellman group (**dh-group5**), and 1024-bit Diffie-Hellman group (**dh-group2**).

This command allows IPsec to perform an additional key exchange process during the negotiation phase 2, providing an additional level of security.

The local Diffie-Hellman group must be the same as that of the peer.

Examples

Enable and configure PFS for IPsec policy **policy1**.

```
<Sysname> system-view
```

```
[Sysname] ipsec policy policy1 200 isakmp
```

```
[Sysname-ipsec-policy-isakmp-policy1-200] pfs dh-group2
```

Related commands

ipsec policy (system view)

New command: policy enable

Use **policy enable** to enable the IPsec policy.

Use **undo policy enable** to disable the IPsec policy.

Syntax

policy enable

undo policy enable

Default

The IPsec policy is enabled.

Views

IPsec policy view

Default command level

2: System level

Usage guidelines

This command is supported only in FIPS mode.

If the IPsec policy is not enabled for the IKE peer, the peer cannot take part in the IKE negotiation.

Examples

Enable the IPsec policy with the name policy1 and sequence number 100.

```
<Sysname> system-view
```

```
[Sysname] ipsec policy policy1 100 isakmp
```

```
[Sysname-ipsec-policy-isakmp-policy1-100] policy enable
```

Related commands

ipsec policy (system view)

Modified command: proposal (IPsec policy view)

Old syntax

proposal *proposal-name*

undo proposal [*proposal-name*]

New syntax

proposal *proposal-name*&<1-6>

undo proposal [*proposal-name*]

Views

IPsec policy view

Default command level

2: System level

Parameters

proposal-name&<1-6>: Name of the IPsec proposal, a string of 1 to 32 characters. &<1-6> means that you can specify the *proposal-name* argument for up to six times.

Change description

Before modification: Because parameters of the security policy are only manually configured, only one security proposal can be referenced.

After modification: Because parameters of the security policy are automatically negotiated through IKE, up to six security proposals can be referenced, and IKE searches for a fully matched IPsec proposal during negotiation.

New command: qos pre-classify

Use **qos pre-classify** to enable packet information pre-extraction.

Use **undo qos pre-classify** to restore the default.

Syntax

qos pre-classify

undo qos pre-classify

Default

Packet information pre-extraction is disabled.

Views

IPsec policy view

Default command level

2: System level

Usage guidelines

This command is supported only in FIPS mode.

With the packet information pre-extraction feature enabled, QoS classifies a packet based on the header of the original IP packet—the header of the IP packet that has not been encapsulated by IPsec.

Examples

```
# Enable packet information pre-extraction.
<Sysname> system-view
[Sysname] ipsec policy policy1 100 isakmp
[Sysname-ipsec-policy-isakmp-policy1-100] qos pre-classify
```

Related commands

ipsec policy (system view)

Modified command: reset ipsec sa

Use **reset ipsec sa** to clear IPsec SAs.

Old syntax

reset ipsec sa [**policy** *policy-name* [*seq-number*]]

New syntax

reset ipsec sa [**parameters** *dest-address protocol spi* | **policy** *policy-name* [*seq-number*] | **remote** *ip-address*]

Views

User view

Default command level

2: System level

Parameters

parameters: Specifies IPsec SAs that use the specified destination IP address, security protocol, and SPI. This keyword is supported only in FIPS mode.

dest-address: Destination address, in dotted decimal notation.

protocol: Security protocol, which can be keyword **ah** or **esp**, case insensitive.

spi: Security parameter index, in the range 256 to 4294967295.

policy: Specifies IPsec SAs that use an IPsec policy.

policy-name: Name of the IPsec policy, a case-insensitive string of 1 to 15 characters, including letters and digits.

seq-number: Sequence number of the IPsec policy, in the range 1 to 65535. If no *seq-number* is specified, all the policies in the IPsec policy group named *policy-name* are specified.

remote: Specifies SAs to or from a remote address, in dotted decimal notation. This keyword is supported only in FIPS mode.

Usage guidelines

Immediately after a manually set up SA is cleared, the system automatically sets up a new SA based on the parameters of the IPsec policy. After IKE negotiated SAs are cleared, the system sets up new SAs only when IKE negotiation is triggered by interesting packets.

IPsec SAs appear in pairs. If you specify the **parameters** keyword to clear an IPsec SA, the IPsec SA in the other direction is also automatically cleared.

If you do not specify any parameter, the command clears all IPsec SAs.

Change description

Before modification: This command clears only IPsec SAs that are manually created.

After modification: This command clears IPsec SAs that are manually created or created through IKE negotiation.

New command: reset ipsec session

Use **reset ipsec session** to clear the sessions of a specified IPsec tunnel or all IPsec tunnels.

Syntax

reset ipsec session [**tunnel-id** *integer*]

Views

User view

Default command level

2: System level

Parameters

integer: ID of the IPsec tunnel, in the range 1 to 2000000000.

Usage guidelines

This command is supported only in FIPS mode.

Examples

Clear all IPsec sessions.

```
<Sysname> reset ipsec session
```

Clear the sessions of IPsec tunnel 5.

```
<Sysname> reset ipsec session tunnel-id 5
```

Related commands

display ipsec session

New command: sa duration

Use **sa duration** to set an SA lifetime for the IPsec policy.

Use **undo sa duration** to restore the default.

Syntax

sa duration { **time-based** *seconds* | **traffic-based** *kilobytes* }

undo sa duration { **time-based** | **traffic-based** }

Default

The SA lifetime of an IPsec policy equals the current global SA lifetime.

The time-based global SA lifetime is 3600 seconds, and traffic-based SA lifetime is 1843200 kilobytes.

Views

IPsec policy view

Default command level

2: System level

Parameters

seconds: Time-based SA lifetime in seconds, in the range 180 to 604800.

kilobytes: Traffic-based SA lifetime in kilobytes, in the range 2560 to 4294967295.

Usage guidelines

This command is supported only in FIPS mode.

When negotiating to set up an SA, IKE prefers the lifetime settings of the IPsec policy that it uses. If the IPsec policy or IPsec proposal is not configured with its own lifetime settings, IKE uses the global SA lifetime settings, which are configured with the **ipsec sa global-duration** command.

When negotiating to set up an SA, IKE prefers the shorter ones of the local lifetime settings and those proposed by the remote.

The SA lifetime applies to only IKE negotiated SAs. It is not effective for manually configured SAs.

For CC evaluation in FIPS mode, if IPsec uses IKE automatic negotiation, when IPsec SAs reach the traffic-based lifetime, the system notifies IKE to re-perform phase 1 and phase 2 negotiations.

Related commands: **ipsec sa global-duration**, **ipsec policy (system view)**.

Examples

Set the SA lifetime for IPsec **policy1** to 7200 seconds (two hours).

```
<Sysname> system-view
```

```
[Sysname] ipsec policy policy1 100 isakmp
```

```
[Sysname-ipsec-policy-isakmp-policy1-100] sa duration time-based 7200
```

Set the SA lifetime for IPsec policy **policy1** to 20480 kilobytes (20 Mbytes).

```
<Sysname> system-view
```

```
[Sysname] ipsec policy policy1 100 isakmp
```

```
[Sysname-ipsec-policy-isakmp-policy1-100] sa duration traffic-based 20480
```

Modified command: sa string-key

Syntax

sa string-key { inbound | outbound } { ah | esp } [cipher | simple] *string-key*

undo sa string-key { inbound | outbound } { ah | esp }

Views

IPsec policy view

Default command level

2: System level

Parameters

inbound: Specifies the inbound SA through which IPsec processes the received packets.

outbound: Specifies the outbound SA through which IPsec processes the packets to be sent.

ah: Uses AH.

esp: Uses ESP.

cipher: Sets a ciphertext key.

simple: Sets a plaintext key.

string-key: Specifies the key string. This argument is case sensitive. If **cipher** is specified, it must be a ciphertext string of 1 to 373 characters. If **simple** is specified, it must be a string of 1 to 255 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string. For different algorithms, enter strings of any length in the specified range. Using this key string, the system automatically generates keys meeting the algorithm requirements. When the protocol is ESP, the system generates the keys for both the authentication algorithm and encryption algorithm.

Change description

After modification: This command is not supported in FIPS mode.

New command: security acl

Use **security acl** to specify the ACL for the IPsec policy to reference.

Use **undo security acl** to remove the configuration.

Syntax

security acl *acl-number*

undo security acl

Default

An IPsec policy references no ACL.

Views

IPsec policy view

Default command level

2: System level

Parameters

acl-number: Number of the ACL for the IPsec policy to reference, in the range 3000 to 3999.

Usage guidelines

This command is supported only in FIPS mode.

With an IKE-dependent IPsec policy configured, data flows can be protected in standard mode. In standard mode, one tunnel protects one data flow. The data flow permitted by each ACL rule is protected by one tunnel that is established separately for it.

When you specify an ACL for an IPsec policy, follow these guidelines:

- You must create a mirror image ACL rule at the remote end for each ACL rule created at the local end. Otherwise, IPsec may protect traffic in only one direction.
- The ACL cannot be deployed to an aggregate interface or a tunnel interface.
- You cannot specify multiple ACLs for one IPsec policy or one ACL for multiple IPsec policies. To configure ACL rules you want to deploy for an IPsec policy, you must configure all of them in one ACL and specify the ACL for the IPsec policy.
- You can specify only one ACL for an IPsec policy. To deploy multiple ACL rules, configure the ACL rules in one ACL, and then reference the ACL in an IPsec policy.
- ACLs referenced by IPsec cannot be used by other services.

Examples

Configure IPsec policy policy1 to reference ACL 3001.

```

<Sysname> system-view
[Sysname] acl number 3001
[Sysname-acl-adv-3001] rule permit tcp source 10.1.1.0 0.0.0.255 destination 10.1.2.0
0.0.0.255
[Sysname-acl-adv-3001] quit
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] security acl 3001

```

Related commands

ipsec policy (system view)

Modified command: transform

Syntax

```

transform { ah | ah-esp | esp }
undo transform

```

Views

IPsec proposal view

Default command level

2: System level

Parameters

ah: Uses the AH protocol.
ah-esp: Uses ESP first and then AH.
esp: Uses the ESP protocol.

Change description

After modification: In FIPS mode,,

- If AH is used, the default authentication algorithm is SHA1.
- If ESP is used, the default encryption and authentication algorithms are AES-128 and SHA1, respectively.
- If both AH and ESP are used, AH uses the SHA1 authentication algorithm by default, and ESP uses the AES-128 encryption algorithm and the SHA1 authentication algorithm by default.

New command: tunnel local

Use **tunnel local** to configure the local address of an IPsec tunnel.

Use **undo tunnel local** to remove the configuration.

Syntax

```

tunnel local ip-address
undo tunnel local

```

Default

No local address is configured for an IPsec tunnel.

Views

IPsec policy view

Default command level

2: System level

Parameters

ip-address: Local address for the IPsec tunnel.

Usage guidelines

This command is supported only in FIPS mode.

The local address, if not configured, will be the address of the interface to which the IPsec policy is applied.

Examples

```
# Set the local address of the IPsec tunnel to the address of Loopback 0, 10.0.0.1.
```

```
<Sysname> system-view
```

```
[Sysname] interface loopback 0
```

```
[Sysname-LoopBack0] ip address 10.0.0.1 32
```

```
[Sysname-LoopBack0] quit
```

```
[Sysname] ipsec policy policy1 100 manual
```

```
[Sysname-ipsec-policy-manual-policy1-100] tunnel local 10.0.0.1
```

Related commands

ipsec policy (system view)

New command: tunnel remote

Use **tunnel remote** to configure the remote address of an IPsec tunnel.

Use **undo tunnel remote** to remove the configuration.

Syntax

tunnel remote *ip-address*

undo tunnel remote [*ip-address*]

Default

No remote address is configured for the IPsec tunnel.

Views

IPsec policy view

Default command level

2: System level

Parameters

ip-address: Remote address for the IPsec tunnel.

Usage guidelines

This command is supported only in FIPS mode.

If you configure the remote address repeatedly, the last one takes effect.

An IPsec tunnel is established between the local and remote ends. The remote IP address of the local end must be the same as that of the local IP address of the remote end.

Examples

```
# Set the remote address of the IPsec tunnel to 10.1.1.2.
```

```
<Sysname> system-view
```



```
[Sysname] ipsec policy policy1 10 manual
[Sysname-ipsec-policy-policy1-10] tunnel remote 10.1.1.2
```

Related commands

ipsec policy (system view)

New feature: IKE

NOTE:

This chapter is applicable to only the switches in FIPS mode.

IKE overview

Built on a framework defined by the Internet Security Association and Key Management Protocol (ISAKMP), Internet Key Exchange (IKE) provides automatic key negotiation and SA establishment services for IPsec, simplifying the application, management, configuration and maintenance of IPsec dramatically.

Instead of transmitting keys directly across a network, IKE peers transmit keying materials between them, and calculate shared keys respectively. Even if a third party captures all exchanged data for calculating the keys, it cannot calculate the keys.

IKE security mechanism

IKE has a series of self-protection mechanisms and supports secure identity authentication, key distribution, and IPsec SA establishment on insecure networks.

Data authentication

Data authentication involves two concepts:

- **Identity authentication**—Mutual identity authentication between peers. Two authentication methods are available: pre-shared key authentication and PKI-based digital signature authentication (RSA signature).
- **Identity protection**—Encrypts the identity information with the generated keys before sending the information.

DH

The Diffie-Hellman (DH) algorithm is a public key algorithm. With this algorithm, two peers can exchange keying material and then use the material to calculate the shared keys. Due to the decryption complexity, a third party cannot decrypt the keys even after intercepting all keying materials.

PFS

The Perfect Forward Secrecy (PFS) feature is a security feature based on the DH algorithm. By making sure keys have no derivative relations, it guarantees a broken key brings no threats to other keys. For IPsec, PFS is implemented by adding an additional key exchange at IKE negotiation phase 2.

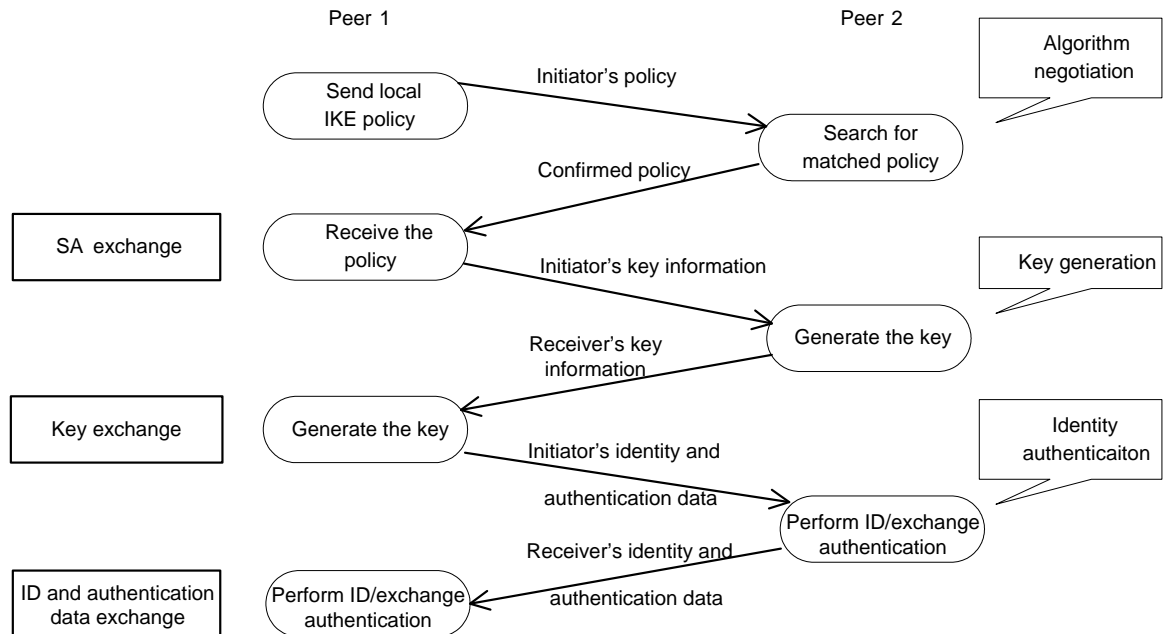
IKE operation

IKE negotiates keys and establishes SAs for IPsec in two phases:

1. **Phase 1**—The two peers establish an ISAKMP SA, a secure, authenticated channel for communication.

2. **Phase 2**—Using the ISAKMP SA established in phase 1, the two peers negotiate to establish IPsec SAs.

Figure 12 IKE exchange process in main mode



As shown in [Figure 12](#), the main mode of IKE negotiation in phase 1 involves three pairs of messages:

- SA exchange, used for negotiating the security policy.
- Key exchange, used for exchanging the Diffie-Hellman public value and other values like the random number. Key data is generated in this stage.
- ID and authentication data exchange, used for identity authentication and authentication of data exchanged in phase 1.

IKE functions

IKE provides the following functions for IPsec:

- Automatically negotiates IPsec parameters such as the keys.
- Performs DH exchange when establishing an SA, making sure that each SA has a key independent of other keys.
- Automatically negotiates SAs when the sequence number in the AH or ESP header overflows, making sure that IPsec provides the anti-replay service normally by using the sequence number.
- Provides end-to-end dynamic authentication.
- Identity authentication and management of peers influence IPsec deployment. A large-scale IPsec deployment needs the support of certificate authorities (CAs) or other institutes which manage identity data centrally.

Relationship between IKE and IPsec

Figure 13 Relationship between IKE and IPsec

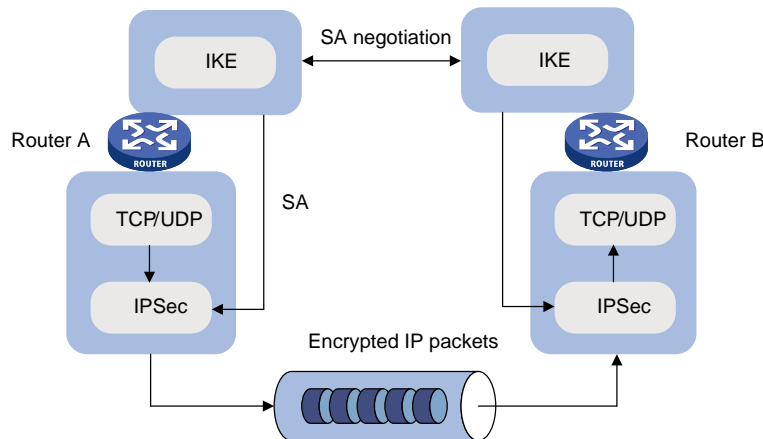


Figure 13 illustrates the relationship between IKE and IPsec:

- IKE is an application layer protocol using UDP and functions as the signaling protocol of IPsec.
- IKE negotiates SAs for IPsec and delivers negotiated parameters and generated keys to IPsec.
- IPsec uses the SAs set up through IKE negotiation for encryption and authentication of IP packets.

Protocols and standards

These protocols and standards are relevant to IKE:

- RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*
- RFC 2409, *The Internet Key Exchange (IKE)*
- RFC 2412, *The OAKLEY Key Determination Protocol*

IKE configuration task list

Prior to IKE configuration, you must determine the following parameters:

- The strength of the algorithms for IKE negotiation (the security protection level), including the identity authentication method, encryption algorithm, authentication algorithm, and DH group. Different algorithms provide different levels of protection. A stronger algorithm means more resistant to decryption of protected data but requires more resources. Generally, the longer the key, the stronger the algorithm.
- The pre-shared key or the PKI domain the certificate belongs to. For more information about PKI configuration, see the chapter "PKI configuration."

To configure IKE:

Task	Remarks
Configuring a name for the local security gateway	Optional.
Configuring an IKE proposal	Optional. Required if you want to specify an IKE proposal for an IKE peer to reference.
Configuring an IKE peer	Required.

Task	Remarks
Setting keepalive timers	Optional.
Setting the NAT keepalive timer	Optional.
Configuring a DPD detector	Optional.
Disabling next payload field checking	Optional.

Configuring a name for the local security gateway

If the IKE negotiation peer uses the security gateway name as its ID to initiate IKE negotiation (the **id-type name** or **id-type user-fqdn** command is configured on the initiator), configure the **ike local-name** command in system view or the **local-name** command in IKE peer view on the local device. If you configure both commands, the name configured in IKE peer view is used.

To configure a name for the local security gateway:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure a name for the local security gateway.	ike local-name <i>name</i>	Optional. By default, the device name is used as the name of the local security gateway.

Configuring an IKE proposal

An IKE proposal defines a set of attributes describing how IKE negotiation should take place. You may create multiple IKE proposals with different preferences. The preference of an IKE proposal is represented by its sequence number, and the lower the sequence number, the higher the preference.

Two peers must have at least one matching IKE proposal for successful IKE negotiation. During IKE negotiation, the initiator sends its IKE proposals to the peer, and the peer searches its own IKE proposals for a match. The search starts from the one with the lowest sequence number and proceeds in the ascending order of sequence number until a match is found or all the IKE proposals are found mismatching. The matching IKE proposals will be used to establish the secure tunnel.

Two matching IKE proposals have the same encryption algorithm, authentication method, authentication algorithm, and DH group. The SA lifetime will take the smaller one of the settings on the two sides.

By default, there is an IKE proposal, which has the lowest preference and uses the default encryption algorithm, authentication method, authentication algorithm, DH group, and ISAKMP SA lifetime.

To configure an IKE proposal:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create an IKE proposal and enter its view.	ike proposal <i>proposal-number</i>	N/A
3. Specify an encryption algorithm for the IKE proposal.	encryption-algorithm aes-cbc [<i>key-length</i>]	Optional. The default is AES-CBC-128.
4. Specify an authentication method for the IKE proposal.	authentication-method { pre-share rsa-signature }	Optional. Pre-shared key by default.

Step	Command	Remarks
5. Specify an authentication algorithm for the IKE proposal.	authentication-algorithm sha	Optional. SHA1 by default.
6. Specify a DH group for key negotiation in phase 1.	dh { group2 group5 group14 }	Optional. group2 (the 1024-bit DH group) by default.
7. Set the ISAKMP SA lifetime for the IKE proposal.	sa duration seconds	Optional. 86400 seconds by default.

NOTE:

Before an ISAKMP SA expires, IKE negotiates a new SA to replace it. DH calculation in IKE negotiation takes time, especially on low-end devices. To prevent SA updates from influencing normal communication, set the lifetime greater than 10 minutes.

Configuring an IKE peer

For an IPsec policy that uses IKE, you must configure an IKE peer by performing the following tasks:

- Specify the IKE negotiation mode (main mode) for the local end to use in IKE negotiation phase 1. When acting as the IKE negotiation responder, the local end uses the IKE negotiation mode of the remote end.
- Specify the IKE proposals for the local end to use when acting as the IKE negotiation initiator. When acting as the responder, the local end uses the IKE proposals configured in system view for negotiation.
- Configure a pre-shared key for pre-shared key authentication or a PKI domain for digital signature authentication.
- Specify the ID type for the local end to use in IKE negotiation phase 1. With pre-shared key authentication, the ID type must be IP address for main mode IKE negotiation.
- Specify the name or IP address of the local security gateway. You perform this task only when you want to specify a special address, for example, a loopback interface address, as the local security gateway address.
- Specify the name or IP address of the remote security gateway. For the local end to initiate IKE negotiation, you must specify the name or IP address of the remote security gateway on the local end so the local end can find the remote end.
- Enable NAT traversal. If there is NAT gateway on the path for tunneling, you must configure NAT traversal at the two ends of the IPsec tunnel, because one end may use a public address while the other end uses a private address.
- Specify the dead peer detection (DPD) detector for the IKE peer.

To configure an IKE peer:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create an IKE peer and enter IKE peer view.	ike peer peer-name	N/A
3. Specify the IKE negotiation mode for phase 1.	exchange-mode main	Optional. The default is main .

Step	Command	Remarks
4. Specify the IKE proposals for the IKE peer to reference.	proposal <i>proposal-number</i> <1-6>	Optional. By default, an IKE peer references no IKE proposals, and, when initiating IKE negotiation, it uses the IKE proposals configured in system view.
5. Configure the pre-shared key for pre-shared key authentication.	pre-shared-key [cipher simple] <i>key</i>	Configure either command according to the authentication method for the IKE proposal.
6. Configure the PKI domain for digital signature authentication.	certificate domain <i>domain-name</i>	
7. Select the ID type for IKE negotiation phase 1.	id-type { ip name user-fqdn }	Optional. ip by default.
8. Configure the names of the two ends.	<ul style="list-style-type: none"> Specify a name for the local security gateway: local-name <i>name</i> Configure the name of the remote security gateway: remote-name <i>name</i> 	<p>Optional.</p> <p>By default, no name is configured for the local security gateway in IKE peer view, and the security gateway name configured by using the ike local-name command is used.</p> <p>The remote gateway name configured with remote-name command on the local gateway must be identical to the local name configured with the local-name command on the peer.</p>
9. Configure the IP addresses of the two ends.	<ul style="list-style-type: none"> Specify an IP address for the local gateway: local-address <i>ip-address</i> Configure the IP addresses of the remote gateway: remote-address { <i>hostname</i> [dynamic] <i>low-ip-address</i> [<i>high-ip-address</i>] } 	<p>Optional.</p> <p>By default, it is the primary IP address of the interface referencing the security policy.</p> <p>The remote IP address configured with the remote-address command on the local gateway must be identical to the local IP address configured with the local-address command on the peer.</p>
10. Enable the NAT traversal function for IPsec/IKE.	nat traversal	<p>Optional.</p> <p>Required when a NAT gateway is present in the VPN tunnel constructed by IPsec/IKE.</p> <p>Disabled by default.</p>
11. Apply a DPD detector to the IKE peer.	dpd <i>dpd-name</i>	<p>Optional.</p> <p>No DPD detector is applied to an IKE peer by default.</p> <p>For more information about DPD configuration, see "Configuring a DPD detector."</p>

NOTE:

After modifying the configuration of an IPsec IKE peer, execute the **reset ipsec sa** and **reset ike sa** commands to clear existing IPsec and IKE SAs. Otherwise, SA re-negotiation will fail.

Setting keepalive timers

IKE maintains the link status of an ISAKMP SA by keepalive packets. Generally, if the peer is configured with the keepalive timeout, you must configure the keepalive packet transmission interval on the local end. If the peer receives no keepalive packet during the timeout interval, the ISAKMP SA will be tagged with the TIMEOUT tag (if it does not have the tag), or be deleted along with the IPsec SAs it negotiated (when it has the tag already).

To set the keepalive timers:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the ISAKMP SA keepalive interval.	ike sa keepalive-timer interval <i>seconds</i>	No keepalive packet is sent by default.
3. Set the ISAKMP SA keepalive timeout.	ike sa keepalive-timer timeout <i>seconds</i>	No keepalive packet is sent by default.

NOTE:

The keepalive timeout configured at the local end must be longer than the keepalive interval configured at the remote end. Since it seldom occurs that more than three consecutive packets are lost on a network, the keepalive timeout can be configured to be three times of the keepalive interval.

Setting the NAT keepalive timer

If IPsec traffic needs to pass through NAT security gateways, you must configure the NAT traversal function. If no packet travels across an IPsec tunnel in a certain period of time, the NAT mapping may get aged and be deleted, disabling the tunnel beyond the NAT gateway from transmitting data to the intended end. To prevent NAT mappings from being aged, an ISAKMP SA behind the NAT security gateway sends NAT keepalive packets to its peer at a certain interval to keep the NAT session alive.

To set the NAT keepalive timer:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the NAT keepalive interval.	ike sa nat-keepalive-timer interval <i>seconds</i>	20 seconds by default.

Configuring a DPD detector

Dead peer detection (DPD) irregularly detects dead IKE peers. It works as follows:

1. When the local end sends an IPsec packet, it checks the time the last IPsec packet was received from the peer.
2. If the time interval exceeds the DPD interval, it sends a DPD hello to the peer.
3. If the local end receives no DPD acknowledgement within the DPD packet retransmission interval, it retransmits the DPD hello.

4. If the local end still receives no DPD acknowledgement after having made the maximum number of retransmission attempts (two by default), it considers the peer already dead, and clears the IKE SA and the IPsec SAs based on the IKE SA.

DPD enables an IKE entity to check the liveness of its peer only when necessary. It generates less traffic than the keepalive mechanism, which exchanges messages periodically.

To configure a DPD detector:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a DPD detector and enter its view.	ike dpd <i>dpd-name</i>	N/A
3. Set the DPD interval.	interval-time <i>interval-time</i>	Optional. 10 seconds by default.
4. Set the DPD packet retransmission interval.	time-out <i>time-out</i>	Optional. 5 seconds by default.

Disabling next payload field checking

The Next payload field is in the generic payload header of the last payload of the IKE negotiation message (the message comprises multiple payloads). According to the protocol, this field must be 0 if the payload is the last payload of the packet. However, it may be set to other values on some brands of devices. For interoperability, disable the checking of this field.

To disable Next payload field checking:

Step	Command	Remark
1. Enter system view.	system-view	N/A
2. Disable Next payload field checking.	ike next-payload check disabled	Enabled by default.

Displaying and maintaining IKE

Task	Command	Remarks
Display IKE DPD information	display ike dpd [<i>dpd-name</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display IKE peer information	display ike peer [<i>peer-name</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display IKE SA information	display ike sa [verbose [connection-id <i>connection-id</i> remote-address <i>remote-address</i>]] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display IKE proposal information	display ike proposal [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Clear SAs established by IKE	reset ike sa [<i>connection-id</i>]	Available in user view.

IKE configuration example

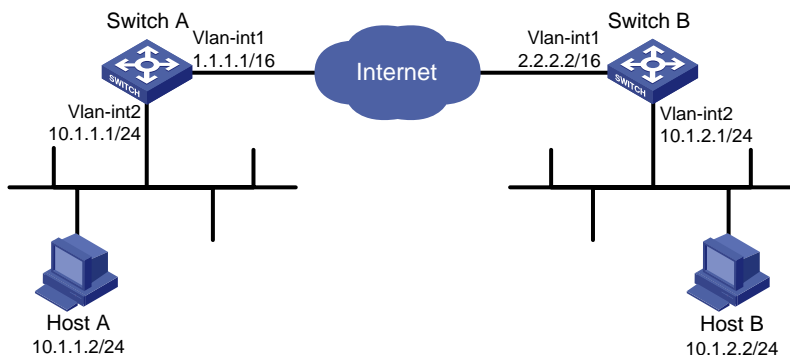
Network requirements

As shown in [Figure 14](#), configure an IPsec tunnel that uses IKE negotiation between gateways Switch A and Switch B to secure the communication between subnet 10.1.1.0/24 and subnet 10.1.2.0/24.

For Switch A, configure an IKE proposal that uses the sequence number 10 and the authentication algorithm SHA1. Configure Switch B to use the default IKE proposal.

Configure the two routers to use the pre-shared key authentication method.

Figure 14 Network diagram



Configuration procedure

1. Make sure Switch A and Switch B can reach each other.
2. Configure Switch A:

Assign an IP address to VLAN-interface 1.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-vlan-interface1] ip address 1.1.1.1 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

Assign an IP address to VLAN-interface 2.

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 10.1.1.1 255.255.255.0
[SwitchA-Vlan-interface2] quit
```

Configure a static route to subnet 10.1.2.0/24.

```
[SwitchA] ip route-static 10.1.2.0 255.255.255.0 2.2.2.2
```

Configure ACL 3101 to identify traffic from subnet 10.1.1.0/24 to subnet 10.1.2.0/24.

```
[SwitchA] acl number 3101
[SwitchA-acl-adv-3101] rule 0 permit ip source 10.1.1.0 0.0.0.255 destination
10.1.2.0 0.0.0.255
[SwitchA-acl-adv-3101] rule 1 permit ip source 10.1.2.0 0.0.0.255 destination
10.1.1.0 0.0.0.255
[SwitchA-acl-adv-3101] quit
```

Create IPsec proposal tran1.

```
[SwitchA] ipsec proposal tran1
```

Set the packet encapsulation mode to tunnel.

```
[SwitchA-ipsec-proposal-tran1] encapsulation-mode tunnel
```

```

# Use security protocol ESP.
[Switch-ipsec-proposal-tran1] transform esp
# Specify encryption and authentication algorithms.
[SwitchA-ipsec-proposal-tran1] esp encryption-algorithm aes 128
[SwitchA-ipsec-proposal-tran1] esp authentication-algorithm sha1
[SwitchA-ipsec-proposal-tran1] quit
# Create an IKE proposal numbered 10.
[SwitchA] ike proposal 10
# Set the authentication algorithm to SHA1.
[SwitchA-ike-proposal-10] authentication-algorithm sha
# Configure the authentication method as pre-shared key.
[SwitchA-ike-proposal-10] authentication-method pre-share
# Set the ISAKMP SA lifetime to 5000 seconds.
[SwitchA-ike-proposal-10] sa duration 5000
[SwitchA-ike-proposal-10] quit
# Create IKE peer peer.
[SwitchA] ike peer peer
# Configure the IKE peer to reference IKE proposal 10.
[SwitchA-ike-peer-peer] proposal 10
# Set the pre-shared key.
[SwitchA-ike-peer-peer] pre-shared-key AAbbcc1234%
# Specify the IP address of the peer security gateway.
[SwitchA-ike-peer-peer] remote-address 2.2.2.2
[SwitchA-ike-peer-peer] quit
# Create an IPsec policy that uses IKE negotiation.
[SwitchA] ipsec policy map1 10 isakmp
# Reference IPsec proposal tran1.
[SwitchA-ipsec-policy-isakmp-map1-10] proposal tran1
# Reference ACL 3101 to identify the protected traffic.
[SwitchA-ipsec-policy-isakmp-map1-10] security acl 3101
# Reference IKE peer peer.
[SwitchA-ipsec-policy-isakmp-map1-10] ike-peer peer
[SwitchA-ipsec-policy-isakmp-map1-10] quit
# Apply the IPsec policy to VLAN-interface 1.
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ipsec policy map1

```

3. Configure Switch B:

```

# Assign an IP address to VLAN-interface 1.
[SwitchB] interface Vlan-interface1
[SwitchB-Vlan-interface1] ip address 2.2.2.2 255.255.255.0
[SwitchB-Vlan-interface1] quit
# Assign an IP address to VLAN-interface 2.
[SwitchB] interface Vlan-interface2
[SwitchB-Vlan-interface2] ip address 10.1.2.1 255.255.255.0
[SwitchB-Vlan-interface2] quit
# Configure a static route to subnet 10.1.1.0/24.
[SwitchB] ip route-static 10.1.1.0 255.255.255.0 1.1.1.1

```

```

# Configure ACL 3101 to identify traffic from subnet 10.1.2.0/24 to subnet 10.1.1.0/24.
<SwitchB> system-view
[SwitchB] acl number 3101
[SwitchB-acl-adv-3101] rule 0 permit ip source 10.1.2.0 0.0.0.255 destination
10.1.1.0 0.0.0.255
[SwitchB-acl-adv-3101] rule 1 permit ip source 10.1.1.0 0.0.0.255 destination
10.1.2.0 0.0.0.255
[SwitchB-acl-adv-3101] quit
# Create IPsec proposal tran1.
[SwitchB] ipsec proposal tran1
# Set the packet encapsulation mode to tunnel.
[SwitchB-ipsec-proposal-tran1] encapsulation-mode tunnel
# Use security protocol ESP.
[SwitchB-ipsec-proposal-tran1] transform esp
# Specify encryption and authentication algorithms.
[SwitchB-ipsec-proposal-tran1] esp encryption-algorithm aes 128
[SwitchB-ipsec-proposal-tran1] esp authentication-algorithm sha1
[SwitchB-ipsec-proposal-tran1] quit
# Create an IKE proposal numbered 10.
[SwitchB] ike proposal 10
# Set the authentication algorithm to SHA1.
[SwitchB-ike-proposal-10] authentication-algorithm sha
# Configure the authentication method as pre-shared key.
[SwitchB-ike-proposal-10] authentication-method pre-share
# Set the ISAKMP SA lifetime to 5000 seconds.
[SwitchB-ike-proposal-10] sa duration 5000
[SwitchB-ike-proposal-10] quit
# Create IKE peer peer.
[SwitchB] ike peer peer
# Configure the IKE peer to reference IKE proposal 10.
[SwitchB-ike-peer-peer] proposal 10
# Set the pre-shared key.
[SwitchB-ike-peer-peer] pre-shared-key AAbbcc1234%
# Specify the IP address of the peer security gateway.
[SwitchB-ike-peer-peer] remote-address 1.1.1.1
[SwitchB-ike-peer-peer] quit
# Create an IPsec policy that uses IKE negotiation.
[SwitchB] ipsec policy use1 10 isakmp
# Reference ACL 3101 to identify the protected traffic.
[SwitchB-ipsec-policy-isakmp-use1-10] security acl 3101
# Reference IPsec proposal tran1.
[SwitchB-ipsec-policy-isakmp-use1-10] proposal tran1
# Reference IKE peer peer.
[SwitchB-ipsec-policy-isakmp-use1-10] ike-peer peer
[SwitchB-ipsec-policy-isakmp-use1-10] quit
# Apply the IPsec policy to VLAN-interface 1.
[SwitchB] interface Vlan-interface1

```

```
[SwitchB-Vlan-interface1] ipsec policy use1
```

Verifying the configuration

After the above configuration, send traffic from subnet 10.1.1.0/24 to subnet 10.1.2.0/24. Switch A starts IKE negotiation with Switch B when receiving the first packet. IKE proposal matching starts with the one having the highest priority. During the matching process, lifetime is not involved but it is determined by the IKE negotiation parties.

Troubleshooting IKE

When you configure parameters to establish an IPsec tunnel, enable IKE error debugging to locate configuration problems:

```
<Switch> debugging ike error
```

Invalid user ID

Symptom

Invalid user ID.

Analysis

In IPsec, user IDs are used to identify data flows and to set up different IPsec tunnels for different data flows. Now, the IP address and username are used as the user ID.

The following is the debugging information:

```
got NOTIFY of type INVALID_ID_INFORMATION
```

Or

```
drop message from A.B.C.D due to notification type INVALID_ID_INFORMATION
```

Solution

Check that the ACLs in the IPsec policies configured on the interfaces at both ends are compatible. Configure the ACLs to mirror each other. For more information about ACL mirroring, see the chapter "IPsec configuration."

Proposal mismatch

Symptom

The proposals mismatch.

Analysis

The following is the debugging information:

```
got NOTIFY of type NO_PROPOSAL_CHOSEN
```

Or

```
drop message from A.B.C.D due to notification type NO_PROPOSAL_CHOSEN
```

The two parties in the negotiation have no matched proposals.

Solution

For the negotiation in phase 1, look up the IKE proposals for a match. For the negotiation in phase 2, check whether the parameters of the IPsec policies applied on the interfaces are matched, and whether the referred IPsec proposals have a match in protocol, encryption and authentication algorithms.

Failing to establish an IPsec tunnel

Symptom

The expected IPsec tunnel cannot be established.

Analysis

Sometimes this may happen that an IPsec tunnel cannot be established or there is no way to communicate in the presence of an IPsec tunnel in an unstable network. According to examination results, however, ACLs of both parties are configured correctly, and proposals are also matched.

In this case, the problem is usually caused by the reboot of one router after the IPsec tunnel is established.

Solution

- Use the **display ike sa** command to check whether both parties have established an SA in phase 1.
- Use the **display ipsec sa policy** command to check whether the IPsec policy on the interface has established IPsec SA.
- If the two commands show that one party has an SA but the other does not, use the **reset ipsec sa** command to clear the IPsec SA that has no corresponding SA, use the **reset ike sa** command to clear the IKE SA that has no corresponding IKE SA, and trigger SA re-negotiation.

ACL configuration error

Symptom

ACL configuration error results in data flow blockage.

Analysis

When multiple devices create different IPsec tunnels early or late, a device may have multiple peers. If the device is not configured with ACL rule, the peers send packets to it to set up different IPsec tunnels in different protection granularity respectively. As the priorities of IPsec tunnels are determined by the order they are established, a device cannot interoperate with other peers in fine granularity when its outbound packets are first matched with an IPsec tunnel in coarse granularity.

Solution

When a device has multiple peers, configure ACLs on the device to distinguish different data flows and try to avoid configuring overlapping ACL rules for different peers. If it is unavoidable, the subrules in fine granularity should be configured with higher preferences.

Command reference

authentication-algorithm

Use **authentication-algorithm** to specify an authentication algorithm for an IKE proposal.

Use **undo authentication-algorithm** to restore the default.

Syntax

authentication-algorithm sha

undo authentication-algorithm

Default

An IKE proposal uses the SHA1 authentication algorithm.

Views

IKE proposal view

Default command level

2: System level

Parameters

sha: Uses HMAC-SHA1.

Examples

```
# Set SHA1 as the authentication algorithm for IKE proposal 10.
```

```
<Sysname> system-view
```

```
[Sysname] ike proposal 10
```

```
[Sysname-ike-proposal-10] authentication-algorithm sha
```

Related commands

- **display ike proposal**
- **ike proposal**

authentication-method

Use **authentication-method** to specify an authentication method for an IKE proposal.

Use **undo authentication-method** to restore the default.

Syntax

authentication-method { pre-share | rsa-signature }

undo authentication-method

Default

An IKE proposal uses the pre-shared key authentication method.

Views

IKE proposal view

Default command level

2: System level

Parameters

pre-share: Uses the pre-shared key method.

rsa-signature: Uses the RSA digital signature method.

Examples

```
# Specify that IKE proposal 10 uses the pre-shared key authentication method.
```

```
<Sysname> system-view
```

```
[Sysname] ike proposal 10
```

```
[Sysname-ike-proposal-10] authentication-method pre-share
```

Related commands

- **display ike proposal**
- **ike proposal**

certificate domain

Use **certificate domain** to configure the PKI domain of the certificate when IKE uses digital signature as the authentication mode.

Use **undo certificate domain** to remove the configuration.

Syntax

certificate domain *domain-name*

undo certificate domain

Views

IKE peer view

Default command level

2: System level

Parameters

domain-name: Name of the PKI domain, a string of 1 to 15 characters.

Examples

Configure the PKI domain as **abcde** for IKE negotiation.

```
<Sysname> system-view
```

```
[Sysname] ike peer peer1
```

```
[Sysname-ike-peer-peer1] certificate domain abcde
```

Related commands

- **authentication-method**
- **pki domain**

dh

Use **dh** to specify the DH group to be used in key negotiation phase 1 for an IKE proposal.

Use **undo dh** to restore the default.

Syntax

dh { group2 | group5 | group14 }

undo dh

Default

Group2, the 1024-bit Diffie-Hellman group, is used.

Views

IKE proposal view

Default command level

2: System level

Parameters

group2: Uses the 1024-bit Diffie-Hellman group for key negotiation in phase 1.

group5: Uses the 1536-bit Diffie-Hellman group for key negotiation in phase 1.

group14: Uses the 2048-bit Diffie-Hellman group for key negotiation in phase 1.

Examples

```
# Specify 1536-bit Diffie-Hellman for IKE proposal 10.
<Sysname> system-view
[Sysname] ike proposal 10
[Sysname-ike-proposal-10] dh group5
```

Related commands

- **display ike proposal**
- **ike proposal**

display ike dpd

Use **display ike dpd** to display information about Dead Peer Detection (DPD) detectors.

Syntax

```
display ike dpd [ dpd-name ] [ | { begin | exclude | include } regular-expression ]
```

Views

Any view

Default command level

1: Monitor level

Parameters

dpd-name: DPD name, a string of 1 to 32 characters.

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

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

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

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

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

Usage guidelines

If you do not specify any parameters, the command displays information about all DPD detectors.

Examples

```
# Display information about all DPD detectors.
<Sysname> display ike dpd
```

```
-----
IKE dpd: dpd1
  references: 1
  interval-time: 10
  time_out: 5
-----
```

Table 7 Command output

Field	Description
references	Number of IKE peers that use the DPD detector.
Interval-time	DPD query triggering interval in seconds.

Field	Description
time_out	DPD packet retransmission interval in seconds.

Related commands

ike dpd

display ike peer

Use **display ike peer** to display information about IKE peers.

Syntax

display ike peer [*peer-name*] [| { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

peer-name: Name of the IKE peer, a string of 1 to 32 characters.

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

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

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

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

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

Usage guidelines

If you do not specify any parameters, the command displays information about all IKE peers.

Examples

Display information about all IKE peers.

```
<Sysname> display ike peer
```

```
-----
IKE Peer: aaa
  exchange mode: main on phase 1
  peer id type: ip
  peer ip address: 0.0.0.0 ~ 255.255.255.255
  local ip address:
  peer name:
  nat traversal: disable
  dpd:
-----
```

Table 8 Command output

Field	Description
exchange mode	IKE negotiation mode in phase 1.

Field	Description
pre-shared-key	Pre-shared key used in phase 1.
peer id type	ID type used in phase 1.
peer ip address	IP address of the remote security gateway.
local ip address	IP address of the local security gateway.
peer name	Name of the remote security gateway.
nat traversal	Whether NAT traversal is enabled.
dpd	Name of the peer DPD detector.

Related commands

ike peer

display ike proposal

Use **display ike proposal** to view the settings of all IKE proposals.

Syntax

display ike proposal [| { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

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

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

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

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

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

Usage guidelines

This command displays the configuration information of all IKE proposals in the descending order of proposal priorities.

Examples

Display the settings of all IKE proposals.

```
<Sysname> display ike proposal
```

```
priority authentication authentication encryption Diffie-Hellman duration
                method      algorithm      algorithm      group          (seconds)
-----
  11      PRE_SHARED      SHA          AES_CBC_128      MODP_1024      86400
default  PRE_SHARED      SHA          AES_CBC_128      MODP_1024      86400
```

Table 9 Command output

Field	Description
priority	Priority of the IKE proposal.
authentication method	Authentication method used by the IKE proposal.
authentication algorithm	Authentication algorithm used by the IKE proposal.
encryption algorithm	Encryption algorithm used by the IKE proposal.
Diffie-Hellman group	DH group used in IKE negotiation phase 1.
duration (seconds)	ISAKMP SA lifetime of the IKE proposal in seconds.

Related commands

- **authentication-algorithm**
- **authentication-method**
- **dh**
- **encryption-algorithm**
- **ike proposal**
- **sa duration**

display ike sa

Use **display ike sa** to display information about the current IKE SAs.

Syntax

```
display ike sa [ verbose [ connection-id connection-id | remote-address remote-address ] ] [ [ { begin | exclude | include } ] regular-expression ]
```

Views

Any view

Default command level

1: Monitor level

Parameters

verbose: Displays detailed information.

connection-id *connection-id*: Displays detailed information about IKE SAs by connection ID, in the range 1 to 2000000000.

remote: Displays detailed information about IKE SAs with a specified remote address.

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

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

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

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

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

Usage guidelines

If you do not specify any parameters or keywords, the command displays brief information about the current IKE SAs.

Examples

Display brief information about the current IKE SAs.

```
<Sysname> display ike sa
total phase-1 SAs: 1
connection-id peer          flag          phase    doi
-----
1             202.38.0.2      RD|ST         1        IPSEC
2             202.38.0.2      RD|ST         2        IPSEC
```

flag meaning

RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT

Table 10 Command output

Field	Description
total phase-1 SAs	Total number of SAs for phase 1.
connection-id	Identifier of the ISAKMP SA.
peer	Remote IP address of the SA.
flag	Status of the SA: <ul style="list-style-type: none">• RD (READY)—The SA has been established.• ST (STAYALIVE)—This end is the initiator of the tunnel negotiation.• RL (REPLACED)—The tunnel has been replaced by a new one and will be deleted later.• FD (FADING)—The soft lifetime is over but the tunnel is still in use. The tunnel will be deleted when the hard lifetime is over.• TO (TIMEOUT)—The SA has received no keepalive packets after the last keepalive timeout. If no keepalive packets are received before the next keepalive timeout, the SA will be deleted.
phase	The phase the SA belongs to: <ul style="list-style-type: none">• Phase 1—The phase for establishing the ISAKMP SA.• Phase 2—The phase for negotiating the security service. IPsec SAs are established in this phase.
doi	Interpretation domain the SA belongs to.

Display detailed information about the current IKE SAs.

```
<Sysname> display ike sa verbose
-----
connection id: 2
vpn-instance: 1
transmitting entity: initiator
-----
local ip: 4.4.4.4
local id type: IPV4_ADDR
local id: 4.4.4.4

remote ip: 4.4.4.5
remote id type: IPV4_ADDR
remote id: 4.4.4.5

authentication-method: PRE-SHARED-KEY
authentication-algorithm: HASH-SHA1
```

encryption-algorithm: AES-CBC

life duration(sec): 86400

remaining key duration(sec): 86379

exchange-mode: MAIN

diffie-hellman group: GROUP1

nat traversal: NO

Display detailed information about the IKE SA with the connection ID of 2.

<Sysname> display ike sa verbose connection-id 2

```
-----
connection id: 2
vpn-instance: vpn1
transmitting entity: initiator
-----
local ip: 4.4.4.4
local id type: IPV4_ADDR
local id: 4.4.4.4

remote ip: 4.4.4.5
remote id type: IPV4_ADDR
remote id: 4.4.4.5

authentication-method: PRE-SHARED-KEY
authentication-algorithm: HASH-SHA1
encryption-algorithm: AES-CBC

life duration(sec): 86400
remaining key duration(sec): 82480
exchange-mode: MAIN
diffie-hellman group: GROUP14
nat traversal: NO
```

Display detailed information about the IKE SA with the remote address of 4.4.4.5.

<Sysname> display ike sa verbose remote-address 4.4.4.5

```
-----
connection id: 2
vpn-instance: vpn1
transmitting entity: initiator
-----
local ip: 4.4.4.4
local id type: IPV4_ADDR
local id: 4.4.4.4

remote ip: 4.4.4.5
remote id type: IPV4_ADDR
remote id: 4.4.4.5

authentication-method: PRE-SHARED-KEY
authentication-algorithm: HASH-SHA1
```

```

encryption-algorithm: DES-CBC

life duration(sec): 86400
remaining key duration(sec): 82236
exchange-mode: MAIN
diffie-hellman group: GROUP1
nat traversal: NO

```

Table 11 Command output

Field	Description
connection id	Identifier of the ISAKMP SA.
vpn-instance	MPLS L3VPN that the protected data belongs to.
transmitting entity	Entity in the IKE negotiation.
local ip	IP address of the local gateway.
local id type	Identifier type of the local gateway.
local id	Identifier of the local gateway.
remote ip	IP address of the remote gateway.
remote id type	Identifier type of the remote gateway.
remote id	Identifier of the remote security gateway.
authentication-method	Authentication method used by the IKE proposal.
authentication-algorithm	Authentication algorithm used by the IKE proposal.
encryption-algorithm	Encryption algorithm used by the IKE proposal.
life duration(sec)	Lifetime of the ISAKMP SA in seconds.
remaining key duration(sec)	Remaining lifetime of the ISAKMP SA in seconds.
exchange-mode	IKE negotiation mode in phase 1.
diffie-hellman group	DH group used for key negotiation in IKE phase 1.
nat traversal	Whether NAT traversal is enabled.

Related commands

- **ike peer**
- **ike proposal**

dpd

Use **dpd** to apply a DPD detector to an IKE peer.

Use **undo dpd** to remove the application.

Syntax

dpd *dpd-name*

undo dpd

Default

No DPD detector is applied to an IKE peer.

Views

IKE peer view

Default command level

2: System level

Parameters

dpd-name: DPD detector name, a string of 1 to 32 characters.

Examples

```
# Apply dpd1 to IKE peer peer1.  
<Sysname> system-view  
[Sysname] ike peer peer1  
[Sysname-ike-peer-peer1] dpd dpd1
```

encryption-algorithm

Use **encryption-algorithm** to specify an encryption algorithm for an IKE proposal.

Use **undo encryption-algorithm** to restore the default.

Syntax

```
encryption-algorithm aes-cbc [ key-length ]  
undo encryption-algorithm
```

Default

The encryption algorithm for an IKE proposal is AES-128.

Views

IKE proposal view

Default command level

2: System level

Parameters

aes-cbc: Uses the AES algorithm in CBC mode as the encryption algorithm. The AES algorithm uses 128-bit, 192-bit, or 256-bit keys for encryption.

key-length: Key length for the AES algorithm, which can be 128, 192 or 256 bits and is defaulted to 128 bits.

Examples

```
# Use 128-bit AES in CBC mode as the encryption algorithm for IKE proposal 10.  
<Sysname> system-view  
[Sysname] ike proposal 10  
[Sysname-ike-proposal-10] encryption-algorithm aes 128
```

Related commands

- **display ike proposal**
- **ike proposal**

exchange-mode

Use **exchange-mode** to select an IKE negotiation mode.

Use **undo exchange-mode** to restore the default.

Syntax

exchange-mode main
undo exchange-mode

Default

Main mode is used.

Views

IKE peer view

Default command level

2: System level

Parameters

main: Main mode.

Examples

```
# Specify that IKE negotiation works in main mode.  
<Sysname> system-view  
[Sysname] ike peer peer1  
[Sysname-ike-peer-peer1] exchange-mode main
```

Related commands

id-type

id-type

Use **id-type** to select the type of the ID for IKE negotiation.

Use **undo id-type** to restore the default.

Syntax

id-type { ip | name | user-fqdn }
undo id-type

Default

The ID type is IP address.

Views

IKE peer view

Default command level

2: System level

Parameters

ip: Uses an IP address as the ID during IKE negotiation.

name: Uses a FQDN name as the ID during IKE negotiation.

user-fqdn: Uses a user FQDN name as the ID during IKE negotiation.

Usage guidelines

In main mode, only the ID type of IP address can be used in IKE negotiation and SA creation.

Examples

```
# Use the ID type of name during IKE negotiation.
```



```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] id-type name
```

Related commands

- **exchange-mode**
- **ike local-name**
- **local-address**
- **local-name**
- **remote-address**
- **remote-name**

ike dpd

Use **ike dpd** to create a DPD detector and enter IKE DPD view.

Use **undo ike dpd** to remove a DPD detector.

Syntax

```
ike dpd dpd-name
undo ike dpd dpd-name
```

Views

System view

Default command level

2: System level

Parameters

dpd-name: Name for the dead peer detection (DPD) detector, a string of 1 to 32 characters.

Usage guidelines

Dead peer detection (DPD) irregularly detects dead IKE peers. It works as follows:

1. When the local end sends an IPsec packet, it checks the time the last IPsec packet was received from the peer.
2. If the time interval exceeds the DPD interval, it sends a DPD hello to the peer.
3. If the local end receives no DPD acknowledgement within the DPD packet retransmission interval, it retransmits the DPD hello.
4. If the local end still receives no DPD acknowledgement after having made the maximum number of retransmission attempts (two by default), it considers the peer already dead, and clears the IKE SA and the IPsec SAs based on the IKE SA.

DPD enables an IKE entity to check the liveliness of its peer only when necessary. It generates less traffic than the keepalive mechanism, which exchanges messages periodically.

Examples

Create a DPD detector named **dpd2**.

```
<Sysname> system-view
[Sysname] ike dpd dpd2
```

Related commands

- **display ike dpd**
- **interval-time**

- **time-out**

ike local-name

Use **ike local-name** to configure a name for the local security gateway.

Use **undo ike local-name** to restore the default.

Syntax

ike local-name *name*

undo ike local-name

Default

The device name is used as the name of the local security gateway.

Views

System view

Default command level

2: System level

Parameters

name: Name of the local security gateway for IKE negotiation, a case-sensitive string of 1 to 32 characters.

Usage guidelines

If you configure the **id-type name** or **id-type user-fqdn** command on the initiator, the IKE negotiation peer uses the security gateway name as its ID to initiate IKE negotiation, and you must configure the **ike local-name** command in system view or the **local-name** command in IKE peer view on the local device. If you configure both the **ike local-name** command and the **local-name** command, the name configured by the **local-name** command is used.

The IKE negotiation initiator sends its security gateway name as its ID to the peer, and the peer uses the security gateway name configured with the **remote-name** command to authenticate the initiator. Make sure the local gateway name matches the remote gateway name configured on the peer.

Examples

Configure the local security gateway name as **app**.

```
<Sysname> system-view
```

```
[Sysname] ike local-name app
```

Related commands

id-type

remote-name

ike next-payload check disabled

Use **ike next-payload check disabled** to disable the checking of the Next payload field in the last payload of an IKE message during IKE negotiation, gaining interoperability with products assigning the field a value other than zero.

Use **undo ike next-payload check disabled** to restore the default.

Syntax

ike next-payload check disabled

undo ike next-payload check disabled

Default

The Next payload field is checked.

Views

System view

Default command level

2: System level

Examples

Disable Next payload field checking for the last payload of an IKE message.

```
<Sysname> system-view
```

```
[Sysname] ike next-payload check disabled
```

ike peer (system view)

Use **ike peer** to create an IKE peer and enter IKE peer view.

Use **undo ike peer** to delete an IKE peer.

Syntax

ike peer *peer-name*

undo ike peer *peer-name*

Views

System view

Default command level

2: System level

Parameters

peer-name: IKE peer name, a string of 1 to 32 characters.

Examples

Create an IKE peer named peer1 and enter IKE peer view.

```
<Sysname> system-view
```

```
[Sysname] ike peer peer1
```

```
[Sysname-ike-peer-peer1]
```

ike proposal

Use **ike proposal** to create an IKE proposal and enter IKE proposal view.

Use **undo ike proposal** to delete an IKE proposal.

Syntax

ike proposal *proposal-number*

undo ike proposal *proposal-number*

Views

System view

Default command level

2: System level

Parameters

proposal-number: IKE proposal number, in the range 1 to 65535. The lower the number, the higher the priority of the IKE proposal. During IKE negotiation, a high priority IKE proposal is matched before a low priority IKE proposal.

Usage guidelines

The system provides a default IKE proposal, which has the lowest priority and uses these settings:

- Encryption algorithm AES-128.
- Authentication algorithm HMAC-SHA1.
- Authentication method Pre-shared key.
- DH group MODP_1024.
- SA lifetime 86400 seconds.

Examples

Create IKE proposal 10 and enter IKE proposal view.

```
<Sysname> system-view
[Sysname] ike proposal 10
[Sysname-ike-proposal-10]
```

Related commands

display ike proposal

ike sa keepalive-timer interval

Use **ike sa keepalive-timer interval** to set the ISAKMP SA keepalive interval.

Use **undo ike sa keepalive-timer interval** to disable the ISAKMP SA keepalive transmission function.

Syntax

ike sa keepalive-timer interval *seconds*

undo ike sa keepalive-timer interval

Default

No keepalive packet is sent.

Views

System view

Default command level

2: System level

Parameters

seconds: Transmission interval of ISAKMP SA keepalives in seconds, in the range 20 to 28,800.

Usage guidelines

The keepalive interval configured at the local end must be shorter than the keepalive timeout configured at the remote end.

Examples

Set the keepalive interval to 200 seconds.

```
<Sysname> system-view
[Sysname] ike sa keepalive-timer interval 200
```

Related commands

ike sa keepalive-timer timeout

ike sa keepalive-timer timeout

Use **ike sa keepalive-timer timeout** to set the ISAKMP SA keepalive timeout.

Use **undo ike sa keepalive-timer timeout** to disable the function.

Syntax

ike sa keepalive-timer timeout *seconds*

undo ike sa keepalive-timer timeout

Default

No keepalive packet is sent.

Views

System view

Default command level

2: System level

Parameters

seconds: ISAKMP SA keepalive timeout in seconds, in the range 20 to 28800.

Usage guidelines

The keepalive timeout configured at the local end must be longer than the keepalive interval configured at the remote end. Since it seldom occurs that more than three consecutive packets are lost on a network, the keepalive timeout can be configured to be three times of the keepalive interval.

Examples

```
# Set the keepalive timeout to 20 seconds.  
<Sysname> system-view  
[Sysname] ike sa keepalive-timer timeout 20
```

Related commands

ike sa keepalive-timer interval

ike sa nat-keepalive-timer interval

Use **ike sa nat-keepalive-timer interval** to set the NAT keepalive interval.

Use **undo ike sa nat-keepalive-timer interval** to disable the function.

Syntax

ike sa nat-keepalive-timer interval *seconds*

undo ike sa nat-keepalive-timer interval

Default

The NAT keepalive interval is 20 seconds.

Views

System view

Default command level

2: System level

Parameters

seconds: NAT keepalive interval in seconds, in the range 5 to 300.

Examples

```
# Set the NAT keepalive interval to 5 seconds.
<Sysname> system-view
[Sysname] ike sa nat-keepalive-timer interval 5
```

interval-time

Use **interval-time** to set the DPD query triggering interval for a DPD detector.

Use **undo interval-time** to restore the default.

Syntax

```
interval-time interval-time
undo interval-time
```

Default

The DPD interval is 10 seconds.

Views

IKE DPD view

Default command level

2: System level

Parameters

interval-time: Sets DPD interval in seconds, in the range of 1 to 300 seconds. When the local end sends an IPsec packet, it checks the time the last IPsec packet was received from the peer. If the time interval exceeds the DPD interval, it sends a DPD hello to the peer.

Examples

```
# Set the DPD interval to 1 second for dpd2.
<Sysname> system-view
[Sysname] ike dpd dpd2
[Sysname-ike-dpd-dpd2] interval-time 1
```

local-address

Use **local-address** to configure the IP address of the local security gateway in IKE negotiation.

Use **undo local-address** to remove the configuration.

Syntax

```
local-address ip-address
undo local-address
```

Default

The primary address of the interface referencing the IPsec policy is used as the local security gateway IP address for IKE negotiation.

Views

IKE peer view

Default command level

2: System level

Parameters

ip-address: IP address of the local security gateway to be used in IKE negotiation.

Usage guidelines

Use this command if you want to specify a different address for the local security gateway.

Examples

```
# Set the IP address of the local security gateway to 1.1.1.1.
<Sysname> system-view
[Sysname] ike peer xhy
[Sysname-ike-peer-xhy] local-address 1.1.1.1
```

local-name

Use **local-name** to configure a name for the local security gateway to be used in IKE negotiation.

Use **undo local-name** to restore the default.

Syntax

```
local-name name
undo local-name
```

Default

The device name is used as the name of the local security gateway view.

Views

IKE peer view

Default command level

2: System level

Parameters

name: Name for the local security gateway to be used in IKE negotiation, a case-sensitive string of 1 to 32 characters.

Usage guidelines

If you configure the **id-type name** or **id-type user-fqdn** command on the initiator, the IKE negotiation peer uses the security gateway name as its ID to initiate IKE negotiation, and you must configure the **ike local-name** command in system view or the **local-name** command in IKE peer view on the local device. If you configure both the **ike local-name** command and the **local-name** command, the name configured by the **local-name** command is used.

The IKE negotiation initiator sends its security gateway name as its ID to the peer, and the peer uses the security gateway name configured with the **remote-name** command to authenticate the initiator. Make sure the local gateway name matches the remote gateway name configured on the peer.

Examples

```
# Set the name of the local security gateway to localgw in IKE peer view of peer1.
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] local-name localgw
```

Relate commands

- **id-type**
- **remote-name**

nat traversal

Use **nat traversal** to enable the NAT traversal function of IKE/IPsec.

Use **undo nat traversal** to disable the NAT traversal function of IKE/IPsec.

Syntax

nat traversal

undo nat traversal

Default

The NAT traversal function is disabled.

Views

IKE peer view

Default command level

2: System level

Examples

Enable the NAT traversal function for IKE peer peer1.

```
<Sysname> system-view
```

```
[Sysname] ike peer peer1
```

```
[Sysname-ike-peer-peer1] nat traversal
```

peer

Use **peer** to set the subnet type of the peer security gateway for IKE negotiation.

Use **undo peer** to restore the default.

Syntax

peer { multi-subnet | single-subnet }

undo peer

Default

The subnet is a single one.

Views

IKE peer view

Default command level

2: System level

Parameters

multi-subnet: Sets the subnet type to multiple.

single-subnet: Sets the subnet type to single.

Usage guidelines

Use this command to enable interoperability with a NetScreen device.

Examples

Set the subnet type of the peer security gateway to **multiple**.

```
<Sysname> system-view
[Sysname] ike peer xhy
[Sysname-ike-peer-xhy] peer multi-subnet
```

pre-shared-key

Use **pre-shared-key** to configure the pre-shared key to be used in IKE negotiation.

Use **undo pre-shared-key** to remove the configuration.

Syntax

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

undo pre-shared-key

Views

IKE peer view

Default command level

2: System level

Parameters

key: Plaintext pre-shared key to be displayed in cipher text, a case-sensitive string of 8 to 128 characters.

cipher *key*: Specifies the ciphertext pre-shared key to be displayed in cipher text, a case-sensitive string of 8 to 201 characters.

simple *key*: Specifies the plaintext pre-shared key to be displayed in plain text, a case-sensitive string of 8 to 128 characters.

Examples

Set the pre-shared key used in IKE negotiation to AAbbcc1234%.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] pre-shared-key AAbbcc1234%
```

Related commands

authentication-method

proposal (IKE peer view)

Use **proposal** to specify the IKE proposals for the IKE peer to reference.

Use **undo proposal** to remove one or all IKE proposals referenced by the IKE peer.

Syntax

proposal *proposal-number*<1-6>

undo proposal [*proposal-number*]

Default

An IKE peer references no IKE proposals and, when initiating IKE negotiation, it uses the IKE proposals configured in system view.

Views

IKE peer view

Default command level

2: System level

Parameters

proposal-number&<1-6>: Sequence number of the IKE proposal for the IKE peer to reference, in the range 1 to 65535. &<1-6> means that you can specify the *proposal-number* argument for up to six times. An IKE proposal with a smaller sequence number has a higher priority.

Usage guidelines

In the IKE negotiation phase 1, the local peer uses the IKE proposals specified for it, if any.

An IKE peer can reference up to six IKE proposals.

The responder uses the IKE proposals configured in system view for negotiation.

Examples

Configure IKE peer **peer1** to reference IKE proposal **10**.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] proposal 10
```

Related commands

- **ike proposal**
- **ike peer** (system view)

remote-address

Use **remote-address** to configure the IP address of the IPsec remote security gateway.

Use **undo remote-address** to remove the configuration.

Syntax

remote-address { *hostname* [**dynamic**] | *low-ip-address* [*high-ip-address*] }

undo remote-address

Views

IKE peer view

Default command level

2: System level

Parameters

hostname: Host name of the IPsec remote security gateway, a case-insensitive string of 1 to 255 characters. The host name uniquely identifies the remote IPsec peer and can be resolved to an IP address by the DNS server.

dynamic: Specifies to use dynamic address resolution for the IPsec remote peer name. If you do not provide this keyword, the local peer has the remote host name resolved only once after you configure the remote host name.

low-ip-address: IP address of the IPsec remote security gateway. It is the lowest address in the address range if you want to specify a range of addresses.

high-ip-address: Highest address in the address range if you want to specify a range of addresses.

Usage guidelines

The IP address configured with the **remote-address** command must match the local security gateway IP address that the remote security gateway uses for IKE negotiation, which is the IP address configured with the **local-address** command or, if the **local-address** command is not configured, the primary IP address of the interface to which the policy is applied.

The local peer can be the initiator of IKE negotiation if the remote address is a host IP address or a host name. The local end can only be the responder of IKE negotiation if the remote address is an address range that the local peer can respond to.

If the IP address of the remote address changes frequently, configure the host name of the remote gateway with the **dynamic** keyword so that the local peer can use the up-to-date remote IP address to initiate IKE negotiation.

Examples

Configure the IP address of the remote security gateway as 10.0.0.1.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] remote-address 10.0.0.1
```

Configure the host name of the remote gateway as **test.com**, and specify the local peer to dynamically update the remote IP address.

```
<Sysname> system-view
[Sysname] ike peer peer2
[Sysname-ike-peer-peer2] remote-address test.com dynamic
```

Related commands

- **id-type ip**
- **local-address**

remote-name

Use **remote-name** to configure the name of the remote gateway.

Use **undo remote-name** to remove the configuration.

Syntax

```
remote-name name
undo remote-name
```

Views

IKE peer view

Default command level

2: System level

Parameters

name: Name of the peer security gateway for IKE negotiation, a string of 1 to 32 characters.

Usage guidelines

If you configure the **id-type name** or **id-type user-fqdn** command on the initiator, the IKE negotiation initiator sends its security gateway name as its ID for IKE negotiation, and the peer uses the security gateway name configured with the **remote-name** command to authenticate the initiator. Make sure the local gateway name matches the remote gateway name configured on the peer.

Examples

Configure the remote security gateway name as **apple** for IKE peer peer1.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] remote-name apple
```

Related commands

- **id-type**
- **ike local-name**
- **local-name**

reset ike sa

Use **reset ike sa** to clear IKE SAs.

Syntax

```
reset ike sa [ connection-id ]
```

Views

User view

Default command level

2: System level

Parameters

connection-id: Connection ID of the IKE SA to be cleared, in the range 1 to 2000000000.

Usage guidelines

If you do not specify a connection ID, the command clears all ISAKMP SAs.

When you clear a local IPsec SA, its ISAKMP SA can transmit the Delete message to notify the remote end to delete the paired IPsec SA. If the ISAKMP SA has been cleared, the local end cannot notify the remote end to clear the paired IPsec SA, and you must manually clear the remote IPsec SA.

Examples

Clear an IPsec tunnel to 202.38.0.2.

```
<Sysname> display ike sa
total phase-1 SAs: 1
connection-id peer          flag          phase   doi
-----
1             202.38.0.2    RD|ST         1       IPSEC
2             202.38.0.2    RD|ST         2       IPSEC
```

flag meaning

RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT

```
<Sysname> reset ike sa 2
```

```
<Sysname> display ike sa
total phase-1 SAs: 1
connection-id peer          flag          phase   doi
-----
1             202.38.0.2    RD|ST         1       IPSEC
```

flag meaning

RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT

Related commands

display ike sa

sa duration

Use **sa duration** to set the ISAKMP SA lifetime for an IKE proposal.

Use **undo sa duration** to restore the default.

Syntax

sa duration *seconds*

undo sa duration

Default

The ISAKMP SA lifetime is 86400 seconds.

Views

IKE proposal view

Default command level

2: System level

Parameters

Seconds: Specifies the ISAKMP SA lifetime in seconds, in the range 60 to 604800.

Usage guidelines

Before an SA expires, IKE negotiates a new SA. The new SA takes effect immediately after being set up, and the old one will be cleared automatically when it expires.

Examples

```
# Specify the ISAKMP SA lifetime for IKE proposal 10 as 600 seconds (10 minutes).
<Sysname> system-view
[Sysname] ike proposal 10
[Sysname-ike-proposal-10] sa duration 600
```

Related commands

- **display ike proposal**
- **ike proposal**

time-out

Use **time-out** to set the DPD packet retransmission interval for a DPD detector.

Use **undo time-out** to restore the default.

Syntax

time-out *time-out*

undo time-out

Default

The DPD packet retransmission interval is 5 seconds.

Views

IKE DPD view

Default command level

2: System level

Parameters

time-out: DPD packet retransmission interval in seconds, in the range 1 to 60.

Examples

```
# Set the DPD packet retransmission interval to 1 second for dpd2.
<Sysname> system-view
[Sysname] ike dpd dpd2
[Sysname-ike-dpd-dpd2] time-out 1
```

New feature: Configuring the log file overwrite-protection function

Configuring the log file overwrite-protection function

In FIPS mode, after the log file overwrite-protection function is enabled, when the storage space is not enough or the quota for log files reaches the limit, the device shuts down all physical Ethernet ports except the management Ethernet port, Ethernet ports configured with stateful failover, and physical IRF ports that have been bound to an IRF port.

Command reference

info-center logfile overwrite-protection

Use **info-center logfile overwrite-protection** to enable the log file overwrite-protection function. When the storage space is not enough or the quota for log files reaches the limit, new logs cannot be written into the log files.

Use **undo info-center logfile overwrite-protection** to disable the log file overwrite-protection function. When the storage space is not enough or the quota for log files reaches the limit, the device deletes the old logs in the log files and write new logs into the log files.

Syntax

info-center logfile overwrite-protection [all-port-powerdown]

undo info-center logfile overwrite-protection

Default

The log file overwrite-protection function is not enabled.

Views

System view

Default command level

2: System level

Parameters

all-port-powerdown: Shuts down all physical Ethernet ports except the management Ethernet port, Ethernet ports configured with stateful failover, and physical IRF ports that have been bound to an IRF port when the number of log files reaches the upper limit or the storage space is not enough.

Examples

```
# Enable the log file overwrite-protection function.
<Sysname> system-view
[Sysname] info-center logfile overwrite-protection
```

New feature: Verifying the correctness and integrity of the file

Verifying the correctness and integrity of the file

Task	Command	Remarks
Verify the correctness and integrity of the file.	crypto-digest sha256 file <i>file-url</i>	Available in user view.

Command reference

crypto-digest

Use **crypto-digest** to calculate the digest value of a specific file.

Syntax

```
crypto-digest sha256 file file-url
```

Views

User view

Default command level

2: System level

Parameters

sha256: Specifies the digest algorithm SHA-256.

file *file-url*: Specifies a filename.

Usage guidelines

The digest value of a file is used to verify the correctness and integrity of the file. For example, you can use this command to calculate the digest value of a software package on your switch and compare it with the digest value issued by HP for the software package. If the two values are identical, it means that the package on your switch is the correct one.

Examples

```
# Use SHA-256 to calculate the digest value of the file 1.bin.
<Sysname> crypto-digest sha256 file 1.bin
Computing digest...
SHA256 digest(1.bin)=7bcb92458222f91f9a09a807c4c4567efd4d5dc4e4abc06c2a741df7045433eb
```

New feature: Displaying per-port queue-based traffic statistics

Displaying per-port queue-based traffic statistics

Per-port queue-based accounting collects statistics for each port on a per-queue basis, such as the number of packets buffered in each queue, the number of packets sent out of each queue, and the number of packets dropped in each queue.

To display per-port queue-based traffic statistics:

Task	Command	Remarks
Display per-port queue-based traffic statistics.	display qos queue-statistics interface [<i>interface-type interface-number</i>] [outbound] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.

Command reference

display qos queue-statistics

Use **display qos queue-statistics interface** to display statistics collected for an interface on a per-queue basis.

Syntax

display qos queue-statistics interface [*interface-type interface-number*] [**outbound**] [| { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

outbound: Displays queue-based outbound traffic statistics.

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

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

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

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

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

Usage guidelines

If no interface is specified, this command displays statistics for all interfaces.

Examples

Display queue-based traffic statistics in the outbound direction of GigabitEthernet 1/0/1.

```
<Sysname> display qos queue-statistics interface gigabitethernet 1/0/1
```

```
Interface: GigabitEthernet1/0/1
```


Direction: Outbound

Queue	Queued packets	Passed packets	Dropped packets
0	0	0	0
1	0	0	0
2	2,689	94,816,515	94,851,667
3	0	0	0
4	0	0	0
5	0	0	0
6	0	0	0
7	0	26	0

Table 12 Command output

Field	Description
Interface	Interface for which queue-based traffic statistics are displayed.
Direction	Direction of traffic for which statistics are collected.
Queued packets	Number of packets buffered in the queue.
Passed packets	Number of packets sent out of the queue.
Dropped packets	Number of packets dropped in the queue.

Modified feature: Configuring MAC authentication timers

Feature change description

Changed the *offline-detect-value* argument.

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 of the *offline-detect-value* argument ranges from 60 to 65535.

After modification: The value of the *offline-detect-value* argument ranges from 60 to 2147483647.

Modified feature: NTP

Feature change description

Added NTP version 4.

Command changes

Modified command: ntp-service broadcast-server

syntax

ntp-service broadcast-server [**authentication-keyid** *keyid* | **version** *number*] *

Views

Layer 3 Ethernet interface view, VLAN interface view

Change description

Before modification: The value of the *number* argument ranges from 1 to 3.

After modification: The value of the *number* argument ranges from 1 to 4.

Modified command: ntp-service multicast-server

syntax

ntp-service multicast-server [*ip-address*] [**authentication-keyid** *keyid* | **ttl** *ttl-number* | **version** *number*] *

Views

Layer 3 Ethernet interface view, VLAN interface view

Change description

Before modification: The value of the *number* argument ranges from 1 to 3.

After modification: The value of the *number* argument ranges from 1 to 4.

Modified command: ntp-service unicast-peer

syntax

ntp-service unicast-peer [**vpn-instance** *vpn-instance-name*] { *ip-address* | *peer-name* } [**authentication-keyid** *keyid* | **priority** | **source-interface** *interface-type interface-number* | **version** *number*] *

Views

System view

Change description

Before modification: The value of the *number* argument ranges from 1 to 3.

After modification: The value of the *number* argument ranges from 1 to 4.

Modified command: ntp-service unicast-server

syntax

ntp-service unicast-server [**vpn-instance** *vpn-instance-name*] { *ip-address* | *server-name* } [**authentication-keyid** *keyid* | **priority** | **source-interface** *interface-type interface-number* | **version** *number*] *

Views

System view

Change description

Before modification: The value of the *number* argument ranges from 1 to 3.

After modification: The value of the *number* argument ranges from 1 to 4.

Modified feature: Configuring a password for the local user

Feature change description

Supported password to be saved by hash encryption algorithm and displayed as hash value.

Command changes

Modified command: password (local user view)

Old syntax

```
password [ { cipher | simple } password ]
```

New syntax

```
password [ [hash] { cipher | simple } password ]
```

Views

Local user view

Change description

Before modification:

- Both ciphertext and plaintext passwords are supported.
- A plaintext password is a string of 1 to 63 characters. A ciphertext password is a string of 1 to 117 characters.

After modification:

- Both ciphertext and plaintext passwords are supported. The password is saved by hash encryption algorithm and displayed as hash value.
- If you do not specify hash encryption algorithm, a plaintext password is a string of 1 to 63 characters and a ciphertext password is a string of 1 to 117 characters.
- If you specify hash encryption algorithm, a plaintext password is a string of 1 to 63 characters and a ciphertext password is a string of 1 to 110 characters.

Modified feature: 802.1X critical VLAN

Feature change description

The events that trigger an 802.1X user to be removed from the 802.1X critical VLAN change in this release. Any of the following events reflects that a RADIUS authentication server is reachable:

- An authentication server is added.
- A response from a RADIUS authentication server is received.
- The RADIUS server probing function detects that a RADIUS authentication server is reachable.

Command changes

None.

Modified feature: MAC authentication critical VLAN

Feature change description

The events that trigger an user to be removed from the MAC authentication critical VLAN change in this release. Any of the following events reflects that a RADIUS authentication server is reachable:

- An authentication server is added.
- A response from a RADIUS authentication server is received.
- The RADIUS server probing function detects that a RADIUS authentication server is reachable.

Command changes

None.

Modified feature: Modifying CLI configuration commands executed in FIPS mode for CC evaluation

Feature change description

Changed CLI configuration command keywords and value ranges when the device is operating in FIPS mode.

Modified command: super password

Old syntax

```
super password [ level user-level ] { cipher | simple } password  
undo super password [ level user-level ]
```

New syntax

In non-FIPS mode:

```
super password [ level user-level ] [ hash ] { cipher | simple } password  
undo super password [ level user-level ]
```

In FIPS mode:

```
super password [ level user-level ] { cipher | simple } password  
undo super password [ level user-level ]
```

Views

2: System level

Parameters

level *user-level*: User privilege level, which ranges from 1 to 3 and defaults to 3.

Hash: Specifies hash encryption algorithm for generating password. (This keyword is not available for FIPS mode.)

cipher: Sets a ciphertext password for user privilege level switching.

simple: Sets a plaintext password for user privilege level switching.

password: Password string, case sensitive. Change description

In FIPS mode, the password must contain uppercase and lowercase letters, digits, and special characters.

In non-FIPS mode:

- If you specify the **simple** keyword, the password is a plaintext string 1 to 16 characters.
- If you specify the **cipher** and **hash** keywords, the password is a ciphertext string of 1 to 110 characters.
- If you specify the **cipher** keyword only, the password is a ciphertext string of 1 to 53 characters.

In FIPS mode:

- If you specify the **simple** keyword, the password is a plaintext string of 8 to 16 characters.
- If you specify the **cipher** keyword, the password is a ciphertext string of 8 to 53 characters.

Change description

After modification:

- In non-FIPS mode
 - The **hash** keyword was added to support hash encryption algorithm for generating passwords for user privilege level switching.
 - The length of the ciphertext password was changed. A ciphertext password can be a string of 1 to 53 characters, or 1 to 110 characters with the **hash** keyword specified.
- In FIPS mode
 - The length of a plaintext password was changed to be a string of 8 to 16 characters.
 - The length of a ciphertext password was changed to be a string of 8 to 53 characters.
 - The password string must contain uppercase and lowercase letters, digits, and special characters.

Modified feature: Modifying login management commands executed in FIPS mode for CC evaluation

Feature change description

- Changed related command keywords and value ranges when the device is operating in FIPS mode.
- Added restrictions to related commands when the device is operating in FIPS mode: The commands **lock**, **user privilege level**, and **set authentication password** are not supported in FIPS mode.

Command changes

Modified command: authentication-mode

Use **authentication-mode** to set the authentication mode for the user interface.

Use **undo authentication-mode** to restore the default.

Old syntax

authentication-mode { **none** | **password** | **scheme** }

undo authentication-mode

New syntax

In non-FIPS mode:

authentication-mode { none | password | scheme }

undo authentication-mode

In FIPS mode:

authentication-mode scheme

undo authentication-mode

Default

In non-FIPS mode, the default authentication mode for VTY user interfaces is **password**, and for AUX user interfaces is **none**.

In FIPS mode, the default authentication mode is **scheme**.

Views

User interface view

Default command level

3: Manage level

Parameters

none: Performs no authentication. This keyword is not available for FIPS mode.

password: Performs local password authentication. This keyword is not available for FIPS mode.

scheme: Performs AAA authentication.

Change description

After modification: In FIPS mode, only the authentication mode **scheme** is supported and the keywords **none** and **password** are deleted.

Modified command: protocol inbound

Use **protocol inbound** to enable the current user interface to support either Telnet, SSH, or all of them. The configuration takes effect next time you log in.

Use **undo protocol inbound** to restore the default.

Old syntax

protocol inbound { all | ssh | telnet }

undo protocol inbound

New syntax

In non-FIPS mode:

protocol inbound { all | ssh | telnet }

undo protocol inbound

In FIPS mode:

protocol inbound { all | ssh }

undo protocol inbound

Default

All the three protocols are supported.

Views

VTY interface view

Default command level

3: Manage level

Parameters

all: Specifies both Telnet and SSH in non-FIPS mode, and only SSH in FIPS mode.

ssh: Specifies SSH only.

telnet: Specifies Telnet only. This keyword is not available for FIPS mode.

Change description

After modification: In FIPS mode, Telnet is not supported.

Modified command: set authentication password

In non-FIPS mode:

Use **set authentication password** to set an authentication password.

Use **undo set authentication password** to remove the local authentication password.

Old syntax

set authentication password { cipher | simple } password

undo set authentication password

New syntax

set authentication password [hash] { cipher | simple } password

undo set authentication password

Default

No local authentication password is set.

Views

User interface view

Default command level

3: Manage level

Parameters

Hash: Specifies hash encryption algorithm for generating password. (This keyword is not available for FIPS mode.)

cipher: Sets a ciphertext password for authentication.

simple: Sets a plaintext password for authentication.

- If you specify the **simple** keyword, the password is a plaintext string 1 to 16 characters.
- If you specify the **cipher** and **hash** keywords, the password is a ciphertext string of 1 to 110 characters.
- If you specify the **cipher** keyword only, the password is a ciphertext string of 1 to 53 characters.

Usage guidelines

For secrecy, all passwords, including passwords configured in plain text, are saved in cipher text.

This command is not supported in FIPS mode.

Change description

After modification: In non-FIPS mode,

- The **hash** keyword was added to support hash encryption algorithm for generating passwords for user privilege level switching.
- The length of the ciphertext password was changed. A ciphertext password can be a string of 1 to 53 characters, or 1 to 110 characters with the **hash** keyword specified.

Modified Feature: Modifying software upgrade commands executed in FIPS mode for CC evaluation

Feature change description

Added verification to the signatures of the system software image, Boot ROM image, and path files when the device is operating in FIPS mode.

- The system verifies the signature of the system software image after you execute the commands **boot-loader** and **boot-loader update file**. If the verification succeeds, the commands take effect.
- The system verifies the signature of the Boot ROM image after you execute the command **bootrom**. If the verification succeeds, the command takes effect.
- The system verifies the signatures of the path files after you execute the commands **patch install** and **patch load**. If the verification succeeds, the commands take effect.

Command changes

None.

Modified Feature: Modifying configuration file management commands executed in FIPS mode for CC evaluation

Feature change description

The **backup startup-configuration** and **restore startup-configuration** commands are not supported when the device is operating in FIPS mode.

Command changes

N/A

Modified Feature: Modifying security commands executed in FIPS mode for CC evaluation

Feature change description

Changed related security command keywords and value ranges when the device is operating in FIPS mode.

Command changes

Modified command: key (HWTACACS scheme view)

Syntax

```
key { accounting | authentication | authorization } [ cipher | simple ] key  
undo key { accounting | authentication | authorization }
```

Views

HWTACACS scheme view

Default command level

2: System level

Change description

Before modification: The *key* argument specifies the plaintext or ciphertext key string and must contain at least 1 character.

After modification: In FIPS mode, the *key* argument specifies the plaintext or ciphertext key string and must contain at least 8 characters.

Modified command: key (RADIUS scheme view)

Syntax

```
key { accounting | authentication } [ cipher | simple ] key  
undo key { accounting | authentication }
```

Views

RADIUS scheme view

Default command level

2: System level

Change description

Before modification: The *key* argument specifies the plaintext or ciphertext key string and must contain at least 1 character.

After modification: In FIPS mode, the *key* argument specifies the plaintext or ciphertext key string and must contain at least 8 characters.

Modified command: password

Old syntax

```
password [ [ hash ] { cipher | simple } password ]  
undo password
```

New syntax

In non-FIPS mode:

```
password [ [ hash ] { cipher | simple } password ]  
undo password
```

In FIPS mode:

```
password
```

undo password

Views

Local user view

Default command level

2: System level

Change description

In FIPS mode, parameters [**hash**] { **cipher** | **simple** } *password* are deleted.

The FIPS mode must operate with the password control feature. You always set the password in interactive mode. To use the interactive mode, enable the password control feature by the **password-control enable** command, and then do not specify any option for this command. For more information about password control commands, see the chapter "Password control configuration commands."

When password control is enabled, the password attributes, such as the password length and complexity, are under the restriction of the password control, and the local user password will not be displayed.

Modified command: primary accounting (RADIUS scheme view)

Syntax

primary accounting { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** [**cipher** | **simple**] *key* | **vpn-instance** *vpn-instance-name*] *

undo primary accounting

Views

RADIUS scheme view

Default command level

2: System level

Change description

Before modification: The *key* argument specifies the plaintext or ciphertext key string and must contain at least 1 character.

After modification: In FIPS mode, the *key* argument specifies the plaintext or ciphertext key string and must contain at least 8 characters.

Modified command: primary authentication (RADIUS scheme view)

Syntax

primary authentication { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** [**cipher** | **simple**] *key* | **vpn-instance** *vpn-instance-name* | **probe username** *name* [**interval** *interval*]] *

undo primary authentication

Views

RADIUS scheme view

Default command level

2: System level

Change description

Before modification: The *key* argument specifies the plaintext or ciphertext key string and must contain at least 1 character.

After modification: In FIPS mode, the *key* argument specifies the plaintext or ciphertext key string and must contain at least 8 characters.

Modified command: secondary accounting (RADIUS scheme view)

Syntax

secondary accounting { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** [**cipher** | **simple**] *key* | **vpn-instance** *vpn-instance-name*] *

undo secondary accounting [*ipv4-address* | **ipv6** *ipv6-address*]

Views

RADIUS scheme view

Default command level

2: System level

Change description

Before modification: The *key* argument specifies the plaintext or ciphertext key string and must contain at least 1 character.

After modification: In FIPS mode, the *key* argument specifies the plaintext or ciphertext key string and must contain at least 8 characters.

Modified command: secondary authentication (RADIUS scheme view)

Syntax

secondary authentication { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** [**cipher** | **simple**] *key* | **vpn-instance** *vpn-instance-name* | **probe username** *name* [**interval** *interval*]] *

undo secondary authentication [*ipv4-address* | **ipv6** *ipv6-address*]

Views

RADIUS scheme view

Default command level

2: System level

Change description

Before modification: The *key* argument specifies the plaintext or ciphertext key string and must contain at least 1 character.

After modification: In FIPS mode, the *key* argument specifies the plaintext or ciphertext key string and must contain at least 8 characters.

Modified command: password-control composition

Syntax

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

undo password-control composition

Views

System view, user group view, local user view

Default command level

2: System level

Change description

Before modification:

- The value range for the *type-number* argument is 1 to 4.
- The default global password composition policy is as follows: the minimum number of password composition types is 1 and the minimum number of characters of a password composition type is 1.

After modification:

- In FIPS mode, the value of the *type-number* argument must be 4.
- In FIPS mode, the default global password composition policy is as follows: the minimum number of password composition types is 4 and the minimum number of characters of a password composition type is 1.

Modified command: password-control length

Syntax

password-control length *length*

undo password-control length

Views

System view, user group view, local user view

Default command level

2: System level

Change description

Before modification: The *length* argument specifies the minimum password length in the range of 4 to 32.

After modification: The value range for the *length* argument is 8 to 32.

Modified command: password-control super composition

Syntax

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

undo password-control super composition

Views

System view

Default command level

2: System level

Change description

Before modification:

- The value range for the *type-number* argument is 1 to 4.

- By default, the minimum number of composition types is 1 and the minimum number of characters of a composition type is 1 for super passwords.

After modification:

- In FIPS mode, the value of the *type-number* argument must be 4.
- By default, the minimum number of composition types is 4 and the minimum number of characters of a composition type is 1 for super passwords in FIPS mode.

Modified command: password-control super length

Syntax

```
password-control super length length
undo password-control super length
```

Views

System view

Default command level

2: System level

Change description

Before modification: The *length* argument specifies the minimum length of a super password, in the range of 4 to 16.

After modification: The value range for the *length* argument is 8 to 16.

Modified command: public-key local create

Syntax

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

Views

System view

Default command level

2: System level

Change description

Before modification: The DSA or RSA key modulus length is in the range of 512 to 2048 bits, and the default is 1024 bits.

After modification: In FIPS mode, the DSA key modulus length is in the range of 1024 to 2048 bits, and defaults to 1024 bits; the RSA key modulus length is 2048 bits. If the type of key pair already exists, the system asks you whether you want to overwrite it.

Modified command: scp

Old syntax

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

New syntax

In non-FIPS mode:

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

In FIPS mode:

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

Views

User view

Default command level

3: Manage level

Change description

After modification:

- In FIPS mode, the following parameters are added:
 - **prefer-ctos-cipher aes256**: Specifies **aes256-cbc** as the preferred encryption algorithm from client to server.
 - **prefer-stoc-cipher aes256**: Specifies **aes256-cbc** as the preferred encryption algorithm from server to client.
- In FIPS mode, the following parameters are deleted:
 - **identity-key dsa**: Specifies **dsa** as the algorithm for public key authentication.
 - **prefer-ctos-cipher 3des**: Specifies **3des-cbc** as the preferred encryption algorithm from client to server.
 - **prefer-ctos-cipher des**: Specifies **des-cbc** as the preferred encryption algorithm from client to server.
 - **prefer-ctos-hmac md5**: Specifies **hmac-md5** as the preferred HMAC algorithm from client to server.
 - **prefer-ctos-hmac md5-96**: Specifies **hmac-md5-96** as the preferred HMAC algorithm from client to server.
 - **prefer-kex dh-group-exchange**: Specifies **diffie-hellman-group-exchange-sha1** as the preferred key exchange algorithm.
 - **prefer-kex dh-group1**: Specifies **diffie-hellman-group1-sha1** as the preferred key exchange algorithm.
 - **prefer-stoc-cipher 3des**: Specifies **3des-cbc** as the preferred encryption algorithm from server to client.
 - **prefer-stoc-cipher des**: Specifies **des-cbc** as the preferred encryption algorithm from server to client.
 - **prefer-stoc-hmac md5**: Specifies **hmac-md5** as the preferred HMAC algorithm from server to client.
 - **prefer-stoc-hmac md5-96**: Specifies **hmac-md5-96** as the preferred HMAC algorithm from server to client.

Modified command: ssh user

Old syntax

```
ssh user username service-type stelnet authentication-type { password | { any |
password-publickey | publickey } assign publickey keyname }
```

```
ssh user username service-type { all | scp | sftp } authentication-type { password | { any | password-publickey | publickey } assign publickey keyname work-directory directory-name }  
undo ssh user username
```

New syntax

In non-FIPS mode:

```
ssh user username service-type stelnet authentication-type { password | { any | password-publickey | publickey } assign publickey keyname }  
ssh user username service-type { all | scp | sftp } authentication-type { password | { any | password-publickey | publickey } assign publickey keyname work-directory directory-name }  
undo ssh user username
```

In FIPS mode:

```
ssh user username service-type stelnet authentication-type { password | password-publickey assign publickey keyname }  
ssh user username service-type { all | scp | sftp } authentication-type { password | password-publickey assign publickey keyname work-directory directory-name }  
undo ssh user username
```

Views

System view

Default command level

3: Manage level

Change description

After modification: In FIPS mode, the any authentication method and public key authentication method are deleted.

Modified command: ssh2

Old syntax

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

New syntax

In non-FIPS mode:

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

In FIPS mode:

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

Views

User view

Default command level

0: Visit level

Change description

After modification:

- In FIPS mode, the following parameters are added:
 - **prefer-ctos-cipher aes256**: Specifies **aes256-cbc** as the preferred encryption algorithm from client to server.
 - **prefer-stoc-cipher aes256**: Specifies **aes256-cbc** as the preferred encryption algorithm from server to client.
- In FIPS mode, the following parameters are deleted:
 - **identity-key dsa**: Specifies **dsa** as the algorithm for public key authentication.
 - **prefer-ctos-cipher 3des**: Specifies **3des-cbc** as the preferred encryption algorithm from client to server.
 - **prefer-ctos-cipher des**: Specifies **des-cbc** as the preferred encryption algorithm from client to server.
 - **prefer-ctos-hmac md5**: Specifies **hmac-md5** as the preferred HMAC algorithm from client to server.
 - **prefer-ctos-hmac md5-96**: Specifies **hmac-md5-96** as the preferred HMAC algorithm from client to server.
 - **prefer-kex dh-group-exchange**: Specifies **diffie-hellman-group-exchange-sha1** as the preferred key exchange algorithm.
 - **prefer-kex dh-group1**: Specifies **diffie-hellman-group1-sha1** as the preferred key exchange algorithm.
 - **prefer-stoc-cipher 3des**: Specifies **3des-cbc** as the preferred encryption algorithm from server to client.
 - **prefer-stoc-cipher des**: Specifies **des-cbc** as the preferred encryption algorithm from server to client.
 - **prefer-stoc-hmac md5**: Specifies **hmac-md5** as the preferred HMAC algorithm from server to client.
 - **prefer-stoc-hmac md5-96**: Specifies **hmac-md5-96** as the preferred HMAC algorithm from server to client.

Modified command: `sftp`

Old syntax

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

New syntax

In non-FIPS mode:

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

In FIPS mode:

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


Views

User view

Default command level

3: Manage level

Change description

After modification:

- In FIPS mode, the following parameters are added:
 - **prefer-ctos-cipher aes256**: Specifies **aes256-cbc** as the preferred encryption algorithm from client to server.
 - **prefer-stoc-cipher aes256**: Specifies **aes256-cbc** as the preferred encryption algorithm from server to client.
- In FIPS mode, the following parameters are deleted:
 - **identity-key dsa**: Specifies **dsa** as the algorithm for public key authentication.
 - **prefer-ctos-cipher 3des**: Specifies **3des-cbc** as the preferred encryption algorithm from client to server.
 - **prefer-ctos-cipher des**: Specifies **des-cbc** as the preferred encryption algorithm from client to server.
 - **prefer-ctos-hmac md5**: Specifies **hmac-md5** as the preferred HMAC algorithm from client to server.
 - **prefer-ctos-hmac md5-96**: Specifies **hmac-md5-96** as the preferred HMAC algorithm from client to server.
 - **prefer-kex dh-group-exchange**: Specifies **diffie-hellman-group-exchange-sha1** as the preferred key exchange algorithm.
 - **prefer-kex dh-group1**: Specifies **diffie-hellman-group1-sha1** as the preferred key exchange algorithm.
 - **prefer-stoc-cipher 3des**: Specifies **3des-cbc** as the preferred encryption algorithm from server to client.
 - **prefer-stoc-cipher des**: Specifies **des-cbc** as the preferred encryption algorithm from server to client.
 - **prefer-stoc-hmac md5**: Specifies **hmac-md5** as the preferred HMAC algorithm from server to client.
 - **prefer-stoc-hmac md5-96**: Specifies **hmac-md5-96** as the preferred HMAC algorithm from server to client.

Modified command: ciphersuite

Old syntax

```
ciphersuite [ rsa_3des_edc_cbc_sha | rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha |  
rsa_des_cbc_sha | rsa_rc4_128_md5 | rsa_rc4_128_sha ] *
```

New syntax

In non-FIPS mode:

```
ciphersuite [ rsa_3des_edc_cbc_sha | rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha |  
rsa_des_cbc_sha | rsa_rc4_128_md5 | rsa_rc4_128_sha ] *
```

In FIPS mode:

```
ciphersuite [ dhe_rsa_aes_128_cbc_sha | dhe_rsa_aes_256_cbc_sha | rsa_aes_128_cbc_sha  
| rsa_aes_256_cbc_sha ] *
```

Views

SSL server policy view

Default command level

2: System level

Change description

After modification:

- In FIPS mode, the following parameters are added:
 - **dhe_rsa_aes_128_cbc_sha**: Specifies the key exchange algorithm of DH_RSA, the data encryption algorithm of 128-bit AES_CBC, and the MAC algorithm of SHA.
 - **dhe_rsa_aes_256_cbc_sha**: Specifies the key exchange algorithm of DH_RSA, the data encryption algorithm of 256-bit AES_CBC, and the MAC algorithm of SHA.
- In FIPS mode, the following parameters are deleted:
 - **rsa_3des_ede_cbc_sha**: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 3DES_EDE_CBC, and the MAC algorithm of SHA.
 - **rsa_des_cbc_sha**: Specifies the key exchange algorithm of RSA, the data encryption algorithm of DES_CBC, and the MAC algorithm of SHA.
 - **rsa_rc4_128_md5**: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of MD5.
 - **rsa_rc4_128_sha**: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of SHA.

Modified command: prefer-cipher

Old syntax

```
prefer-cipher { rsa_3des_ede_cbc_sha | rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha |  
rsa_des_cbc_sha | rsa_rc4_128_md5 | rsa_rc4_128_sha }
```

undo prefer-cipher

New syntax

In non-FIPS mode:

```
prefer-cipher { rsa_3des_ede_cbc_sha | rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha |  
rsa_des_cbc_sha | rsa_rc4_128_md5 | rsa_rc4_128_sha }
```

undo prefer-cipher

In FIPS mode:

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

undo prefer-cipher

Views

SSL client policy view

Default command level

2: System level

Change description

After modification:

- In FIPS mode, the following parameters are added:

- **dhe_rsa_aes_128_cbc_sha**: Specifies the key exchange algorithm of DH_RSA, the data encryption algorithm of 128-bit AES_CBC, and the MAC algorithm of SHA.
- **dhe_rsa_aes_256_cbc_sha**: Specifies the key exchange algorithm of DH_RSA, the data encryption algorithm of 256-bit AES_CBC, and the MAC algorithm of SHA.
- In FIPS mode, the following parameters are deleted:
 - **rsa_3des_edc_cbc_sha**: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 3DES_EDE_CBC, and the MAC algorithm of SHA.
 - **rsa_des_cbc_sha**: Specifies the key exchange algorithm of RSA, the data encryption algorithm of DES_CBC, and the MAC algorithm of SHA.
 - **rsa_rc4_128_md5**: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of MD5.
 - **rsa_rc4_128_sha**: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of SHA.

Modified command: certificate request mode

Syntax

```
certificate request mode { auto [ key-length key-length | password { cipher | simple } password ]
* | manual }
```

```
undo certificate request mode
```

Views

PKI domain view

Default command level

2: System level

Change description

Before modification: The *key-length* argument specifies the RSA key length in the range of 512 to 2048 bits, and the default is 1024 bits.

After modification: In FIPS mode, the value of the *key-length* argument must be 2048 bits.

Modified feature: Modifying SNMP commands executed in FIPS mode for CC evaluation

Feature change description

Changed related SNMP command keywords and value ranges when the device is operating in FIPS mode.

Command changes

Modified command: display snmp-agent community

Syntax

```
display snmp-agent community [ read | write ] [ | { begin | exclude | include }
regular-expression ]
```

Views

Any view

Change description

This command is not supported in FIPS mode.

Modified command: snmp-agent community

Syntax

```
snmp-agent community { read | write } [ cipher ] community-name [ mib-view view-name ] [ acl  
acl-number | acl ipv6 ipv6-acl-number ] *
```

```
undo snmp-agent community { read | write } community-name
```

Views

System view

Change description

This command is not supported in FIPS mode.

Modified command: snmp-agent group

Syntax

```
snmp-agent group { v1 | v2c } group-name [ read-view view-name ] [ write-view view-name ]  
[ notify-view view-name ] [ acl acl-number | acl ipv6 ipv6-acl-number ] *
```

```
undo snmp-agent group { v1 | v2c } group-name
```

Views

System view

Change description

This command is not supported in FIPS mode.

Modified command: snmp-agent usm-user { v1 | v2c }

Syntax

```
snmp-agent usm-user { v1 | v2c } user-name group-name [ acl acl-number | acl ipv6  
ipv6-acl-number ] *
```

```
undo snmp-agent usm-user { v1 | v2c } user-name group-name
```

Views

System view

Change description

This command is not supported in FIPS mode.

Modified command: snmp-agent calculate-password

Old syntax

```
snmp-agent calculate-password plain-password mode { 3desmd5 | 3dessha | md5 | sha }  
{ local-engineid | specified-engineid engineid }
```

New syntax

In non-FIPS mode:

```
snmp-agent calculate-password plain-password mode { 3desmd5 | 3dessha | md5 | sha }  
{ local-engineid | specified-engineid engineid }
```

In FIPS mode:

```
snmp-agent calculate-password plain-password mode sha { local-engineid |  
specified-engineid engineid }
```

Views

System view

Change description

After modification: In FIPS mode, the keywords **3desmd5**, **3dessha**, and **md5** are deleted.

Modified command: snmp-agent sys-info

Old syntax

```
snmp-agent sys-info { contact sys-contact | location sys-location | version { all | { v1 | v2c |  
v3 }* } }
```

```
undo snmp-agent sys-info { contact | location | version { all | { v1 | v2c | v3 }* } }
```

New syntax

In non-FIPS mode:

```
snmp-agent sys-info { contact sys-contact | location sys-location | version { all | { v1 | v2c |  
v3 }* } }
```

```
undo snmp-agent sys-info { contact | location | version { all | { v1 | v2c | v3 }* } }
```

In FIPS mode:

```
snmp-agent sys-info { contact sys-contact | location sys-location | version v3 }
```

```
undo snmp-agent sys-info { contact | location | version v3 }
```

Views

System view

Change description

After modification: In FIPS mode, the keywords **all**, **v1**, and **v2c** are deleted.

Modified command: snmp-agent target-host

Old syntax

```
snmp-agent target-host trap address udp-domain { ip-address | ipv6 ipv6-address } [ udp-port  
port-number ] [ dscp dscp-value ] [ vpn-instance vpn-instance-name ] params securityname  
security-string [ v1 | v2c | v3 [ authentication | privacy ] ]
```

```
undo snmp-agent target-host trap address udp-domain { ip-address | ipv6 ipv6-address }  
params securityname security-string [ vpn-instance vpn-instance-name ]
```

New syntax

In non-FIPS mode:

```
snmp-agent target-host trap address udp-domain { ip-address | ipv6 ipv6-address } [ udp-port  
port-number ] [ dscp dscp-value ] [ vpn-instance vpn-instance-name ] params securityname  
security-string [ v1 | v2c | v3 [ authentication | privacy ] ]
```

```
undo snmp-agent target-host trap address udp-domain { ip-address | ipv6 ipv6-address }  
params securityname security-string [ vpn-instance vpn-instance-name ]
```

In FIPS mode:

```
snmp-agent target-host trap address udp-domain { ip-address | ipv6 ipv6-address } [ udp-port port-number ] [ dscp dscp-value ] [ vpn-instance vpn-instance-name ] params securityname security-string v3 [ authentication | privacy ]
```

```
undo snmp-agent target-host trap address udp-domain { ip-address | ipv6 ipv6-address } params securityname security-string [ vpn-instance vpn-instance-name ]
```

Views

System view

Change description

After modification: In FIPS mode, the keywords **v1** and **v2c** are deleted.

Modified command: **snmp-agent usm-user v3**

Old syntax

```
snmp-agent usm-user v3 user-name group-name [ cipher ] [ authentication-mode { md5 | sha } auth-password [ privacy-mode { 3des | aes128 | des56 } priv-password ] ] [ acl acl-number | acl ipv6 ipv6-acl-number ] *
```

```
undo snmp-agent usm-user v3 user-name group-name { local | engineid engineid-string }
```

New syntax

In non-FIPS mode:

```
snmp-agent usm-user v3 user-name group-name [ cipher ] [ authentication-mode { md5 | sha } auth-password [ privacy-mode { 3des | aes128 | des56 } priv-password ] ] [ acl acl-number | acl ipv6 ipv6-acl-number ] *
```

```
undo snmp-agent usm-user v3 user-name group-name { local | engineid engineid-string }
```

In FIPS mode:

```
snmp-agent usm-user v3 user-name group-name [ cipher ] [ authentication-mode sha ] auth-password [ privacy-mode aes128 priv-password ] ] [ acl acl-number | acl ipv6 ipv6-acl-number ] *
```

```
undo snmp-agent usm-user v3 user-name group-name { local | engineid engineid-string }
```

Views

System view

Change description

After modification: In FIPS mode, the keywords **md5**, **3des**, and **des56** are deleted.

Modified feature: Clearing all users from the password control blacklist

Feature change description

Changed the command to clear all users from the password control blacklist.

Command changes

Modified command: reset password-control blacklist

Old syntax

```
reset password-control blacklist [ user-name name ]
```

New syntax

```
reset password-control blacklist { all | user-name name }
```

Views

User view

Change description

Before modification: The **reset password-control blacklist** command without the **user-name** *name* option specified clears all users from the password control blacklist.

After modification: The **reset password-control blacklist all** command clears all users from the password control blacklist.

Modified feature: Setting the interval for saving system information to the log file

Feature change description

Changed the interval for saving system information to the log file.

Command changes

Modified command: info-center logfile frequency

Syntax

```
info-center logfile frequency freq-sec
```

```
undo info-center logfile frequency
```

Views

System view

Change description

Before modification: The *freq-sec* argument ranges from 1 to 86400.

After modification: The *freq-sec* argument ranges from 3600 to 86400.

F5102

This release has the following changes:

- [Modified feature: Password configuration and display](#)
- [Modified feature: Task ID for IPv6 socket display](#)
- [Removed feature: Local user password display](#)

Modified feature: Password configuration and display

Feature change description

Modified password setup and display for password-related security features.

NOTE:

To improve security, this release saves all plaintext and ciphertext passwords (keys) in cipher text in the configuration file.

Command changes

Modified command: area-authentication-mode

Old syntax

```
area-authentication-mode { md5 | simple } password [ ip | osi ]
```

New syntax

```
area-authentication-mode { md5 | simple } [ cipher ] password [ ip | osi ]
```

Views

IS-IS view

Parameters

md5: MD5 authentication mode.

simple: Simple authentication mode.

cipher: Sets a password in cipher text. If this keyword is not specified, set a password in plain text.

password: Password, a case-sensitive string of 1 to 16 characters in plain text, or 33 to 53 characters in cipher text.

ip: Checks IP related fields in LSPs.

osi: Checks OSI related fields in LSPs.

NOTE:

Whether a password should use **ip** or **osi** is not affected by the actual network environment.

Change description

Before modification:

- For MD5 authentication, a ciphertext password must comprise 24 characters.

- For simple authentication, you must set a plaintext password.

After modification:

- For MD5 authentication, a ciphertext password comprises 33 to 53 characters.
- For simple authentication, you can use the **cipher** keyword to set a ciphertext password of 33 to 53 characters.

Modified command: bims-server

Old syntax

bims-server ip *ip-address* [**port** *port-number*] **sharekey** *key*

New syntax

bims-server ip *ip-address* [**port** *port-number*] **sharekey** [**cipher** | **simple**] *key*

Views

DHCP address pool view

Parameters

ip *ip-address*: Specifies an IP address for the BIMS server.

port *port-number*: Specifies a port number for the BIMS server in the range of 1 to 65534.

cipher: Sets a ciphertext key.

simple: Sets a plaintext key.

key: Specifies the key string. This argument is case sensitive. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If **simple** is specified, it must be a string of 1 to 16 characters. If neither **simple** nor **cipher** is specified, you set a plaintext key.

Change description

Before modification: You can only set a plaintext shared key.

After modification: You can set a plaintext or a ciphertext shared key. A ciphertext shared key can comprise 1 to 53 characters.

Modified command: certificate request mode

Syntax

certificate request mode { **auto** [**key-length** *key-length* | **password** { **cipher** | **simple** } *password*] * | **manual** }

Views

PKI domain view

Parameters

auto: Requests a certificate in auto mode.

key-length: Length of the RSA keys in bits, in the range of 512 to 2048. It is 1024 bits by default.

cipher: Sets a ciphertext key for certificate revocation.

simple: Sets a plaintext key for certificate revocation.

password: Specifies the key. This argument is case sensitive. If **simple** is specified, it must be a plaintext string of 1 to 31 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 73 characters.

manual: Requests a certificate in manual mode.

Change description

Before modification: A ciphertext key comprises 1 to 31 characters.

After modification: A ciphertext key comprises 1 to 73 characters.

Modified command: cluster-local-user

Syntax

cluster-local-user *user-name* [**password** { **cipher** | **simple** } *password*]

Views

Cluster view

Parameters

user-name: Specifies the username for logging onto the cluster member devices through Web. It is a string of 1 to 55 characters.

password: Specifies the password for logging onto the cluster member devices through Web. If this keyword is not specified, you can log in without a password.

cipher: Specifies a ciphertext password.

simple: Specifies a plaintext password.

password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 63 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 117 characters.

Change description

Before modification:

- **cipher**: Sets a plaintext or ciphertext password. The password will be saved in cipher text in the configuration file.
- **cipher password**: Specifies the password string, which can be a plaintext string of 1 to 63 characters, or a 24-character or 88-character ciphertext string.

After modification:

- **cipher**: Sets a ciphertext password.
- **cipher password**: Specifies a ciphertext password of 1 to 117 characters.

Modified command: cluster-snmp-agent usm-user v3

Old syntax

cluster-snmp-agent usm-user v3 *user-name group-name* [**authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode des56** *priv-password*]]

New syntax

cluster-snmp-agent usm-user v3 *user-name group-name* [**authentication-mode** { **md5** | **sha** } [**cipher** | **simple**] *auth-password* [**privacy-mode des56** [**cipher** | **simple**] *priv-password*]]

Views

Cluster view

Parameters

user-name: User name, a string of 1 to 32 characters.

group-name: Group name, a string of 1 to 32 characters.

authentication-mode: Specifies the security level to be authentication needed.

md5: Specifies the authentication protocol to be HMAC-MD5-96.

sha: Specifies the authentication protocol to be HMAC-SHA-96.

cipher: Specifies a ciphertext password.

simple: Specifies a plaintext password.

auth-password: Specifies the authentication password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **cipher** nor **simple** is specified, you set a plaintext string.

privacy-mode: Specifies the security level to be encrypted.

des56: Specifies the encryption protocol to be DES (data encryption standard).

priv-password: Specifies the privacy password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **cipher** nor **simple** is specified, you set a plaintext string.

Change description

Before modification:

- **cipher** and **simple** keywords are not supported. You can directly enter a plaintext or a ciphertext password.
- The authentication password (*auth-password*) and the privacy password (*priv-password*) can be a plaintext string of 1 to 16 characters, or a 24-character ciphertext string.

After modification:

- You can use the **cipher** keyword to set a ciphertext password or use the **simple** keyword to set a plaintext password. If neither **cipher** nor **simple** is specified, you set a plaintext password.
- A plaintext password comprises 1 to 16 characters. A ciphertext password comprises 1 to 53 characters.

Modified command: cwmp acs password

Old syntax

cwmp acs password *passowrd*

New syntax

cwmp acs password [**cipher** | **simple**] *passowrd*

Views

CWMP view

Parameters

cipher: Specifies a ciphertext password.

simple: Specifies a plaintext password.

password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 255 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 373 characters. If neither **cipher** nor **simple** is specified, you set a plaintext password string.

Change description

Before modification: You can only set a plaintext password.

After modification: You can set a plaintext password or a ciphertext password. A ciphertext password comprises 1 to 373 characters.

Modified command: cwmp cpe password

Old syntax

cwmp cpe password *passowrd*

New syntax

cwmp cpe password [**cipher** | **simple**] *passowrd*

Views

CWMP view

Parameters

cipher: Specifies a ciphertext password.

simple: Specifies a plaintext password.

password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 255 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 373 characters. If neither **cipher** nor **simple** is specified, you set a plaintext password string.

Change description

Before modification: You can only set a plaintext password.

After modification: You can set a plaintext password or a ciphertext password. A ciphertext password comprises 1 to 373 characters.

Modified command: dldp authentication-mode

Old syntax

dldp authentication-mode { **md5** *md5-password* | **none** | **simple** *simple-password* }

New syntax

dldp authentication-mode { **none** | { **md5** | **simple** } *password* }

Views

System view

Parameters

none: Specifies not to perform authentication.

md5: Specifies to perform MD5 authentication and sets the password in plain text or cipher text.

simple: Specifies to perform simple authentication and sets the password in plain text or cipher text.

password: Plain text password, a case-sensitive string of 1 to 16 characters; or a cipher text password, a case-sensitive string of 33 to 53 characters.

Change description

Before modification: You can set only a plaintext password for simple authentication, and a plaintext password or a 24-character ciphertext password for MD5 authentication.

After modification: You can set a plaintext password or a ciphertext password for both simple authentication and MD5 authentication. A ciphertext password comprises 33 to 53 characters.

Modified command: domain-authentication-mode

Old syntax

domain-authentication-mode { **md5** | **simple** } *password* [**ip** | **osi**]

New syntax

domain-authentication-mode { **md5** | **simple** } [**cipher**] *password* [**ip** | **osi**]

Views

IS-IS view

Parameters

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

cipher: Sets a password in cipher text. If this keyword is not specified, set a password in plain text.

password: Password, a case-sensitive string of 1 to 16 characters in plain text, or 33 to 53 characters in cipher text.

ip: Checks IP related fields in LSPs.

osi: Checks OSI related fields in LSPs.

NOTE:

Whether a password should use **ip** or **osi** is not affected by the actual network environment.

Change description

Before modification:

- For MD5 authentication, a ciphertext password must comprise 24 characters.
- For simple authentication, you must set a plaintext password.

After modification:

- For MD5 authentication, a ciphertext password comprises 33 to 53 characters.
- For simple authentication, you can use the **cipher** keyword to set a ciphertext password of 33 to 53 characters.

Modified command: ftp-server

Syntax

ftp-server *ip-address* [**user-name** *username* **password** { **cipher** | **simple** } *password*]

Views

Cluster view

Parameters

ip-address: Specifies the IP address of the FTP server.

username: Specifies the username for logging onto the FTP server, a string of 1 to 32 characters.

cipher: Specifies a ciphertext password.

simple: Specifies a plaintext password.

password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters.

Change description

Before modification:

- **cipher**: Sets a plaintext or ciphertext password. The password will be saved in cipher text in the configuration file.

- **cipher password:** Specifies the password string, which can be a plaintext string of 1 to 16 characters, or a 24-character ciphertext string.

After modification:

- **cipher:** Sets a ciphertext password.
- **cipher password:** Specifies a ciphertext password of 1 to 53 characters.

Modified command: isis authentication-mode

Old syntax

isis authentication-mode { **md5** | **simple** } *password* [**level-1** | **level-2**] [**ip** | **osi**]

New syntax

isis authentication-mode { **md5** | **simple** } [**cipher**] *password* [**level-1** | **level-2**] [**ip** | **osi**]

Views

Interface view

Parameters

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

cipher: Sets a password in cipher text. If this keyword is not specified, set a password in plain text.

password: Password, a case-sensitive string of 1 to 16 characters in plain text, or 33 to 53 characters in cipher text.

level-1: Configures the password for Level-1.

level-2: Configures the password for Level-2.

ip: Checks IP related fields in LSPs and SNPs.

osi: Checks OSI related fields in LSPs and SNPs.

NOTE:

Whether a password should use **ip** or **osi** is not affected by the actual network environment.

Change description

Before modification:

- For MD5 authentication, a ciphertext password must comprise 24 characters.
- For simple authentication, you must set a plaintext password.

After modification:

- For MD5 authentication, a ciphertext password comprises 33 to 53 characters.
- For simple authentication, you can use the **cipher** keyword to set a ciphertext password of 33 to 53 characters.

Modified command: key (HWTACACS scheme view)

Syntax

key { **accounting** | **authentication** | **authorization** } [**cipher** | **simple**] *key*

Views

HWTACACS scheme view

Parameters

accounting: Sets the shared key for secure HWTACACS accounting communication.

authentication: Sets the shared key for secure HWTACACS authentication communication.

authorization: Sets the shared key for secure HWTACACS authorization communication.

cipher: Sets a ciphertext shared key.

simple: Sets a plaintext shared key.

key: Specifies the shared key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 255 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 373 characters. If neither **cipher** nor **simple** is specified, you set a plaintext shared key string.

Change description

Before modification: A ciphertext password comprises 1 to 352 characters.

After modification: A ciphertext password comprises 1 to 373 characters.

Modified command: key (RADIUS scheme view)

Syntax

```
key { accounting | authentication } [ cipher | simple ] key
```

Views

RADIUS scheme view

Parameters

accounting: Sets the shared key for secure RADIUS accounting communication.

authentication: Sets the shared key for secure RADIUS authentication/authorization communication.

cipher: Sets a ciphertext shared key.

simple: Sets a plaintext shared key.

key: Specifies the shared key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 64 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 117 characters. If neither **cipher** nor **simple** is specified, you set a plaintext shared key string.

Change description

Before modification: A ciphertext shared key must comprise 12, 24, 32, 44, 64, 76, 88, or 96 characters.

After modification: A ciphertext shared key comprises 1 to 117 characters.

Modified command: mac-authentication user-name-format

Syntax

```
mac-authentication user-name-format { fixed [ account name ] [ password { cipher | simple } password ] | mac-address [ { with-hyphen | without-hyphen } [ lowercase | uppercase ] ] }
```

Views

System view

Parameters

fixed: Uses a shared account for all MAC authentication users.

account name: Specifies the username for the shared account. The name takes a case-insensitive string of 1 to 55 characters. If no username is specified, the default name **mac** applies.

password: Specifies the password for the shared user account:

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Specifies the password. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 63 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 117 characters.

mac-address: Uses MAC-based user accounts for MAC authentication users. If this option is specified, you must create one user account for each user, and use the MAC address of the user as both the username and password for the account. You can also specify the format of username and password:

- **with-hyphen**—Hyphenates the MAC address, for example xx-xx-xx-xx-xx-xx.
- **without-hyphen**—Excludes hyphens from the MAC address, for example, xxxxxxxxxxxx.
- **lowercase**—Enters letters in lower case.
- **uppercase**—Capitalizes letters.

Change description

Before modification: If **cipher** is specified, you can enter a plaintext password of 1 to 63 characters, or a ciphertext password of 24 or 88 characters.

After modification: If **cipher** is specified, you must enter a ciphertext password of 1 to 117 characters.

Modified command: md5-password

Syntax

md5-password { **cipher** | **plain** } *peer-lsr-id password*

Views

MPLS LDP view, MPLS LDP VPN instance view

Parameters

cipher: Sets a ciphertext key.

plain: Sets a plaintext key.

peer-lsr-id: Specifies the MPLS LSR ID of a peer.

password: Specifies the key string. This argument is case sensitive. If **plain** is specified, it must be a plaintext string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters.

Change description

Before modification: If **cipher** is specified, you can enter a plaintext key string of 1 to 16 characters or a 24-character ciphertext key string.

After modification: If **cipher** is specified, you must enter a ciphertext key string of 1 to 53 characters.

Modified command: mpls rsvp-te authentication

Syntax

mpls rsvp-te authentication { **cipher** | **plain** } *auth-key*

Views

Interface view

Parameters

cipher: Sets a ciphertext key.

plain: Sets a plaintext key.

auth-key: Specifies the key. This argument is case sensitive. If the **cipher** keyword is specified, it must be a ciphertext string of 8 to 53 characters. If the **plain** keyword is specified, it must be a plaintext string of 8 to 16 characters.

Change description

Before modification: If **cipher** is specified, you can enter a plaintext key string of 8 to 16 characters or a 24-character ciphertext key string.

After modification: If **cipher** is specified, you must enter a ciphertext key string of 8 to 53 characters.

Modified command: `ntp-service authentication-keyid`

Old syntax

`ntp-service authentication-keyid keyid authentication-mode md5 value`

New syntax

`ntp-service authentication-keyid keyid authentication-mode md5 [cipher | simple] value`

Views

System view

Parameters

keyid: Authentication key ID, which is in the range of 1 to 4294967295.

cipher: Sets a ciphertext key.

simple: Sets a plaintext key. This key will be saved in cipher text for secrecy.

value: Specifies the MD5 authentication key string. This argument is case sensitive. If **simple** is specified, it must be a plaintext string of 1 to 32 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 73 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string.

Change description

Before modification: You can only set a plaintext key.

After modification: You can set a plaintext or ciphertext key. A ciphertext key comprises 1 to 73 characters.

Modified command: `ospf authentication-mode`

syntax

For MD5/HMAC-MD5 authentication:

`ospf authentication-mode { hmac-md5 | md5 } key-id [cipher | plain] password`

For simple authentication:

`ospf authentication-mode simple [cipher | plain] password`

Views

Interface view

Parameters

hmac-md5: HMAC-MD5 authentication.

md5: MD5 authentication.

simple: Simple authentication.

key-id: Authentication key ID, in the range of 1 to 255.

cipher: Specifies a ciphertext password.

plain: Specifies a plaintext password.

If no **cipher** or **plain** is specified, the default password type for MD5/HMAC-MD5 authentication mode is **cipher**, and the default password type for simple authentication mode is **plain**.

password: Password.

- In simple authentication mode, a plaintext password is a case-sensitive string of 1 to 8 characters, and a ciphertext password is a case-sensitive string of 1 to 41 characters.
- In MD5/HMAC-MD5 authentication mode, a plaintext password is a case-sensitive string of 1 to 16 characters, and a ciphertext password is a case-sensitive string of 1 to 53 characters.

Change description

Before modification: If **cipher** is specified, you can enter a plaintext password or a 24-character ciphertext password.

After modification: For simple authentication, a ciphertext password comprises 1 to 41 characters. For MD5 authentication, a ciphertext password comprises 1 to 53 characters.

Modified command: password (FTP operation type view)

Old syntax

password *password*

New syntax

password [**cipher** | **simple**] *password*

Views

FTP operation type view

Parameters

cipher: Sets a password in cipher text.

simple: Sets a password in plain text.

password: Specifies the password used to log in to the FTP server, a case-sensitive string of 1 to 32 characters in plain text, or 1 to 73 characters in cipher text. If the **cipher** or **simple** keyword is not specified, the password is in plain text.

Change description

Before modification: You can only set a plaintext password.

After modification: You can set a plaintext password or a ciphertext password. A ciphertext password comprises 1 to 73 characters.

Modified command: password (local user view)

Syntax

password [{ **cipher** | **simple** } *password*]

Views

Local user view

Parameters

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 63 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 117 characters. If neither **cipher** nor **simple** is specified, you set a plaintext password string in interactive mode.

Change description

Before modification: If **cipher** is specified, you can set a plaintext password, or a 24-character or 88-character ciphertext password.

After modification: If **cipher** is specified, you must enter a ciphertext password of 1 to 117 characters.

Modified command: password (RADIUS-server user view)

Syntax

password [**cipher** | **simple**] *password*

Views

RADIUS-server user view

Parameters

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 128 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 201 characters. If neither **cipher** nor **simple** is specified, you set a plaintext password string.

Change description

Before modification: A ciphertext password must comprise 12, 24, 32, 44, 64, 76, 88, 96, 108, 120, 128, 140, 152, 160, 172, or 184 characters.

After modification: A ciphertext password comprises 1 to 201 characters.

Modified command: peer password (IPv6 address family view)

Syntax

peer { *group-name* | *ipv6-address* } **password** { **cipher** | **simple** } *password*

Views

IPv6 address family view

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Specifies the password string.

- If **simple** is specified, a plaintext password is a case-sensitive string of 1 to 80 characters.
- If **cipher** is specified, a plaintext password is a case-sensitive string of 1 to 80 characters, and a ciphertext password is a case-sensitive string of 1 to 137 characters.

Change description

Before modification: A ciphertext password must comprise 24 or 88 characters.

After modification: A ciphertext password comprises 1 to 137 characters.

Modified command: peer password (MSDP view)

Syntax

peer *peer-address* **password** { **cipher** | **simple** } *password*

Views

Public network MSDP view, VPN instance MSDP view

Parameters

peer-address: Specifies an MSDP peer.

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Specifies the password string. This argument is case sensitive.

- If **simple** is specified, the plaintext password comprises 1 to 80 characters.
- If **cipher** is specified, the ciphertext password comprises 1 to 137 characters.

Change description

Before modification: A ciphertext password must comprise 24 or 108 characters.

After modification: A ciphertext password comprises 1 to 137 characters.

Modified command: portal server

Old syntax

portal server *server-name* **ip** *ip-address* [**key** *key-string* | **port** *port-id* | **url** *url-string* | **vpn-instance** *vpn-instance-name*] *

New syntax

portal server *server-name* **ip** *ip-address* [**key** [**cipher** | **simple**] *key-string* | **port** *port-id* | **url** *url-string* | **vpn-instance** *vpn-instance-name*] *

Views

System view

Parameters

server-name: Specifies the name of a portal server, a case-sensitive string of 1 to 32 characters.

ip *ip-address*: Specifies the IPv4 address of a portal server.

key: Specifies a shared key for communication with the portal server. Portal packets exchanged between the access device and the portal server carry an authenticator, which is generated with the shared key. The receiver uses the authenticator to check the correctness of the received portal packets.

cipher: Sets a ciphertext shared key.

simple: Sets a plaintext shared key.

key-string: Specifies the shared key. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **simple** nor **cipher** is specified, you set a plaintext shared key.

port *port-id*: Specifies the destination port number used when the device sends an unsolicited message to the portal server, in the range of 1 to 65534. The default is 50100.

url *url-string*: Specifies the uniform resource locator (URL) to which HTTP packets are to be redirected. The default URL is in the `http://ip-address` format, where *ip-address* is the IP address of the portal server. You can also specify the domain name of the portal server, in which case you must use the **portal free-rule** command to configure the IP address of the DNS server as a portal authentication-free destination IP address.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN to which the portal server belongs. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If the portal server is on the public network, do not specify this option.

Change description

Before modification: You can only set a plaintext shared key.

After modification: You can set a plaintext or a ciphertext shared key. A ciphertext shared key comprise 1 to 53 characters.

Modified command: primary accounting (RADIUS scheme view)

Syntax

```
primary accounting { ipv4-address | ipv6 ipv6-address } [ port-number | key [ cipher | simple ] key | vpn-instance vpn-instance-name ] *
```

Views

RADIUS scheme view

Parameters

ipv4-address: Specifies the IPv4 address of the primary RADIUS accounting server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the primary RADIUS accounting server, which must be a valid global unicast address.

port-number: Specifies the service port number of the primary RADIUS accounting server, which is a UDP port number in the range 1 to 65535 and defaults to 1813.

key [**cipher** | **simple**] *key*: Specifies the shared key for secure communication with the primary RADIUS accounting server.

- **cipher** *key*: Specifies a ciphertext shared key, a case-sensitive ciphertext string of 1 to 117 characters.
- **simple** *key*: Specifies a plaintext shared key, a case-sensitive plaintext string of 1 to 64 characters.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN that the primary RADIUS accounting server belongs to, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

Change description

Before modification: A ciphertext shared key must comprise 12, 24, 32, 44, 64, 76, 88, or 96 characters.

After modification: A ciphertext shared key comprises 1 to 117 characters.

Modified command: primary authentication (RADIUS scheme view)

Syntax

```
primary authentication { ipv4-address | ipv6 ipv6-address } [ port-number | key [ cipher | simple ] key | vpn-instance vpn-instance-name ] *
```

Views

RADIUS scheme view

Parameters

ipv4-address: Specifies the IPv4 address of the primary RADIUS authentication/authorization server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the primary RADIUS authentication/authorization server, which must be a valid global unicast address.

port-number: Specifies the service port number of the primary RADIUS authentication/authorization server, which is a UDP port number in the range 1 to 65535 and defaults to 1812.

key [**cipher** | **simple**] *key*: Specifies the shared key for secure communication with the primary RADIUS authentication/authorization server.

- **cipher** *key*: Specifies a ciphertext shared key, a case-sensitive ciphertext string of 1 to 117 characters.
- **simple** *key*: Specifies a plaintext shared key, a case-sensitive plaintext string of 1 to 64 characters.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN that the primary RADIUS authentication/authorization server belongs to, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

Change description

Before modification: A ciphertext shared key must comprise 12, 24, 32, 44, 64, 76, 88, or 96 characters.

After modification: A ciphertext shared key comprises 1 to 117 characters.

Modified command: radius-server client-ip

Old syntax

radius-server client-ip *ip-address* [**key** *string*]

New syntax

radius-server client-ip *ip-address* [**key** [**cipher** | **simple**] *string*]

Views

System view

Parameters

ip-address: Specifies the IPv4 address of the RADIUS client.

key: Sets the shared key for secure communication with the RADIUS client.

cipher: Sets a ciphertext shared key.

simple: Sets a plaintext shared key.

string: Specifies the shared key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 64 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 117 characters. If neither **cipher** nor **simple** is specified, you set a plaintext shared key string.

all: Specifies all RADIUS clients.

Change description

Before modification: You can only set a plaintext shared key.

After modification: You can set a plaintext or a ciphertext shared key. A ciphertext shared key comprises 1 to 117 characters.

Modified command: rip authentication-mode

Old syntax

```
rip authentication-mode { md5 { rfc2082 key-string key-id | rfc2453 key-string } | simple password }
```

New syntax

```
rip authentication-mode { md5 { rfc2082 [ cipher ] key-string key-id | rfc2453 [ cipher ] key-string } | simple [ cipher ] password }
```

Views

Interface view

Parameters

md5: Specifies the MD5 authentication mode.

rfc2082: Uses the message format defined in RFC 2082.

cipher: Sets an authentication key or password in cipher text. If this keyword is not specified, set an authentication key or password in plain text.

key-string: MD5 key, a case-sensitive string of 1 to 16 characters in plain text, or 33 to 53 characters in cipher text.

key-id: MD5 key number, in the range of 1 to 255.

rfc2453: Uses the message format defined in RFC 2453 (IETF standard).

simple: Specifies the simple authentication mode.

password: Password in simple authentication mode, a case-sensitive string of 1 to 16 characters in plain text, or 33 to 53 characters in cipher text.

Change description

Before modification:

- For MD5 authentication, a ciphertext password comprises 1 to 24 characters.
- For simple authentication, you must set a plaintext password.

After modification:

- For MD5 authentication, a ciphertext password comprises 33 to 53 characters.
- For simple authentication, you can use the **cipher** keyword to set a ciphertext password of 33 to 53 characters.

Modified command: sa authentication-hex

Old syntax

```
sa authentication-hex { inbound | outbound } { ah | esp } hex-key
```

New syntax

```
sa authentication-hex { inbound | outbound } { ah | esp } [ cipher | simple ] hex-key
```

Views

IPsec policy view

Parameters

inbound: Specifies the inbound SA through which IPsec processes the received packets.

outbound: Specifies the outbound SA through which IPsec processes the packets to be sent.

ah: Uses AH.

esp: Uses ESP.

cipher: Sets a ciphertext authentication key.

simple: Sets a plaintext authentication key.

hex-key: Specifies the key string. If **cipher** is specified, this argument is case sensitive and must be a ciphertext string of 1 to 117 characters. If **simple** is specified, this argument is case insensitive, and must be a 16-byte hexadecimal string for MD5, a 20-byte hexadecimal string for SHA1, 32-byte hexadecimal string for SHA2, or a 16-byte hexadecimal string for AES-XBC-MAC. If neither **cipher** nor **simple** is specified, you set a plaintext authentication key string.

Change description

Before modification: You can set only a plaintext authentication key.

After modification: You can set a plaintext or a ciphertext authentication key. A ciphertext authentication key comprises 117 characters at most.

Modified command: sa encryption-hex

Old syntax

```
sa encryption-hex { inbound | outbound } esp hex-key
```

New syntax

```
sa encryption-hex { inbound | outbound } esp [ cipher | simple ] hex-key
```

Views

IPsec policy view

Parameters

inbound: Specifies the inbound SA through which IPsec processes the received packets.

outbound: Specifies the outbound SA through which IPsec processes the packets to be sent.

esp: Uses ESP.

cipher: Sets a ciphertext encryption key.

simple: Sets a plaintext encryption key.

hex-key: Specifies the key string. If **cipher** is specified, this argument is case sensitive and must be a ciphertext string of 1 to 117 characters. If **simple** is specified, this argument is case insensitive, and must be an 8-byte hexadecimal string for DES-CBC, a 16-byte hexadecimal string for AES128-CBC and camellia128-CBC, a 20-byte hexadecimal string for AESCTR-128, a 24-byte hexadecimal string for 3DES-CBC, AES192-CBC, and camellia192-CBC, or a 32-byte hexadecimal string for camellia256-CBC. If neither **cipher** nor **simple** is specified, you set a plaintext authentication key string.

Change description

Before modification: You can set only a plaintext encryption key.

After modification: You can set a plaintext or a ciphertext encryption key. A ciphertext encryption key comprises 117 characters at most.

Modified command: sa string-key

Old syntax

```
sa string-key { inbound | outbound } { ah | esp } string-key
```


New syntax

sa string-key { **inbound** | **outbound** } { **ah** | **esp** } [**cipher** | **simple**] *string-key*

Views

IPsec policy view

Parameters

inbound: Specifies the inbound SA through which IPsec processes the received packets.

outbound: Specifies the outbound SA through which IPsec processes the packets to be sent.

ah: Uses AH.

esp: Uses ESP.

cipher: Sets a ciphertext key.

simple: Sets a plaintext key.

string-key: Specifies the key string. This argument is case sensitive. If **cipher** is specified, it must be a ciphertext string of 1 to 373 characters. If **simple** is specified, it must be a string of 1 to 255 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string. For different algorithms, enter strings of any length in the specified range. Using this key string, the system automatically generates keys meeting the algorithm requirements. When the protocol is ESP, the system generates the keys for the authentication algorithm and encryption algorithm respectively.

Change description

Before modification: You can set only a plaintext key.

After modification: You can set a plaintext or a ciphertext key. A ciphertext key comprises 373 characters at most.

Modified command: secondary accounting (RADIUS scheme view)

Syntax

secondary accounting { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** [**cipher** | **simple**] *key* | **vpn-instance** *vpn-instance-name*] *

Views

RADIUS scheme view

Parameters

ipv4-address: Specifies the IPv4 address of the secondary RADIUS accounting server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the secondary RADIUS accounting server, which must be a valid global unicast address.

port-number: Specifies the service port number of the secondary RADIUS accounting server, which is a UDP port number in the range 1 to 65535 and defaults to 1813.

key [**cipher** | **simple**] *key*: Specifies the shared key for secure communication with the secondary RADIUS accounting server.

- **cipher** *key*: Specifies a ciphertext shared key, a case-sensitive ciphertext string of 1 to 117 characters.
- **simple** *key*: Specifies a plaintext shared key, a case-sensitive plaintext string of 1 to 64 characters.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN that the secondary RADIUS accounting server belongs to, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

Change description

Before modification: A ciphertext shared key must comprise 12, 24, 32, 44, 64, 76, 88, or 96 characters.

After modification: A ciphertext shared key comprises 1 to 117 characters.

Modified command: secondary authentication (RADIUS scheme view)

Syntax

secondary authentication { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** [**cipher** | **simple**] *key* | **vpn-instance** *vpn-instance-name*] *

Views

RADIUS scheme view

Parameters

ipv4-address: Specifies the IPv4 address of the secondary RADIUS authentication/authorization server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the secondary RADIUS authentication/authorization server, which is a valid global unicast address.

port-number: Specifies the service port number of the secondary RADIUS authentication/authorization server, which is a UDP port number in the range 1 to 65535 and defaults to 1812.

key [**cipher** | **simple**] *key*: Specifies the shared key for secure communication with the secondary RADIUS authentication/authorization server.

- **cipher** *key*: Specifies a ciphertext shared key, a case-sensitive ciphertext string of 1 to 117 characters.
- **simple** *key*: Specifies a plaintext shared key, a case-sensitive plaintext string of 1 to 64 characters.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN that the secondary RADIUS authentication/authorization server belongs to, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

Change description

Before modification: A ciphertext shared key must comprise 12, 24, 32, 44, 64, 76, 88, or 96 characters.

After modification: A ciphertext shared key comprises 1 to 117 characters.

Modified command: set authentication password

Syntax

set authentication password { **cipher** | **simple** } *password*

Views

User interface view

Parameters

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a plaintext string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters.

Change description

Before modification: If **cipher** is specified, you can set a plaintext password of 1 to 16 characters or a 24-character ciphertext password.

After modification: If **cipher** is specified, you must set a ciphertext password of 1 to 53 characters.

Modified command: sham-link

Syntax

```
sham-link source-ip-address destination-ip-address [ cost cost | dead dead-interval | hello hello-interval | retransmit retrans-interval | trans-delay delay | simple [ cipher | plain ] password1 | { md5 | hmac-md5 } key-id [ cipher | plain ] password2 ] *
```

Views

OSPF area view

Parameters

source-ip-address: Source IP address for the sham link.

destination-ip-address: Destination IP address for the sham link.

cost: Cost for the sham link. It ranges from 1 to 65,535 and defaults to 1.

dead-interval: Dead Interval in seconds. It ranges from 1 to 32,768 and defaults to 40. It must be equal to the dead interval of the router on the other end of the virtual link and must be at least four times the hello interval.

hello-interval: Interval at which the interface sends hello packets. It ranges from 1 to 8,192 seconds and defaults to 10 seconds. It must be equal to the hello interval of the router on the other end of the virtual link.

retrans-interval: Interval at which the interface retransmits LSAs. It ranges from 1 to 8,192 seconds and defaults to 5 seconds.

delay: Delay interval before the interface sends an LSA. It ranges from 1 to 8,192 seconds and defaults to 1 second.

simple [**cipher** | **plain**] *password1*: Uses simple authentication.

- **cipher**: Sets a ciphertext key.
- **plain**: Sets a plaintext key.
- *password1*: Specifies the key string. This argument is case sensitive. If **cipher** is specified, it must be a ciphertext string of 1 to 41 characters. If **plain** is specified, it must be a string of 1 to 8 characters. If neither **cipher** nor **plain** is specified, you set a plaintext key string.

md5: Uses MD5 algorithm for authentication.

hmac-md5: Uses HMAC-MD5 algorithm for authentication.

key-id: Authentication key ID of the interface, in the range of 1 to 255. It must be the same as that of the peer.

- **cipher**: Sets a ciphertext key.
- **plain**: Sets a plaintext key.
- *password2*: Specifies the key string. This argument is case sensitive. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If **plain** is specified, it must be a string of 1 to 16 characters. If neither **cipher** nor **plain** is specified, you can set a plaintext key of 1 to 16 characters or a ciphertext key of 1 to 53 characters.

Change description

Before modification:

- For simple authentication, if **cipher** is specified, the *password1* argument can be either a plaintext string of 1 to 8 characters, or a ciphertext string of 24 characters.
- For MD5 authentication and HMAC-MD5 authentication, if **cipher** is specified or if neither **cipher** nor **plain** is specified, the *password2* can be either a plaintext string of 1 to 16 characters, or a ciphertext string of 24 characters.

After modification:

- For simple authentication, if **cipher** is specified, the *password1* must be a ciphertext string of 1 to 41 characters.
- For MD5 authentication and HMAC-MD5 authentication, if **cipher** is specified, the *password2* must be a ciphertext string of 1 to 53 characters. If neither **cipher** nor **plain** is specified, the *password2* can be a plaintext string of 1 to 16 characters or a ciphertext string of 1 to 53 characters.

Modified command: snmp-agent usm-user v3

Syntax

```
snmp-agent usm-user v3 user-name group-name [ cipher ] [ authentication-mode { md5 | sha }
auth-password [ privacy-mode { 3des | aes128 | des56 } priv-password ] [ acl acl-number | acl
ipv6 ipv6-acl-number ] *
```

Views

System view

Parameters

user-name: User name, a case-sensitive string of 1 to 32 characters.

group-name: Group name, a case-sensitive string of 1 to 32 characters.

cipher: Specifies that *auth-password* and *priv-password* are encrypted keys, which can be calculated to a hexadecimal string by using the **snmp-agent calculate-password** command. If this keyword is not specified, *auth-password* and *priv-password* are plaintext keys.

authentication-mode: Specifies an authentication algorithm. MD5 is faster but less secure than SHA.

- **md5**: Specifies the MD5 authentication algorithm.
- **sha**: Specifies the SHA-1 authentication algorithm.

auth-password: Specifies a case-sensitive plaintext or encrypted authentication key. A plaintext key is a string of 1 to 64 characters. If the **cipher** is specified, the encrypted authentication key length requirements differ by authentication algorithm and key string format, as shown in [Table 1](#).

Table 1 Encrypted authentication key length requirements

Authentication algorithm	Hexadecimal string	Non-hexadecimal string
MD5	32 characters	53 characters
SHA	40 characters	57 characters

privacy-mode: Specifies an encryption algorithm for privacy. The three encryption algorithms AES, 3DES, and DES are in descending order of security. Higher security means more complex implementation mechanism and lower speed. DES is enough to meet general requirements.

- **3des**: Specifies the 3DES algorithm.
- **des56**: Specifies the DES algorithm.
- **aes128**: Specifies the AES algorithm.

priv-password: Specifies a case-sensitive plaintext or encrypted privacy key. A plaintext key is a string of 1 to 64 characters. If the **cipher** keyword is specified, the encrypted privacy key length requirements differ by authentication algorithm and key string format, as shown in [Table 2](#).

Table 2 Encrypted privacy key length requirements

Authentication algorithm	Encryption algorithm	Hexadecimal string	Non-hexadecimal string
MD5	3DES	64 characters	73 characters
MD5	AES128 or DES-56	32 characters	53 characters
SHA	3DES	80 characters	73 characters
SHA	AES128 or DES-56	40 characters	53 characters

acl *acl-number*: Specifies a basic ACL to filter NMSs by source IPv4 address. The *acl-number* argument represents a basic ACL number in the range of 2000 to 2999. Only the NMSs with the IPv4 addresses permitted in the ACL can use the specified username to access the SNMP agent.

acl ipv6 *ipv6-acl-number*: Specifies a basic ACL to filter NMSs by source IPv6 address. The *ipv6-acl-number* argument represents a basic ACL number in the range of 2000 to 2999. Only the NMSs with the IPv6 addresses permitted in the ACL can use the specified username to access the SNMP agent.

local: Represents a local SNMP entity user.

engineid *engineid-string*: Specifies an SNMP engine ID as a hexadecimal string. The *engineid-string* argument must comprise an even number of hexadecimal characters, in the range of 10 to 64. All-zero and all-F strings are invalid.

Change description

Before modification: You can only set keys in hexadecimal format.

After modification: You can set keys in either hexadecimal or non-hexadecimal format.

- See [Table 1](#) for the ciphertext authentication key length requirements.
- See [Table 2](#) for the ciphertext privacy key length requirements.

Modified command: super password

Syntax

super password [**level** *user-level*] { **cipher** | **simple** } *password*

Views

System view

Parameters

level *user-level*: User privilege level, which ranges from 1 to 3 and defaults to 3.

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a plaintext string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters.

Change description

Before modification: If **cipher** is specified, you can set a plaintext password of 1 to 16 characters or a 24-character ciphertext password.

After modification: If **cipher** is specified, you must set a ciphertext password of 1 to 53 characters.

Modified command: vlink-peer

syntax

```
vlink-peer router-id [ hello seconds | retransmit seconds | trans-delay seconds | dead seconds | simple [ plain | cipher ] password | { md5 | hmac-md5 } key-id [ plain | cipher ] password ] *
```

Views

OSPF area view

Parameters

router-id: Router ID of the neighbor on the virtual link.

hello *seconds*: Hello interval in seconds, in the range of 1 to 8192. The default is 10. It must be identical to the hello interval on the virtual link neighbor.

retransmit *seconds*: Retransmission interval in seconds, in the range of 1 to 3600. The default is 5.

trans-delay *seconds*: Transmission delay interval in seconds, in the range of 1 to 3600. The default is 1.

dead *seconds*: Dead interval in seconds, in the range of 1 to 32768. The default is 40. It must be identical to that on the virtual link neighbor. The dead interval is at least four times the hello interval.

md5: MD5 authentication.

hmac-md5: HMAC-MD5 authentication.

simple: Simple authentication.

key-id: Key ID for MD5 or HMAC-MD5 authentication, in the range of 1 to 255.

cipher: Specifies a ciphertext password.

plain: Specifies a plaintext password.

password: Password. In simple authentication mode, a plaintext password is a case-sensitive string of 1 to 8 characters, and a ciphertext password is a case-sensitive string of 1 to 41 characters. In MD5/HMAC-MD5 authentication mode, a plaintext password is a case-sensitive string of 1 to 16 characters, and a ciphertext password is a case-sensitive string of 1 to 53 characters.

Change description

Before modification: If **cipher** is specified, you can enter a plaintext password or a 24-character ciphertext password.

After modification: For simple authentication, a ciphertext password comprises 1 to 41 characters. For MD5/HMAC-MD5 authentication, a ciphertext password comprises 1 to 53 characters.

Modified command: vrrp ipv6 vrid authentication-mode

Old syntax

```
vrrp ipv6 vrid virtual-router-id authentication-mode simple key
```

New syntax

```
vrrp ipv6 vrid virtual-router-id authentication-mode simple [ cipher ] key
```

Views

Interface view

Parameters

virtual-router-id: VRRP group number, which ranges from 1 to 255.

simple: Specifies the simple authentication mode.

cipher: Sets the authentication key in cipher text.

key: Authentication key, a case-sensitive string. It is a plain-text string of 1 to 8 characters if the **cipher** keyword is not specified; or a cipher text string of 1 to 41 characters if the **cipher** keyword is specified.

Change description

Before modification: In simple authentication mode, you can only set a plaintext password.

After modification: In simple authentication mode, you can use the **cipher** keyword to enter a ciphertext password of 1 to 41 characters.

Modified command: `vrrp vrid authentication-mode`

Old syntax

`vrrp vrid virtual-router-id authentication-mode { md5 | simple } key`

New syntax

`vrrp vrid virtual-router-id authentication-mode { md5 | simple } [cipher] key`

Views

Interface view

Parameters

virtual-router-id: VRRP group number, which ranges from 1 to 255.

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

cipher: Sets the authentication key in cipher text.

key: Authentication key, a case-sensitive string.

- When **md5** authentication applies, the authentication key is a plain-text string of 1 to 8 characters or a cipher text string of 24 characters if the **cipher** keyword is not specified; or a cipher text string of 1 to 41 characters if the **cipher** keyword is specified.
- When **simple** authentication applies, the authentication key is a plain-text string of 1 to 8 characters if the **cipher** keyword is not specified; or a cipher text string of 1 to 41 characters if the **cipher** keyword is specified.

Change description

Before modification:

- For MD5 authentication, a ciphertext password must comprise 24 characters.
- For simple authentication, you can only set a plaintext key.

After modification:

- For MD5 authentication, if **cipher** is specified, enter a ciphertext key of 1 to 41 characters.
- For simple authentication, if **cipher** is specified, enter a ciphertext key of 1 to 41 characters.

Modified feature: Task ID for IPv6 socket display

Feature change description

Changed the task ID value range for IPv6 socket display.

Command changes

Modified command: display ipv6 socket

Syntax

```
display ipv6 socket [ socktype socket-type ] [ task-id socket-id ] [ slot slot-number ] [ | { begin | exclude | include } regular-expression ]
```

Views

Any view

Change description

Before modification: The task ID is in the range of 1 to 150.

After modification: The task ID is in the range of 1 to 255.

Removed feature: Local user password display

Feature change description

Deleted the feature used to set a display mode for all local user passwords.

Removed commands

local-user password-display-mode

Syntax

```
local-user password-display-mode { auto | cipher-force }  
undo local-user password-display-mode
```

Views

System view

R5101P01

This release has the following changes:

None.

R5101

This release has the following changes:

None.

E5101

First release.