Contents

Introduction .......................................................................................................................... 1

Version information ............................................................................................................. 1
Version number .................................................................................................................... 1
Version history ..................................................................................................................... 1
Hardware and software compatibility matrix ................................................................... 5
ISSU compatibility list ......................................................................................................... 8
Upgrade restrictions and guidelines ................................................................................... 8

Hardware feature updates .................................................................................................. 9
Hardware feature updates in R1810P16 .............................................................................. 9
Hardware feature updates in R1810P13 ............................................................................ 9
Hardware feature updates in R1810P12 ............................................................................ 9
Hardware feature updates in R1810P11 ............................................................................ 9
Hardware feature updates in R1810P10 ............................................................................ 9
Hardware feature updates in R1810P07 .......................................................................... 9
Hardware feature updates in R1810P06 .......................................................................... 9
Hardware feature updates in R1810P03 .......................................................................... 10
Hardware feature updates in R1810P01 .......................................................................... 10
Hardware feature updates in R1810 ................................................................................ 10
Hardware feature updates in R1809P11 .......................................................................... 10
Hardware feature updates in R1809P10 .......................................................................... 10
Hardware feature updates in R1809P09 .......................................................................... 10
Hardware feature updates in R1809P06 .......................................................................... 10
Hardware feature updates in R1809P05 .......................................................................... 10
Hardware feature updates in R1809P03 .......................................................................... 10
Hardware feature updates in R1809P02 .......................................................................... 10
Hardware feature updates in R1809P01 .......................................................................... 10
Hardware feature updates in R1808P27 .......................................................................... 11
Hardware feature updates in R1808P25 .......................................................................... 11
Hardware feature updates in R1808P23 .......................................................................... 11
Hardware feature updates in R1808P22 .......................................................................... 11
Hardware feature updates in R1808P21 .......................................................................... 11
Hardware feature updates in R1808P17 .......................................................................... 11
Hardware feature updates in R1808P16 .......................................................................... 11
Hardware feature updates in R1808P15 .......................................................................... 11
Hardware feature updates in R1808P13 .......................................................................... 11
Hardware feature updates in R1808P11 .......................................................................... 11
Hardware feature updates in R1808P08 .......................................................................... 11
Hardware feature updates in R1808P06 ................................................................. 12
Hardware feature updates in R1808P02 ................................................................. 12
Hardware feature updates in R1807P02 ................................................................. 12
Hardware feature updates in F1807P01 ................................................................. 12
Hardware feature updates in F1805P02 ................................................................. 12
Hardware feature updates in F1805P01 ................................................................. 12
Hardware feature updates in F1803L03 ................................................................. 12
Hardware feature updates in F1803L01 ................................................................. 12
Hardware feature updates in F1305P01 ................................................................. 12
Hardware feature updates in R1211P04 ................................................................. 12
Hardware feature updates in R1211P02 ................................................................. 12
Hardware feature updates in R1211 ..................................................................... 13

Software feature and command updates .............................................................. 13
MIB updates ......................................................................................................... 13
Operation changes ......................................................................................... 19
  Operation changes in R1810P16 ................................................................. 19
  Operation changes in R1810P13 ................................................................. 19
  Operation changes in R1810P12 ................................................................. 19
  Operation changes in R1810P11 ................................................................. 19
  Operation changes in R1810P10 ................................................................. 19
  Operation changes in R1810P07 ................................................................. 19
  Operation changes in R1810P06 ................................................................. 19
  Operation changes in R1810P03 ................................................................. 19
  Operation changes in R1810P01 ................................................................. 20
  Operation changes in R1810 ..................................................................... 20
  Operation changes in R1809P11 ................................................................. 20
  Operation changes in R1809P10 ................................................................. 20
  Operation changes in R1809P09 ................................................................. 20
  Operation changes in R1809P06 ................................................................. 20
  Operation changes in R1809P05 ................................................................. 20
  Operation changes in R1809P03 ................................................................. 20
  Operation changes in R1809P02 ................................................................. 20
  Operation changes in R1809P01 ................................................................. 20
  Operation changes in R1808P27 ................................................................. 21
  Operation changes in R1808P25 ................................................................. 21
  Operation changes in R1808P23 ................................................................. 21
  Operation changes in R1808P22 ................................................................. 21
  Operation changes in R1808P21 ................................................................. 21
  Operation changes in R1808P17 ................................................................. 21
Operation changes in R1808P16 ................................................................. 21
Operation changes in R1808P15 ................................................................. 21
Operation changes in R1808P13 ................................................................. 21
Operation changes in R1808P11 ................................................................. 22
Operation changes in R1808P08 ................................................................. 22
Operation changes in R1808P06 ................................................................. 22
Operation changes in R1808P02 ................................................................. 22
Operation changes in R1807P02 ................................................................. 22
Operation changes in F1807P01 ................................................................. 23
Operation changes in F1805P02 ................................................................. 23
Operation changes in F1805P01 ................................................................. 23
Operation changes in F1803L03 ................................................................. 24
Operation changes in F1803L01 ................................................................. 24
Operation changes in F1305P01 ................................................................. 24
Operation changes in R1211P04 ................................................................. 25
Operation changes in R1211P02 ................................................................. 25
Operation changes in R1211 ................................................................. 25

Restrictions and cautions ........................................................................ 25
Open problems and workarounds ............................................................. 25
List of resolved problems ................................................................. 26
  Resolved Problems in R1810P16 ................................................................. 26
  Resolved Problems in R1810P13 ................................................................. 27
  Resolved Problems in R1810P12 ................................................................. 28
  Resolved Problems in R1810P11 ................................................................. 28
  Resolved Problems in R1810P10 ................................................................. 28
  Resolved Problems in R1810P07 ................................................................. 29
  Resolved Problems in R1810P06 ................................................................. 30
  Resolved Problems in R1810P03 ................................................................. 30
  Resolved Problems in R1810P01 ................................................................. 31
  Resolved Problems in R1810 ................................................................. 31
  Resolved Problems in R1809P11 ................................................................. 31
  Resolved Problems in R1809P10 ................................................................. 32
  Resolved Problems in R1809P09 ................................................................. 33
  Resolved Problems in R1809P06 ................................................................. 34
  Resolved Problems in R1809P05 ................................................................. 35
  Resolved Problems in R1809P03 ................................................................. 36
  Resolved Problems in R1809P02 ................................................................. 37
  Resolved Problems in R1809P01 ................................................................. 37
  Resolved Problems in R1808P27 ................................................................. 39
Resolved Problems in R1808P25 ................................................................. 39
Resolved Problems in R1808P23 ................................................................. 41
Resolved Problems in R1808P22 ................................................................. 41
Resolved Problems in R1808P21 ................................................................. 42
Resolved Problems in R1808P17 ................................................................. 42
Resolved Problems in R1808P16 ................................................................. 44
Resolved Problems in R1808P15 ................................................................. 44
Resolved Problems in R1808P13 ................................................................. 45
Resolved problems in R1808P11 ................................................................. 45
Resolved problems in R1808P08 ................................................................. 48
Resolved problems in R1808P06 ................................................................. 49
Resolved problems in R1808P02 ................................................................. 50
Resolved problems in R1807P02 ................................................................. 54
Resolved problems in F1807P01 ................................................................. 54
Resolved problems in F1805P02 ................................................................. 55
Resolved problems in F1805P01 ................................................................. 55
Resolved problems in F1803L03 ................................................................. 57
Resolved problems in F1803L01 ................................................................. 57
Resolved problems in F1305P01 ................................................................. 58
Resolved problems in R1211P04 ................................................................. 59
Resolved problems in R1211P02 ................................................................. 61
Resolved problems in R1211 ....................................................................... 62

Support and other resources ..................................................................... 62
Accessing Hewlett Packard Enterprise Support ........................................ 62
Documents ................................................................................................. 63
Related documents .................................................................................... 63
Documentation feedback ........................................................................... 63

Appendix A Feature list ............................................................................. 64
Hardware features ...................................................................................... 64
5800 ........................................................................................................ 64
5820X ..................................................................................................... 70
Software features ...................................................................................... 72

Appendix B Upgrading software ................................................................. 83
Upgrading software from Boot ROM menus ............................................. 83
Accessing the basic Boot menu ................................................................. 85
Accessing the extended Boot menu .......................................................... 86
Using XMODEM to upgrade software through the console port ............... 88
Using TFTP to upgrade software through an Ethernet port .................... 97
Using FTP to upgrade software through an Ethernet Port ....................... 100
List of tables

Table 1 Version history ................................................................. 1
Table 2 Hardware and software compatibility matrix ...................................................... 5
Table 3 ISSU compatibility list .......................................................... 8
Table 4 MIB updates ........................................................................ 13
Table 5 Models in the HPE 5800 Switch Series ......................................................... 64
Table 6 HPE 5800 Switch Series technical specifications ........................................... 65
Table 7 Pluggable component (except the OAP cards) compatibility matrix ................. 67
Table 8 OAP card compatibility matrix ..................................................................... 69
Table 9 RPS compatibility matrix .......................................................................... 69
Table 10 Models in the HPE 5820X Switch Series .................................................... 70
Table 11 The HPE 5820X Switch Series technical specifications ............................. 70
Table 12 Pluggable components (except the OAP cards) compatibility matrix ............ 71
Table 13 OAP card compatibility matrix .................................................................. 72
Table 14 RPS compatibility matrix .......................................................................... 72
Table 15 Software features of the 5800 series ......................................................... 72
Table 16 Software features of the 5820X series ...................................................... 77
Table 17 Software upgrade methods ........................................................................ 83
Table 18 Shortcut keys ................................................................................. 84
Table 19 Basic Boot ROM menu options ............................................................... 85
Table 20 BASIC-ASSISTANT menu options ......................................................... 86
Table 21 Extended Boot ROM menu options ......................................................... 87
Table 22 EXTEND-ASSISTANT menu options ....................................................... 88
Table 23 Boot ROM update menu options ............................................................ 92
Table 24 File transfer protocol menu options .......................................................... 92
Table 25 TFTP parameter settings ...................................................................... 99
Table 26 FTP parameter settings ..................................................................... 101
Introduction

This document describes the features, restrictions and guidelines, open problems, and workarounds for version A5800_5820X-CMW520-R1810P16. Before you use this version on a live network, back up the configuration and test the version to avoid software upgrade affecting your live network.

Use this document in conjunction with HPE A5800_5820X-CMW520-R1810P16 Release Notes (Software Feature Changes) and the documents listed in "Related documents."

Version information

Version number

Comware software, Version 5.20, Release 1810P16

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

<table>
<thead>
<tr>
<th>Version number</th>
<th>Last version</th>
<th>Release date</th>
<th>Release type</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5800_5820X-CMW520-R1810P16</td>
<td>A5800_5820X-CMW520-R1810P13</td>
<td>2018-07-26</td>
<td>Release version</td>
<td>This version fixed bugs and introduced feature changes. New features include: - ITU channel number for a transceiver module Fixed bugs.</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1810P12</td>
<td>A5800_5820X-CMW520-R1810P11</td>
<td>2017-03-22</td>
<td>Release version</td>
<td>This version fixed bugs and introduced feature changes. New features include: - Transparent transmission for protocol packets in a VPN Fixed bugs.</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1810P11</td>
<td>A5800_5820X-CMW520-R1810P10</td>
<td>2017-02-21</td>
<td>Release version</td>
<td>Fixes bugs</td>
</tr>
<tr>
<td>Version number</td>
<td>Last version</td>
<td>Release date</td>
<td>Release type</td>
<td>Remarks</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------</td>
<td>--------------</td>
<td>--------------</td>
<td>---------</td>
</tr>
<tr>
<td>A5800_5820X-CM W520-R1810P10</td>
<td>A5800_5820X-CMW520-R1810P07</td>
<td>2016-12-20</td>
<td>Release version</td>
<td>Fixes bugs</td>
</tr>
<tr>
<td>A5800_5820X-CM W520-R1810P07</td>
<td>A5800_5820X-CMW520-R1810P06</td>
<td>2016-08-24</td>
<td>Release version</td>
<td>Fixes bugs</td>
</tr>
<tr>
<td>A5800_5820X-CM W520-R1810P06</td>
<td>A5800_5820X-CMW520-R1810P03</td>
<td>2016-07-19</td>
<td>Release version</td>
<td>Fixes bugs</td>
</tr>
<tr>
<td>A5800_5820X-CM W520-R1810P03</td>
<td>A5800_5820X-CMW520-R1810P01</td>
<td>2016-02-18</td>
<td>Release version</td>
<td>Fixes bugs</td>
</tr>
<tr>
<td>A5800_5820X-CM W520-R1810P01</td>
<td>A5800_5820X-CMW520-R1810</td>
<td>2016-01-13</td>
<td>Release version</td>
<td>Fixes bugs</td>
</tr>
<tr>
<td>A5800_5820X-CM W520-R1810</td>
<td>A5800_5820X-CMW520-R1809P11</td>
<td>2015-12-02</td>
<td>Release version</td>
<td>Fixes bugs</td>
</tr>
<tr>
<td>A5800_5820X-CM W520-R1809P11</td>
<td>A5800_5820X-CMW520-R1809P10</td>
<td>2015-09-16</td>
<td>Release version</td>
<td>Fixes bugs</td>
</tr>
<tr>
<td>A5800_5820X-CM W520-R1809P10</td>
<td>A5800_5820X-CMW520-R1809P09</td>
<td>2015-07-29</td>
<td>Release version</td>
<td>Adds the features:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1. Disabling reactivation for edge ports shut down by BPDU guard</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Modify the features:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1. Specifying multiple secondary HWTACACS servers</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2. Disabling advertising prefix information in RA messages</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Fixes bugs</td>
</tr>
<tr>
<td>A5800_5820X-CM W520-R1809P09</td>
<td>A5800_5820X-CMW520-R1809P06</td>
<td>2015-06-10</td>
<td>Release version</td>
<td>Adds the features:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1. VLAN-specific DHCP snooping</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Fixes bugs</td>
</tr>
</tbody>
</table>

**Modified feature:**
- 1. NTP support for ACL
- 1. Displaying VLAN interface information
- 1. Default settings configuration for prefixes advertised in RA messages
- 1. Prefix information configuration in RA messages
- 2. Configuring the description of a VLAN
- 1. Route summarization on an ASBR
- 1. Specifying multiple secondary HWTACACS servers
<table>
<thead>
<tr>
<th>Version number</th>
<th>Last version</th>
<th>Release date</th>
<th>Release type</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| A5800_5820X-CM W520-R1809P06 | A5800_5820X-CMW520-R1809P05 | 2015-04-10   | Release version | Adds the features: 1. link aggregation management VLANs and management port  
<p>|                   |                           |              |               | Fixes bugs                                                              |
| A5800_5820X-CM W520-R1809P05  | A5800_5820X-CMW520-R1809P03 | 2015-03-24   | Release version |                          |
| A5800_5820X-CM W520-R1809P03   | A5800_5820X-CMW520-R1809P02 | 2015-02-12   | Release version | Adds features                                                              |
| A5800_5820X-CM W520-R1809P02   | A5800_5820X-CMW520-R1809P01 | 2014-12-29   | Release version | Adds features                                                              |
| A5800_5820X-CM W520-R1809P01   | A5800_5820X-CMW520-R1808P27 | 2014-11-03   | Release version | Adds features                                                              |
| A5800_5820X-CM W520-R1808P16   | A5800_5820X-CMW520-R1808P15 | 2013-12-03   | Release version | Fixes bugs                                                                |</p>
<table>
<thead>
<tr>
<th>Version number</th>
<th>Last version</th>
<th>Release date</th>
<th>Release type</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5800_5820X-CM W520-R1808P13</td>
<td>A5800_5820X-CMW520-R1808P11</td>
<td>2013-09-06</td>
<td>Release version</td>
<td>Fixes bugs</td>
</tr>
<tr>
<td>A5800_5820X-CM W520-R1808P11</td>
<td>A5800_5820X-CMW520-R1808P08</td>
<td>2013-08-23</td>
<td>Release version</td>
<td>Fixes bugs</td>
</tr>
<tr>
<td>A5800_5820X-CM W520-R1808P08</td>
<td>A5800_5820X-CMW520-R1808P06</td>
<td>2013-06-20</td>
<td>Release version</td>
<td>Fixes bugs</td>
</tr>
<tr>
<td>A5800_5820X-CM W520-R1808P06</td>
<td>A5800_5820X-CMW520-R1808P02</td>
<td>2013-04-22</td>
<td>Release version</td>
<td>Fixes bugs</td>
</tr>
<tr>
<td>A5800_5820X-CM W520-R1808P02</td>
<td>A5800_5820X-CMW520-R1808P07</td>
<td>2013-03-22</td>
<td>Release version</td>
<td>Fixes bugs</td>
</tr>
<tr>
<td>A5800_5820X-CM W520-R1807P02</td>
<td>A5800_5820X-CMW520-F1807P01</td>
<td>2013-01-27</td>
<td>Release version</td>
<td>Adds features</td>
</tr>
<tr>
<td>A5800_5820X-CM W520-F1807P01</td>
<td>A5800_5820X-CMW520-F1805P02</td>
<td>2012-12-17</td>
<td>Feature version</td>
<td>New feature: Disabling MAC entry aging timer refresh based on destination MAC address</td>
</tr>
<tr>
<td>A5800_5820X-CM W520-F1805P02</td>
<td>A5800_5820X-CMW520-F1805P01</td>
<td>2012-10-12</td>
<td>Feature version</td>
<td>Operation changes</td>
</tr>
</tbody>
</table>
## 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

<table>
<thead>
<tr>
<th>Item</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product family</td>
<td>5800/5820X Series</td>
</tr>
<tr>
<td>Hardware platform</td>
<td>HPE 5800-24G-PoE+ Switch(JC099A)</td>
</tr>
<tr>
<td></td>
<td>HPE 5800-24G Switch(JC100A)</td>
</tr>
<tr>
<td></td>
<td>HPE 5800-48G-PoE+ Switch with 2 Interface Slots(JC101A)</td>
</tr>
<tr>
<td></td>
<td>HPE 5800-24G-SFP Switch with 1 Interface Slot(JC103A)</td>
</tr>
<tr>
<td></td>
<td>HPE 5800-48G-PoE+ Switch with 1 Interface Slot(JC104A)</td>
</tr>
<tr>
<td></td>
<td>HPE 5800-48G Switch with 1 Interface Slot(JC105A)</td>
</tr>
<tr>
<td></td>
<td>HPE 5820X-14XG-SFP+ Switch with 2 Interface Slots(JC106A)</td>
</tr>
<tr>
<td>Item</td>
<td>Specifications</td>
</tr>
<tr>
<td>------</td>
<td>----------------</td>
</tr>
<tr>
<td>HPE 5820X-24XG-SFP+ Switch(JC102A)</td>
<td></td>
</tr>
<tr>
<td>HPE 5800AF-48G Switch(JG225A)</td>
<td></td>
</tr>
<tr>
<td>HPE 5820AF-24XG Switch(JG219A)</td>
<td></td>
</tr>
<tr>
<td>HPE 5800-24G-PoE+ TAA Switch(JG254A)</td>
<td></td>
</tr>
<tr>
<td>HPE 5800-24G TAA Switch(JG255A)</td>
<td></td>
</tr>
<tr>
<td>HPE 5800-48G-PoE+ TAA Switch with 2 Interface Slots(JG242A)</td>
<td></td>
</tr>
<tr>
<td>HPE 5800-24G-SFP TAA Switch with 1 Interface Slot(JG256A)</td>
<td></td>
</tr>
<tr>
<td>HPE 5800-48G-PoE+ TAA Switch with 1 Interface Slot(JG257A)</td>
<td></td>
</tr>
<tr>
<td>HPE 5800-48G TAA Switch with 1 Interface Slot(JG258A)</td>
<td></td>
</tr>
<tr>
<td>HPE 5820X-14XG-SFP+ TAA Switch with 2 Interface Slots(JG259A)</td>
<td></td>
</tr>
<tr>
<td>HPE 5820X-24XG-SFP+ TAA Switch(JG243A)</td>
<td></td>
</tr>
<tr>
<td>HPE 5800-24G-PoE+ Switch(JC099B)</td>
<td></td>
</tr>
<tr>
<td>HPE 5800-24G Switch(JC100B)</td>
<td></td>
</tr>
<tr>
<td>HPE 5800-48G-PoE+ Switch with 2 Interface Slots(JC101B)</td>
<td></td>
</tr>
<tr>
<td>HPE 5800-24G-SFP Switch with 1 Interface Slot(JC103B)</td>
<td></td>
</tr>
<tr>
<td>HPE 5800-48G-PoE+ Switch with 1 Interface Slot(JC104B)</td>
<td></td>
</tr>
<tr>
<td>HPE 5800-48G Switch with 1 Interface Slot(JC105B)</td>
<td></td>
</tr>
<tr>
<td>HPE 5820X-14XG-SFP+ Switch with 2 Interface Slots(JC106B)</td>
<td></td>
</tr>
<tr>
<td>HPE 5820X-24XG-SFP+ Switch(JC102B)</td>
<td></td>
</tr>
<tr>
<td>HPE 5800AF-48G Switch(JG225B)</td>
<td></td>
</tr>
<tr>
<td>HPE 5820AF-24XG Switch(JG219B)</td>
<td></td>
</tr>
<tr>
<td>HPE 5800-24G-PoE+ TAA Switch(JG254B)</td>
<td></td>
</tr>
<tr>
<td>HPE 5800-24G TAA Switch(JG255B)</td>
<td></td>
</tr>
<tr>
<td>HPE 5800-48G-PoE+ TAA Switch with 2 Interface Slots(JG242B)</td>
<td></td>
</tr>
<tr>
<td>HPE 5800-24G-SFP TAA Switch with 1 Interface Slot(JG256B)</td>
<td></td>
</tr>
<tr>
<td>HPE 5800-48G-PoE+ TAA Switch with 1 Interface Slot(JG257B)</td>
<td></td>
</tr>
<tr>
<td>HPE 5800-48G TAA Switch with 1 Interface Slot(JG258B)</td>
<td></td>
</tr>
<tr>
<td>HPE 5820X-14XG-SFP+ TAA Switch with 2 Interface Slots(JG259B)</td>
<td></td>
</tr>
<tr>
<td>HPE 5820X-24XG-SFP+ TAA Switch(JG243B)</td>
<td></td>
</tr>
</tbody>
</table>

**Memory**: 512 MB/1GB/2GB

**Flash**: 512 MB

**Boot ROM version**: Version 303 or higher (Note: Perform the command display version command in any view to view the version information. See Note ②)

**Host software**: A5800_5820X-CMW520-R1810P16.bin
<table>
<thead>
<tr>
<th>Item</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>iMC version</td>
<td>iMC BIMS 7.3 (E0501)</td>
</tr>
<tr>
<td></td>
<td>iMC EAD 7.3 (E0502)</td>
</tr>
<tr>
<td></td>
<td>iMC UAM 7.3 (E0503)</td>
</tr>
<tr>
<td></td>
<td>iMC TAM 7.3 (E0503)</td>
</tr>
<tr>
<td></td>
<td>iMC MVM 7.3 (E0501)</td>
</tr>
<tr>
<td></td>
<td>iMC NTA 7.3 (E0502)</td>
</tr>
<tr>
<td></td>
<td>iMC PLAT 7.3 (E0605)</td>
</tr>
<tr>
<td></td>
<td>iMC QoS 7.3 (E0501)</td>
</tr>
<tr>
<td></td>
<td>iMC RAM 7.3 (E0502)</td>
</tr>
<tr>
<td></td>
<td>iMC SHM 7.3 (E0502)</td>
</tr>
<tr>
<td></td>
<td>iMC UBA 7.3 (E0502)</td>
</tr>
<tr>
<td>iNode version</td>
<td>iNode PC 7.3 (E0504)</td>
</tr>
<tr>
<td>OAA version</td>
<td>Fiber Channel Card: 9.0.6.15.0</td>
</tr>
<tr>
<td></td>
<td>IPS/AV Card: ESS2113P03</td>
</tr>
<tr>
<td></td>
<td>Fire Wall Card: F3171P17</td>
</tr>
<tr>
<td></td>
<td>High Performance Wireless AC Card: R3308P11</td>
</tr>
<tr>
<td></td>
<td>Wireless AC Card: R2308P11</td>
</tr>
</tbody>
</table>

Sample: To display the host software and Boot ROM version of the 5800/5820X, perform the following:

```bash
<HPE>display version
HPE Comware Platform Software
Comware Software, Version 5.20.105, Release 1810P16          ------- Note ①
Copyright (c) 2010-2018 Hewlett Packard Enterprise Development LP
HPE 5800-48G Switch with 1 Interface Slot uptime is 0 week, 2 days, 17 hours, 42 minutes

HPE 5800-48G Switch with 1 Interface Slot with 2 Processors
512M    bytes SDRAM
4M      bytes Nor Flash Memory
512M    bytes Nand Flash Memory
Config Register points to Nand Flash

Hardware Version is Ver.B
CPLD Version is 004
**BootRom Version is 303**                              ------- Note ②
[SubSlot 0] 48GE+4SFP Plus Hardware Version is Ver.B
[SubSlot 1] No Module
```
### ISSU compatibility list

**Table 3 ISSU compatibility list**

<table>
<thead>
<tr>
<th>Current version</th>
<th>Earlier version</th>
<th>Compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5800_5820X-CMW520-R1810P16</td>
<td>A5800_5820X-CMW520-R1810P13</td>
<td>No</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1810P12</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1810P11</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1810P10</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1810P07</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1810P06</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1810P03</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1810P01</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1810</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1809P11</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1809P10</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1809P09</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1809P06</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1809P05</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1809P03</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1809P02</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1809P01</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1808P27</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1808P25</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1808P23</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1808P22</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1808P21</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1808P17</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1808P16</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1808P15</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1808P13</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1808P11</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

### 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.

The version F1803L01 or later adopts a new password encryption algorithm. The password saved in the configuration file has been processed by the new algorithm. If you roll back the software from the
version F1803L01 or later to a version before F1803L01, the password cannot be restored, and login will fail.

Not support using the ISSU compatible mode to upgrade the software from the version before F1807P01 to the version F1807P01 or later.

Release R1809P02 or later don’t support roll back to a version before R1809P02 for product code. The switch with new nandflash and 2G SDRAM cannot run on a version before R1809P01.

[LDP GR] Two switches are connected through an IRF fabric, and LDP GR is enabled on one of the two switches and on the IRF fabric. If a master/subordinate switchover is performed, the two switches cannot communicate with each other until the switchover is complete or the LDP neighbor liveness timer expires.

**Hardware feature updates**

**Hardware feature updates in R1810P16**
None

**Hardware feature updates in R1810P13**
None

**Hardware feature updates in R1810P12**
None

**Hardware feature updates in R1810P11**
None

**Hardware feature updates in R1810P10**
None

**Hardware feature updates in R1810P07**
1. Support SFP GE 80km transceiver

**Hardware feature updates in R1810P06**
None
Hardware feature updates in R1810P03
None

Hardware feature updates in R1810P01
None

Hardware feature updates in R1810
None

Hardware feature updates in R1809P11
None

Hardware feature updates in R1809P10
None

Hardware feature updates in R1809P09
None

Hardware feature updates in R1809P06
None

Hardware feature updates in R1809P05
None

Hardware feature updates in R1809P03
None

Hardware feature updates in R1809P02
None

Hardware feature updates in R1809P01

1. Added support for new nandflash and 2G SDRAM.
Hardware feature updates in R1808P27
  None

Hardware feature updates in R1808P25
  1. Added support for the 10GBase-ZR SFP+ DWDM transceiver.

Hardware feature updates in R1808P23
  None

Hardware feature updates in R1808P22
  None

Hardware feature updates in R1808P21
  None

Hardware feature updates in R1808P17
  1. HP 5820AF-25XG/HP 5800AF-48G support 300W power.

Hardware feature updates in R1808P16
  None

Hardware feature updates in R1808P15
  None

Hardware feature updates in R1808P13
  None

Hardware feature updates in R1808P11
  None

Hardware feature updates in R1808P08
  None
Hardware feature updates in R1808P06

1. Added support for 10GBASE-ZR SFP Plus fiber modules.

Hardware feature updates in R1808P02

1. Added two new 10GBASE-T cards: LSW1XGT4P0 and LSW1XGT2P0.

Hardware feature updates in R1807P02

None

Hardware feature updates in F1807P01

None

Hardware feature updates in F1805P02

None

Hardware feature updates in F1805P01

1. Support for the cable for SFF-8472 11.0.

Hardware feature updates in F1803L03

None

Hardware feature updates in F1803L01

None

Hardware feature updates in F1305P01

None

Hardware feature updates in R1211P04

None

Hardware feature updates in R1211P02

None
Hardware feature updates in R1211

First release

Software feature and command updates

For more information about the software feature and command update history, see HPE A5800_5820X-CMW520-R1810P16 Release Notes (Software Feature Changes).

MIB updates

Table 4 MIB updates

<table>
<thead>
<tr>
<th>Item</th>
<th>MIB file</th>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5800_5820X-CMW520-R1810P16</td>
<td>New</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Modified</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1810P13</td>
<td>New</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Modified</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1810P12</td>
<td>New</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Modified</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1810P11</td>
<td>New</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Modified</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1810P10</td>
<td>New</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Modified</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1810P07</td>
<td>New</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Modified</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1810P06</td>
<td>New</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Modified</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1810P03</td>
<td>New</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Modified</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1810P01</td>
<td>New</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Modified</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Item</td>
<td>MIB file</td>
<td>Module</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td><strong>A5800_5820X-CMW520-R1810</strong></td>
<td>New</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td><strong>A5800_5820X-CMW520-R1809P11</strong></td>
<td>New</td>
<td>hh3c-entity-ext.mib</td>
<td>HH3C-ENTITY-EXT-MIB Add hh3cEntityExtPowerTable</td>
</tr>
<tr>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td><strong>A5800_5820X-CMW520-R1809P10</strong></td>
<td>New</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td><strong>A5800_5820X-CMW520-R1809P09</strong></td>
<td>New</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td><strong>A5800_5820X-CMW520-R1809P06</strong></td>
<td>New</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td><strong>A5800_5820X-CMW520-R1809P05</strong></td>
<td>New</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td><strong>A5800_5820X-CMW520-R1809P03</strong></td>
<td>New</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td><strong>A5800_5820X-CMW520-R1809P02</strong></td>
<td>New</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td><strong>A5800_5820X-CMW520-R1809P01</strong></td>
<td>New</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Modified</td>
<td>rfc4133-entity.mib</td>
<td>ENTITY-MIB</td>
<td>entPhysicalModelName return J number</td>
</tr>
<tr>
<td><strong>A5800_5820X-CMW520-R1808P27</strong></td>
<td>New</td>
<td>rfc4292-ip-forward.mib</td>
<td>IP-FORWARD-MIB Added inetCidrRouteTable Added inetCidrRouteNumber and inetCidrRouteDiscards in Scalar objects</td>
</tr>
<tr>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td><strong>A5800_5820X-CMW520-R1808P25</strong></td>
<td>New</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Item</td>
<td>MIB file</td>
<td>Module</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1808P23</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1808P22</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1808P21</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1808P17</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1808P16</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1808P15</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1808P13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New</td>
<td>hh3c-stack.mib</td>
<td>HH3C-STACK-MIB</td>
<td>hh3cStackPortForwardingPath</td>
</tr>
<tr>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1808P11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New</td>
<td>hh3c-cbqos2.mib</td>
<td>HH3C-CBQOS2-MIB</td>
<td>Added node: hh3cCBQoSAccountingMode</td>
</tr>
<tr>
<td>Modified</td>
<td>hh3c-cbqos2.mib</td>
<td>HH3C-CBQOS2-MIB</td>
<td>Modified node: h3cCBQoSAccountingBytes. If the hh3cCBQoSAccountingMode node is set to byte mode, the h3cCBQoSAccountingBytes node can return the value.</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1808P08</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New</td>
<td>rfc4133-entity.mib, hh3c-splat-mix.mib</td>
<td>ENTITY-MIB, HH3C-LswMix-MIB</td>
<td>Added nodes: hh3cLswMpuSwitchsNum, hh3cLswLastSwitchDate, entPhysicalModelName support for modules' J number</td>
</tr>
<tr>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Item</td>
<td>MIB file</td>
<td>Module</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1808P06</td>
<td>New</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1808P02</td>
<td>New</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Modified</td>
<td>rfc1213.mib rfc3418-snmpv2.mib</td>
<td>RFC1213-MIB</td>
<td>The maximum character string length allowed by the sysLocation and sysContact nodes was changed from 200 to 255.</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-R1807P02</td>
<td>New</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-F1807P01</td>
<td>New</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-F1805P02</td>
<td>New</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-F1805P01</td>
<td>New</td>
<td>hh3c-transceiver-info.mib</td>
<td>Added nodes in hh3cTransceiverInfoTable as below: hh3cTransceiverTempHiAlarm hh3cTransceiverTempLoAlarm hh3cTransceiverTempHiWarn hh3cTransceiverTempLoWarn hh3cTransceiverVccHiAlarm hh3cTransceiverVccLoAlarm hh3cTransceiverVccHiWarn hh3cTransceiverVccLoWarn hh3cTransceiverBiasHiAlarm hh3cTransceiverBiasLoAlarm hh3cTransceiverBiasHiWarn hh3cTransceiverBiasLoWarn hh3cTransceiverPwrOutHiAlarm hh3cTransceiverPwrOutLoAlarm hh3cTransceiverPwrOutHiWarn hh3cTransceiverPwrOutLoWarn hh3cTransceiverRcvPwrHiAlarm hh3cTransceiverRcvPwrLoAlarm hh3cTransceiverRcvPwrHiWarn hh3cTransceiverRcvPwrLoWarn hh3cTransceiverErrors</td>
</tr>
<tr>
<td>Modified</td>
<td>hh3c-syslog.mib</td>
<td>HH3C-SYSLOG-MIB</td>
<td>Added hh3cSyslogLogbufContTable</td>
</tr>
<tr>
<td>Item</td>
<td>MIB file</td>
<td>Module Description</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>-------------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>Hh3c-common-system.mib</td>
<td>HH3C-COMMON-N-SYSTEM-MIB</td>
<td>Added hh3cSysBannerMOTD</td>
</tr>
<tr>
<td>Hh3c-lsw-dev-adm.mib</td>
<td>HH3C-LSW-DEV-ADM-MIB</td>
<td>Add nodes in hh3cLswSlotTable as below: hh3cLswSlotPktBufFree hh3cLswSlotPktBufInit hh3cLswSlotPktBufMin hh3cLswSlotPktBufMiss</td>
<td></td>
</tr>
<tr>
<td>Hh3c-evc.mib</td>
<td>HH3C-EVC-MIB</td>
<td>Added: hh3cEvcSrvInstTable hh3cEvcSrvInstCarTable hh3cEvcSrvInstStatInfoTable</td>
<td></td>
</tr>
<tr>
<td>RFC5602-pw-mpls-std.mib</td>
<td>PW-MPLS-STD-MIB</td>
<td>Added: pwMplsOutboundTable pwMplsTable</td>
<td></td>
</tr>
<tr>
<td>RFC5601-pw-std.mib</td>
<td>PW-STD-MIB</td>
<td>Added: pwPerfCurrentTable pwPeerMappingTable pwTable</td>
<td></td>
</tr>
<tr>
<td>Hh3c-te-tunnel.mib</td>
<td>HH3C-TE-TUNNEL-MIB</td>
<td>Added: hh3cTeTunnelMaxTunnelIndex hh3cTeTunnelStaticCrlspTable hh3cTeTunnelCoTable hh3cTeTunnelPsTable</td>
<td></td>
</tr>
<tr>
<td>RFC4292-ip-forward.mib</td>
<td>IP-FORWARD-MIB</td>
<td>Added ipCidrRouteTable</td>
<td></td>
</tr>
<tr>
<td>Hh3c-cbqos2.mib</td>
<td>HH3C-CBQOS2-MIB</td>
<td>Added hh3cCBQoSPolicyClassCfgInfoTable</td>
<td></td>
</tr>
<tr>
<td>Hh3c-entity-ext.mib</td>
<td>HH3C-ENTITY-EXT-MIB</td>
<td>Modify hh3cEntityExtTemperature in hh3cEntityExtStateTable</td>
<td></td>
</tr>
<tr>
<td>Hh3c-radius.mib</td>
<td>HH3C-RADIUS-MIB</td>
<td>Modified the value returned by the following MIBs from a plaintext or ciphertext password to empty or &quot;******&quot;: hh3cUserPassword hh3cRdKey hh3cRdSecKey hh3cRdAccKey hh3cRdSecAccKey hh3cRadiusSchAuthPrimKey hh3cRadiusSchAuthSecKey hh3cRadiusSchAccPrimKey hh3cRadiusSchAccSecKey hh3cDot11SrvSecurityPskKeyString hh3cSecureRalmAuthPassword hh3cDot11SecurityPskKeyString</td>
<td></td>
</tr>
<tr>
<td>Item</td>
<td>MIB file</td>
<td>Module</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>A5800_5820X-CMW520-F1803L03</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

| A5800_5820X-CMW520-F1803L01 |                           |                 |                                                                             |
| New                   | None                      | None            | None                                                                        |
| Modified              | None                      | None            | None                                                                        |

| A5800_5820X-CMW520-F1305P01 |                           |                 |                                                                             |
| New | Rfc5240-pim-bsr.mib | PIM-BSR-MIB  | Added PIM-BSR-MIB                                                             |
|     | Rfc5060-pim-std.mib | PIM-STD-MIB  | Added PIM-STD-MIB                                                             |
|     | savi-mib.mib      | SAVI-MID      | Added SAVI-MIB                                                               |
| Modified | hh3c-config-man.mib | HH3C-CONFIG-MAN-MIB | Modified hh3cCfgLogTable in HH3C-CONFIG-MAN-MIB.  |
|     | hh3c-flash-man.mib | HH3C-FLASH-MAN-MIB | Modified hh3cFlhOpTable in HH3C-FLASH-MAN-MIB.  |
|     | rfc2011-ip-icmp.mib | IP-MIB        | Modified ipRouteTable in IP-MIB.  |
|     | rfc2465-ipv6.mib  | IPv6-MIB      | Modified ipv6RouteNumber in IPv6-MIB.  |

| A5800_5820X-CMW520-R1211P04 |                           |                 |                                                                             |
| New | hh3c-if-ext.mib   | HH3C-IF-EXT-MIB | Added hh3cIfIsPoe.                                                            |
|     | hh3c-ntp.mib      | HH3C-NTP-MIB   | Added hh3cNTPSysPollSec.                                                     |
|     |                 |                 | Added hh3cNTPSysClockSec.                                                    |
|     |                 |                 | Added hh3cNTPServerIP.                                                       |
| Modified | None          | None            | None                                                                        |

| A5800_5820X-CMW520-R1211P02 |                           |                 |                                                                             |
| New                   | None                      | None            | None                                                                        |
| Modified              | None                      | None            | None                                                                        |

| A5800_5820X-CMW520-R1211 |                           |                 |                                                                             |
| New                   | None                      | None            | None                                                                        |
| Modified              | None                      | None            | None                                                                        |
Operation changes

Operation changes in R1810P16
  None

Operation changes in R1810P13
  None

Operation changes in R1810P12
  None

Operation changes in R1810P11
  None

Operation changes in R1810P10
  1. Packets sent by DHCPv6 relay support carrying Option18/37 added by DHCPv6 relay and DHCPv6 snooping
     Before modification: Packets sent by DHCPv6 relay can carry only Option18/37 added by DHCPv6 relay.
     After modification: Packets sent by DHCPv6 relay support carrying Option18/37 added by DHCPv6 relay and DHCPv6 snooping.

Operation changes in R1810P07
  1. Added log entries for invalid ARP packets: The ARP packets received on an interface have the same IP address as a local learned ARP entry but have different source MAC addresses.
     Before modification: The system does not print log entries when receiving ARP packets that have the same IP address as a local learned ARP entry but have different source MAC addresses.
     After modification: The system prints log entries when receiving ARP packets that have the same IP address as a local learned ARP entry but have different source MAC addresses.

Operation changes in R1810P06
  None

Operation changes in R1810P03
  None
Operation changes in R1810P01

None

Operation changes in R1810

None

Operation changes in R1809P11

None

Operation changes in R1809P10

None

Operation changes in R1809P09

1. Increased the number of supported syslog servers from 4 to 20.
2. Increased the number of gateways that a VLAN can learn and maintain in automatic MFF from 20 to 64.

Operation changes in R1809P06

None

Operation changes in R1809P05

None

Operation changes in R1809P03

None

Operation changes in R1809P02

None

Operation changes in R1809P01

1. Change to the priority order of a 128-bit IPv6 route and an IPv6 neighbor entry
   Before modification, the priority of an IPv6 neighbor entry is higher.
   After modification, the priority of a 128-bit IPv6 route is higher.
Operation changes in R1808P27

1. Change to ACL-based redirect action
   Before modification, the redirect action cannot work with any other action.
   After modification, the redirect action can work with the accounting action.

2. Port range change to advanced ACLs 3000 through 3999
   Before modification, the number of port ranges in all configured advanced ACLs cannot exceed 32.
   After modification, the number of port ranges in all configured advanced ACLs can exceed 32, depending on available ACL resources.

Operation changes in R1808P25

None

Operation changes in R1808P23

None

Operation changes in R1808P22

Changed the maximum number of SubIP addresses from 49 to 400.

Operation changes in R1808P21

None

Operation changes in R1808P17

None

Operation changes in R1808P16

None

Operation changes in R1808P15

Changed the maximum number of secondary VLANs for Isolate-user-VLAN from 192 to 1000.

Operation changes in R1808P13

None
Operation changes in R1808P11

None

Operation changes in R1808P08

1. Static multicast MAC address
   From this version, multicast MAC addresses starting with 01005e can be configured.

2. Loop detection log
   VLAN ID information is added into the log information that is generated when a loop occurs on a port enabled with loop detection.

Operation changes in R1808P06

1. Multi-port ARP
   Before modification, the packets matching a short static multi-port ARP entry cannot be forwarded.
   After modification, a short static multi-port ARP entry can be used to forward the matching packets after an ARP reply is received for that short static multi-port ARP entry.

2. Auto-negotiation
   Before modification, auto-negotiation cannot negotiate flow control capability.
   After modification, a port that is enabled with auto-negotiation and flow control negotiates flow control capability with the peer port during auto-negotiation. Note that: If you enable flow control on an Up port that has been enabled with auto-negotiation, the port goes down and up.

Operation changes in R1808P02

1. Changed the IRF connection mistake handling method.
   IRF-port 1 on one device must be connected to IRF-port 2 on another device. The system blocks incorrectly connected IRF ports and alerts the users to the mistake by settings the port LEDs in amber flashing state.

2. Looped-port status processing mechanism
   Before modification: If a port's loopback protection action is shutdown, the system automatically shuts down the port when it detects a loop on the port, leaving the port in Loop down state at the physical layer. After the loop is removed, you must execute the undo shutdown command on the port to restore the port's forwarding capability.
   After modification: The system automatically starts a port status detection timer when a port is shut down because of a loopback. After the timer expires, the system automatically brings up the port to restore its forwarding capability. The timer is 30 seconds by default. You can use the shutdown-interval time command to change the timer.

Operation changes in R1807P02

1. Changed RPS status output information for 5800-48G (1 slot)/5800-48G TAA (1 slot)/5800-24G/5800-24G TAA.
   In earlier versions, when the RPS does not provide power, the RPS status is displayed as “Fault”. In this version, the RPS status is displayed as “Standby”.

22
2. Changed the maximum number of outgoing interfaces in a static multicast MAC entry from 16 to 32.

**Operation changes in F1807P01**

3. Changed the value range for the offline detect timer.
   The value range changed from 60~65535 to 60~2147483647.
4. Disable telnet server service by default.
   In earlier versions, telnet server is enabled by default. In this version, telnet server is disabled by default.
   To enable telnet server, use the “telnet server enable” command.

**Operation changes in F1805P02**

1. Disable all the TCP/UDP port by default (For example: TCP ports including 23/7547, UDP ports including 68/1812/3318/3799).

**Operation changes in F1805P01**

1. Disable NDP, NTDP, Cluster and Winet protocols by default.
   The cluster management feature provides a simple method to manage multiple units using a single IP address, however it does use some protocols that are not considered totally secure. In this release, the cluster management protocols, including NDP, NTDP, and Cluster, are disabled by default to avoid any possible security risks.
   If cluster management is required it is necessary to re-enable the required protocols with the following commands: ndp enable, ntdp enable, and cluster enable. In addition, HPE recommends that a separate management VLAN for the cluster should be established. Only the access ports that are used to link the cluster members should belong to this VLAN so the inter-switch protocol will not be accessible to insecure devices, including PCs and other network devices.
   The Winet feature is removed in this release as it is not considered totally secure. The Winet functionality is available through other management methods.
2. Disable HTTP service by default.
   In earlier versions, HTTP is enabled by default. In this version, HTTP is disabled by default.
   To enable HTTP, use the “ip http enable” command.
3. Backup the configuration file for old version software.
   If a save operation is performed on a switch where a software version of F1805P01 or later is running and the version number in the current startup configuration file is lower than F1803L01, 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.
4. Operation change for whether a port leaves the critical VLAN after the silent timer expires:
   After a port is assigned to the critical VLAN, the RADIUS server state changes to "blocked", and the silent timer of the RADIUS server starts (this timer is configurable and defaults to 5 minutes).
   In earlier versions:
   (1) If the port uses 802.1X authentication, it leaves the critical VLAN when the silent timer expires. If the port is configured with the dot1x critical recovery-action command, it’s leaving triggers new 802.1X authentication.
(2) If the port uses MAC authentication, it leaves the critical VLAN when the silent timer expires.
In this version:

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

5. Change the maximum number of online users for RADIUS.
In earlier versions, the maximum number of online users for RADIUS is 4096; in this version the number is 6000.

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

Operation changes in F1803L03

1. Changed the maximum number of GRE, IPv4-IPv4, or IPv6-IPv4 tunnels from 128 to 256.
2. Changed the default state for TCP port 179 and port 639 to close.
3. Changed the delay time for MAC authentication from 30 seconds to 0 seconds when both 802.1X authentication and MAC authentication are enabled. You can modify the delay time at the CLI.
4. This release returns a reason for an 802.1X authentication failure to iNode, which is not available in earlier releases F1305P01.
5. Changed the value range for the irf link-delay from 20-2000 ms to 0-30000 ms. The default value is 4 seconds. To minimize the IRF link switchover and master/subordinate switchover delay or guarantee BFD or GR performance, HPE recommends setting the IRF link down report delay to 0.

Operation changes in F1803L01

None

Operation changes in F1305P01

1. DHCP snooping table changed
Modify DHCP snooping table from 8K to 12K.
2. Voice vlan oui mac address specification changed
Modify "voice vlan oui mac address" specification to 128
3. Passing packets deal with method changed.
Modify passing ARP packets solved method from limited speed to non-limited speed.
4. The command that applies an IPsec policy to the OSPFv3 area changed.
In this version, the command changed from ipsec-policy to enable ipsec-policy.
5. Hardware support of IPv6 routes with mask longer than 64bits
In previous versions: IPv6 routes with mask longer than 64bits exists only in software.
In this version: maximum of 128 routes with mask longer than 64bits can be issued into hardware.
6. Synchronizing Voice VLAN mac-addresses automatically within all IRF members.
7. Upgrading software for the IRF fabric by iMC
   In this version, distributed file system is supported. Software upgrading of IRF fabric through iMC is supported.

Operation changes in R1211P04
   None

Operation changes in R1211P02
   None

Operation changes in R1211
   First release

Restrictions and cautions
   1. A5820X works at IPS mirror mode. If the IPS applies “any” rule, the PC connected to the device cannot communicate to its gateway.
   2. IRF connection restrictions:
      o One IRF port can have only one peer port. All physical ports of an IRF port must be connected to the physical ports of the same remote IRF port.
      o If there is a connection mistake between a newly-installed member device and a stack, you must power off the newly-installed member device, reconnect the physical ports, and then power on the newly-installed device.

Open problems and workarounds

LSD50925
   • Symptom: The MTU displayed the `display interface Tunnel` command is 1460, which is different from the actual value.
   • Condition: This symptom exists in the output of the `display interface Tunnel` command.
   • Workaround: None.

LSD60159
   • Symptom: IMC fails to display a hybrid port.
   • Condition: This symptom might occur if you configure the hybrid port to remove the VLAN tag of traffic from VLANs other than VLAN 1.
   • Workaround: None.

LSD67705
   • Symptom: If a unit is downgraded to earlier code, it may no longer be possible to login and manage the device.
   • Condition: In this version of code, the password encryption within configuration files has been enhanced and cannot be interpreted by earlier revisions of the agent code.
   • Workaround:
Before upgrading to the new code, it is necessary to ensure password control is disabled. Execute the "undo password-control enable" and then save this configuration file as a backup in case you need to downgrade the software again. If it is later necessary to downgrade to earlier software, force the switch to use this backup configuration file by executing a "startup saved-configuration (filename)" command before rebooting to the old code. Then, after the code has been downgraded, the device can be logged in from the console or by Telnet, but not SSH. The SSH authentication details will need to be reset.

If no backup configuration has been saved but it is still possible to access the device management via some method while running the old code (e.g. Console, Telnet or SSH), then you can redefine all the device management passwords as required.

If after a downgrade it is impossible to login to the device via any method, then there are two ways to recover the switch:

- From the BOOT menu, set the new code to run again and reboot the device. Disable Telnet authentication:
  
  User-interface vty 0 4
  Authentication mode none

  Then save the configuration and downgrade the code again, login via Telnet and reset all the passwords as required.

- From the BOOT menu. On boot-up, use Ctrl+B to enter the Boot menu and then force the unit to use the factory default configuration (by bypassing the user configuration). The unit will then need to be fully reconfigured.

List of resolved problems

Resolved Problems in R1810P16

Symptom: After IRF reboot, the configuration of DHCP Snooping trust ports in VLAN lost the part of the ports on IRF slave switch.
Condition: Configure DHCP Snooping trust ports in IRF based VLAN, and the trust ports include the ports on IRF slave switch. Save configuration and reboot IRF.
Workaround: Avoid configuring DHCP Snooping trust ports based VLAN include the ports on IRF slave switch.

Symptom: The LSR labels of the peer end are exhausted because routes flap.
Condition: This symptom occurs if the LSR receives Withdraw messages and then receives Mapping messages with the same prefix but different labels.

Symptom: The device is rebooted unexpectedly.
Condition: This symptom occurs if the device receives the specific TCP SYN request packets.

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.

Symptom: The device discards packets with a checksum of 01 00.
Condition: This symptom might occur if the checksum of incoming packets is 01 00.
201712190289
- Symptom: CVE-2017-12190
- Condition: Local attacker can exploit these issues to obtain sensitive information that may lead to further attacks.

201712230093
- 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 R1810P13

201705040044
- Symptom: CVE-2017-6458
- Condition: NTP is prone to a buffer-overflow vulnerability because it fails to properly bounds-check user-supplied data before copying it into an insufficiently sized buffer.

201705040090
- Symptom: CVE-2014-9297
- Condition: An attacker can exploit this issue to obtain sensitive information. When an NTP client decrypted a secret received from an NTP server, it could cause that client to crash.

201705040090
- Symptom: CVE-2014-9298
- Condition: An attacker could bypass source IP restrictions and send malicious control and configuration packets.

201706230694
- 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.

201706230694
- Symptom: CVE-2010-4252
- Condition: A successful exploit may allow attackers to authenticate without the shared secret, aiding in further attacks.

201706230694
- 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.

201706230694
- 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.
201708150258
- **Symptom:** The ACL used by the inbound or outbound packet filter on an interface cannot be removed by executing the **undo packet-filter** command.
- **Condition:** The switch runs R1810P12 software, and configures packet-filter inbound or outbound.

201708020036
- **Symptom:** There are some member ports unselected in the aggregation port.
- **Condition:** The member ports of aggregations UP/DOWN frequently.

### Resolved Problems in R1810P12

201703110146
- **Symptom:** The switch reboot abnormally.
- **Condition:** This symptom occurs if adding, deleting or displaying the rules that included by packet-filter.

201612050641
- **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.

201612050641
- **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.

### Resolved Problems in R1810P11

201612230176
- **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.

### Resolved Problems in R1810P10

201610290061
- **Symptom:** MPLS might fail to forward traffic.
- **Condition:** This symptom occurs if routes flap in the MPLS network.

201608050504
- **Symptom:** For a network segment route, the local device mistakenly sends an LSP label to the peer end. However, the local device does not generate an LFIB entry for the directly-connected network segment. As a result, forwarding fails.
• Condition: This symptom occurs if the following conditions exist in an MPLS network:
  o The device learns a directly-connected network segment route with an outgoing label that is not activated.
  o The directly-connected network segment route is refreshed or any LDP neighbor comes up.

201606300465
• Symptom: BGP neighborship cannot be established after an IRF master/subordinate switchover.
• Condition: This symptom occurs if an IRF master/subordinate switchover occurs.

201605190545
• Symptom: The device reboots unexpectedly.
• Condition: This symptom occurs if the transceiver module diagnosis information is read after a TX_fault alarm occurs to a transceiver module.

201609010376
• 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.

201609010394
• 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.

201609210329
• 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.

Resolved Problems in R1810P07

201608110131
• Symptom: After a reboot, port mirroring configuration on a Layer 2 aggregation group member port can mirror only the outbound packets.
• Condition: This symptom might occur if the following operations are performed:
  o Configure a local mirroring group to mirror both the inbound and outbound packets of a Layer 2 aggregation group member port.
  o Save the running configuration and reboot the switch.

201609020255
• Symptom: The switch reboots unexpectedly.
• Condition: There is no grounding in the switch or a big environmental interruption.

201607050186
• 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.

201605170559
- 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.

201608200078
- 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.

201605090521
- 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.

201605090520
- 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.

Resolved Problems in R1810P06

201607080169
- Symptom: An IRF fabric uses the ring topology. After a subordinate switch directly connected to the master switch is rebooted, the state of the IRF ports on the master and subordinate switches becomes timeout.
- Condition: This symptom might occur if an IRF fabric uses the ring topology, and a subordinate switch directly connected to the master switch is rebooted.

201604050047
- Symptom: The packets with all zero source MAC address can't be discarded by the device.
- Condition: This symptom occurs if a QoS policy that matches any packets is applied.

Resolved Problems in R1810P03

201512290214
- 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.

201511270049
- Symptom: The PVST packets are not dropped by the switch.
- Condition: The command 'bupd-drop any' is configured in the switch.
Resolved Problems in R1810P01

201512280041
- 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 R1810

201509300442
- Symptom: A VLAN interface still filters all packets after the `packet-filter filter route` command is used to modify the applicable scope of packet filtering.
- Condition: This symptom occurs if an IPv6 ACL has been applied to the VLAN interface to filter IPv6 packets.

201510140301
- Symptom: The switch acting as a PE does not forward an incoming route update with new community attributes to the connected CE.
- Condition: This symptom occurs if the PE is in an IPv6 MPLS L3VPN.

201510310164
- Symptom: The portal authentication page cannot be displayed on a portal client.
- Condition: This symptom occurs if the portal client uses a browser running TLS1.2 for authentication.

201511090108
- Symptom: An aggregate interface on an IRF fabric goes down and comes up repeatedly.
- Condition: This symptom occurs if the aggregate interface is bound to a VPLS VSI.

Resolved Problems in R1809P11

201507270256
- Symptom: After a DHCP client sends a DHCP request for keeping its original IP address, the DHCP client can’t receive the NAK packet from the DHCP server.
- Condition: This symptom occurs if the following conditions exist:
  - The switch acts as a DHCP relay agent, and the DHCP client has been assigned an IP address.
  - The DHCP client sends a DHCP request for keeping its original IP address in a different VLAN.

201508210239
- Symptom: Exceptions occur during the reboot of a member device on an IRF fabric.
- Condition: This symptom might occur if the reboot of the member device is performed after you configure link aggregation on the IRF fabric and save the running configuration.

201507200129
- 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.

201507200129
• 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.

201507200129
• 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.

201506290049
• Symptom: On the 5800-48G-PoE+/5800-48G-PoE+ TAA or 5820AF-24XG switch, the SFP+ ports on the LSW1SP2P0 expansion interface card go down if an OAP card is also installed on the switch.
• Condition: This symptom might occur if the following conditions exist:
  o The LSW1SP2P0 expansion interface card is installed in subslot 1, and the LSWM1IPS10, LSWM1FW10, or LSWM1WCM10 OAP card is installed in subslot 3.
  o Both cards have been operating for a period of time.

Resolved Problems in R1809P10

201507140033
• Symptom: The round trip time is long in the result of UDP jitter operations.
• Condition: This symptom might occur if the switch operates as the NQA server to perform UDP jitter operations.

201506180310
• Symptom: The DHCP server on the switch does not preferentially use the static address pool when processing DHCP-INFORM packets.
• Condition: This symptom might occur if the following conditions exist:
  o The DHCP-INFORM packets are sent by a DHCP client bound to an IP address in the static address pool.
  o The address range of a dynamic address pool covers the static address pool.

201507140228
• Symptom: The switch does not update or add ARP entries when it receives ARP replies that carry a subnet broadcast address in the target IP address field.
• Condition: This symptom might occur if the switch receives ARP replies that carry a subnet broadcast address in the target IP address field.
Resolved Problems in R1809P09

201505150228
- Symptom: The CPU usage of the master device in an IRF fabric remains high when a GRE tunnel established by using aggregate interfaces on the IRF fabric forwards packets.
- Condition: This symptom occurs if the member ports that were first brought up are not on the master device. In this case, tunneled packets are forwarded to the master device for decapsulation.

201504200155
- 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.

201504200155
- 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.

201505190409
- Symptom: The DHCP server does not respond with a DHCP-ACK message.
- Condition: This symptom occurs when the switch acts as a DHCP server and receives a DHCP-request from a client for re-requesting an address.

201504090196
- Symptom: CVE-2015-0209
- Condition: A malformed EC private key file consumed via the d2i_ECPrivateKey function could cause a use after free condition. This could lead to a DoS attack or memory corruption for applications that receive EC private keys from untrusted sources.

201504090196
- Symptom: CVE-2015-0287
- Condition: Reusing a structure in ASN.1 parsing may allow an attacker to cause memory corruption via an invalid write. Applications that parse structures containing CHOICE or ANY DEFINED BY components may be affected.

201504090196
- Symptom: CVE-2015-0288
- Condition: The function X509_to_X509_REQ will crash with a NULL pointer dereference if the certificate key is invalid.

201504090196
- Symptom: CVE-2015-0289
- Condition: The PKCS#7 parsing code does not handle missing outer ContentInfo correctly. An attacker can craft malformed ASN.1-encoded PKCS#7 blobs with missing content and trigger a NULL pointer dereference on parsing.

201504090196
- Symptom: CVE-2015-0292
- Condition: A vulnerability existed in previous versions of OpenSSL related to the processing of base64 encoded data.
Symptom: The mirrored packets are counted as error packets on the tunnel interface of the destination device.
Condition: This symptom occurs if Layer 3 remote port mirroring is configured.

Resolved Problems in R1809P06

Symptom: The CPU usage of the switch is continuously high.
Condition: This symptom occurs when the following conditions exist:
  o The switch runs DHCPv6 relay agent and DHCPv6 snooping.
  o The ND entry resources are insufficient because a large number of users log in.

Symptom: The cwmp enable command in the configuration file fails to be executed.
Condition: This symptom occurs after the following operations are performed:
  a. The switch starts with the automatic configuration feature.
  b. The switch automatically downloads a configuration file that contains the cwmp enable command from the TFTP server.

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

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

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

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

Symptom: CVE-2014-8275
Condition: By modifying the contents of the signature algorithm or the encoding of the signature, it is possible to change the certificate's fingerprint. Only custom applications that rely on the uniqueness of the fingerprint may be affected.
201503030229

- 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 R1809P05

201502020262

- Symptom: The switch drops packets when it replaces one VPNv4 route with another VPNv4 route or with an IPv4 route for forwarding the packets.
- Condition: None.

201502270198

- Symptom: iMC cannot connect to a managed switch and generates an ICMP no response alarm for the switch.
- Condition: This symptom occurs if the switch suffers from an SNMP attack that sets the ipDefaultTTL node to 1.

201502040448

- Symptom: The **arp filter binding ip-address mac-address** command configuration cannot be deleted.
- Condition: This symptom occurs if the **arp filter binding ip-address mac-address** command is configured in interface view.

201501260451

- Symptom: In a NetStream flow, the timestamp of the last packet is earlier than that of the first packet.
- Condition: This symptom occurs when the following conditions exist:
  a. The firstPackTime is in the first counting cycle.
  b. The lastPackTime is in the second counting cycle.
  c. The curRegTime and lastPackTime are in the same counting cycle.
  d. curRegTime > firstPackTime > lastPackTime.

201502060374

- Symptom: The prompt message always shows that rule 0 in the ACL is an unsupported rule when the **packet-filter { acl-number | name acl-name } { inbound | outbound }** command fails to be executed.
- Condition: This symptom occurs when the **packet-filter { acl-number | name acl-name } { inbound | outbound }** command fails to be executed on a Layer 3 Ethernet interface.

201502030614

- Symptom: An MAC address entry ages slower than expected.
- Condition: This symptom occurs if the ARP entry for the MAC address is updated because the MAC address moves between ports.

201502090218

- Symptom: The switch reboots unexpectedly after an applied QoS policy is removed.
• Condition: This symptom occurs when the following conditions exist:
  a. The QoS policy is applied to the control plane.
  b. The class name and behavior name are both the same as the policy name.

201503050191
• Symptom: An interface connecting to an IPS card learns the MAC address of the IPS in a VLAN
to which the interface does not belong.
• Condition: This symptom occurs if the IPS detects attack packets in the VLAN and sends
disconnection packets.

201503050192
• Symptom: The 5820X-24XG-SFP+/5820X-24XG-SFP+ TAA or 5820X-14XG-SFP+
/5820X-14XG-SFP+ TAA switch does not create ARP entries if it receives ARP packets from
the second lowest-numbered 10-GE port on the panel. The same symptom occurs on the
5820AF-24XG switch if the switch receives ARP packets from the lowest-numbered 10-GE port
on the panel.
• Condition: This symptom might occur if the switch runs release R1809P03.

Resolved Problems in R1809P03

201412230067
• Symptom: The system displays a message showing that "Warning: CBS is smaller than (100/16)
  CIR and this maybe effect network traffic burst."
• Condition: This symptom occurs when you set the CIR to a value greater than 2560000 and
  then manually set the CBS in CAR of a QoS policy.

201412310370
• Symptom: CVE-2014-9295
• Condition: Stack-based buffer overflows in ntpd in NTP before 4.2.8 allow remote attackers to
  execute arbitrary code via a crafted packet.

201501120235
• 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).

201501080317
• Symptom: When you display information about the transceiver module of an interface, the
  output shows that the connector type is UNKNOWN.
• Condition: This symptom occurs when the interface has a Finisar 1000_BASE_T_AN_SFP
  transceiver module installed.

201501260138
• Symptom: BFD packets are sent out queue 2, and the 802.1p priority in the VLAN tags of the
  BFD packets is 0.
• Condition: This symptom occurs when the switch runs BFD.
Resolved Problems in R1809P02

201410130569
- Symptom: UDP packets cannot be forwarded.
- Condition: This symptom occurs when the *udp-helper server* command is configured with a broadcast subnet IP address.

201411280203
- Symptom: Some routes might be lost after route flapping.
- Condition: This symptom occurs when the switch runs the IS-IS protocol and IS-IS routes keep flapping.

201412080137
- Symptom: ACL rules fail to be applied to some IRF member switches.
- Condition: This symptom occurs when the following procedure is performed on an IRF fabric:
  a. Apply an ACL through policy-based routing (PBR).
  b. Dynamically delete rules of the ACL.
  c. Configure the rules again.

201412030431
- Symptom: Multicast packets cannot be forwarded to Layer 3 aggregate interfaces.
- Condition: This symptom occurs when the switch runs IPv4 multicast and multicast receivers are attached to a Layer 3 aggregate interface.

201410170159
- Symptom: Packets are lost in some VPN instances.
- Condition: Both the public routes and the private routes flapped.

Resolved Problems in R1809P01

201408060506
- Symptom: Static routes might fail.
- Condition: This symptom occurs when a master/subordinate switchover is performed in an IRF fabric.

201408060212
- Symptom: The BGP peer relationship between the switch and its peer is automatically removed after a certain period of time.
- Condition: This symptom occurs when the link between the switch and its peer flaps and the flapping causes TCP packet retransmission over the TCP connection established between the switch and its peer.

201408060171
- Symptom: The routing information is not synchronized among devices in an OSPF network. As a result, traffic forwarding is affected.
- Condition: This symptom occurs when the following procedure is performed:
  a. More than 100 areas are configured in a single OSPF process on a device.
  b. Route flapping occurs in the OSPF network.
• Symptom: MAD IP addresses conflict in BFD MAD.
  Condition: This symptom occurs when the switch receives STP TC BPDUs.

• Symptom: The message "The default route has been changed or deleted, protocol is OSPF" is frequently displayed in the log.
  Condition: This symptom occurs when the optimal default route does not change and the non-optimal default route is deleted.

• Symptom: A DHCP client cannot obtain an IP address.
  Condition: This symptom occurs when the DHCP server and the DHCP client are in different VPNs on the same switch.

• Symptom: When you paste commands in interface range view, these commands might not be completely issued.
  Condition: This symptom occurs when you paste commands in interface range view.

• 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:
    o The attribute 65 (Tunnel-Medium-Type) is set to 802.
    o The attribute 64 (Tunnel-Type) is set to VLAN.
    o No VLAN ID is configured in the attribute 81 (Tunnel-Private-Group-ID).

• Symptom: It takes more than one second to switch traffic to links of other equal-cost routes.
  Condition: This symptom occurs if the link to the next hop of an equal-cost route is disconnected when the switch runs BGP and multiple equal-cost routes to the same destination exist.

• Symptom: Software upgrade frequently fails on the switch.
  Condition: This symptom occurs when CWMP is used to upgrade software for the switch.

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

• 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.

• 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.

201409020110
• Symptom: CVE-2008-5161
• Condition: 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.

201307240532
• Symptom: Known unicast traffic is broadcast in VLANs.
• Condition: This symptom occurs when an aggregation group without member ports is created and then deleted on the switch.

201408060574
• Symptom: Some 10-GE interfaces might fail to go up.
• Condition: This symptom occurs when the state of multiple 10-GE interfaces on an 5800AF-48G switch flaps the same time.

Resolved Problems in R1808P27

201407040460
• Symptom: A headquarter switch might fail to establish IPsec connections with some branch switches.
• Condition: This symptom might be seen if a headquarter switch establishes IPsec connections with multiple branch switches at the same time.

201406230240
• Symptom: A port does not quit the guest VLAN after a user in the guest VLAN passes 802.1X authentication on the port.
• Condition: This symptom can be seen after a user in the guest VLAN (different from the pvid of the port) passes 802.1X authentication on a port.

Resolved Problems in R1808P25

201404040266
• Symptom: The CPU usage is 100% if endless recursive routing occurs.
• Condition: This symptom can be seen if configured routes form endless recursive routing.

201404040239
• Symptom: The DHCP client takes a long time for address acquisition from the DHCP server on the switch.
• Condition: This symptom can be seen if the VLAN interface enabled with the DHCP server has an IP address that is not on the same network as the Request IP address from the client. The DHCP server does not respond with a NAK packet.

201404040421
• Symptom: SSH and Telnet functions are not available after operations are performed on SecureCRT.
- Condition: This symptom can be seen if the following operations are performed:
  a. Generate a public key on SecureCRT and upload it to the switch.
  b. Create user 1 and user 2 on the switch.
  c. Select one-time key authentication for user 1. After user 1 passes authentication, use user 1 again for authentication. Then use user 2 for authentication.

**201405080425**
- Symptom: A DHCP client fails to obtain an IP address through the DHCP relay on the switch.
- Condition: This symptom can be seen if the switch fails to send a DHCP packet to the DHCP client. After that, the switch does not clear relevant VLAN attributes, and sends a DHCP packet (which should be sent to the DHCP server) to a wrong VLAN.

**201405080409**
- Symptom: After a UPE is disconnected and then connected to an SPE, the SPE does not advertise optimal VPNv4 routes learned from the UPE to other PEs.
- Condition: This symptom can be seen when the following conditions exist:
  - In a HoVPN network, an SPE has leaned the same VPNv4 prefixes from a UPE and other PEs, and it prefers the prefixes from the UPE based on local preference.
  - The UPE is disconnected and then connected to the SPE to re-establish a BGP session.

**201405270042**
- Symptom: On an IRF fabric, users passing portal authentication on an aggregate interface are disconnected and must be re-authenticated to come online.
- Condition: This symptom can be seen if the following conditions exist:
  - The aggregate interface includes members ports on both the master and subordinate switches.
  - The member ports on the master quits the aggregate interface.

**201405200026**
- 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.

**201405240023**
- Symptom: The switch discards an incoming ICMP echo request not destined to it and responds with an ICMP echo reply.
- Condition: This symptom can be seen if the ICMP echo request includes a Router Alert Option.

**201407020475**
- Symptom: A 10G SFP+ or 1G SFP port inserted with a 1G module cannot come up. The output from the `display transceiver interface [interface-type interface-number ]` command shows “Error: Reading information from the transceiver failed.”.
- Condition: This symptom can be seen if a 10G SFP+ or 1G SFP port is inserted with a 1G module.

**201406100313**
- Symptom: CVE-2014-0224.
- Condition: When Open SSL Server or Client is used.
Resolved Problems in R1808P23

201404170383
• Symptom: An intra-area or inter-area OSPF route is added with a route tag.
• Condition: This symptom occurs if an OSPF route calculated from a Type 5 LSA, which has a route tag, has the same destination address, mask, and egress interface as the intra-area or inter-area route.

201403250550
• Symptom: The dot1x handshake and dot1x multicast-trigger features fail to be disabled.
• Condition: This symptom can be seen after you execute the undo dot1x handshake and undo dot1x multicast-trigger commands, save the configuration, and reboot the switch.

201402200059
• Symptom: The CPE switch might fail to access the ACS, resulting in memory overflows. The switch stops accepting any commands and sometimes prints stack reboot information.
• Condition: This symptom might occur when a password is configured for the CPE to access the ACS.

Resolved Problems in R1808P22

201402270210
• Symptom: A user fails to log in to the switch.
• Condition: This symptom occurs when the following conditions exist:
  o The user uses RADIUS authentication.
  o The RADIUS server assigns multiple login-service attributes.

201403120042
• Symptom: The speed of downloading files through SFTP is slow.
• Condition: This symptom can be seen when you use SFTP to download files.

201402240199
• Symptom: Traffic interruption occurs between VPLS sites.
• Condition: This symptom can be seen when the following conditions exist:
  o The maximum number of MAC entries is configured for VPLS instance.
  o Flapping occurs to the port on the VPLS link.

201312310475
• Symptom: The PIM BFD session between the PE and CE on the multicast receiver side continually flaps, and advertising BFD packets fails.
• Condition: This symptom occurs if the PE on the multicast source side and the PE on the multicast receiver side are both rebooted at the same time.

201402240237
• Symptom: A DHCPv6 client fails to acquire an IPv6 address from the DHCPv6 server.
• Condition: This symptom occurs when the following conditions exist:
  o The switch resides between the client and the server to relay packets.
  o The multicast ipv6 routing-enable command is configured on the switch.
Resolved Problems in R1808P21

201401090295
- Symptom: After an ISSU on an IRF fabric, member ports in a multi-chassis aggregation group get lost.
- Condition: This symptom occurs after an ISSU on an IRF fabric.

201402130358
- Symptom: The `display qos queue-statistics` command shows incorrect count information for dropped packets on an interface.
- Condition: This symptom can be seen on an interface that dropped packets due to congestion.

Resolved Problems in R1808P17

201303050193
- Symptom: A user fails to change the user privilege level by using the `supper` command although the entered password is correct.
- Condition: This symptom occurs if the following procedure is performed:
  a. After passing AAA authentication, the user tries to change the user privilege level five times, but all attempts are failed because of incorrect passwords.
  b. After that, the user enters the correct password within 15 minutes.

201311070151
- Symptom: The state of OSPF neighbors on IPsec VTI interfaces might change from Full to Down, and the neighbors can be reestablished only after IKE renegotiation.
- Condition: This symptom can be seen if the following conditions exist:
  o The IPsec VTI interfaces have the same source IP address but different destination IP addresses.
  o The IPsec VTI interfaces act as IKE responders.
  o The IPsec VTI interfaces are enabled with OSPF.

201311190381
- Symptom: The CPU usage is very high when the DHCP server is enabled.
- Condition: This symptom occurs if the DHCP server assigns an expired IP address to a client and a large number of expired IP addresses exist.

201310310003
- Symptom: The DHCP relay agent fails to assign an IP address to a client.
- Condition: This symptom occurs if the DHCP relay agent receives an offer packet where the yiaddr is 0.0.0.0, and the Bflag is 0.

201312060179
- Symptom: Traffic interruption occurs during an IRF master/subordinate switchover.
- Condition: This symptom occurs if the following conditions exist:
  o ISIS is enabled on both the local and remote ends.
  o BFD is enabled on one end but is not enabled on the other end.

201312090076
• Condition: This symptom occurs when the following procedure is performed:
  a. The DHCP server enabled on the IRF fabric assigns an IP address from an extended address pool to a client.
  b. After an IRF master/subordinate switchover, the client releases the IP address. Then the IP address exists both in the Free IP and Conflicted IP lists.
  c. The DHCP server reallocates the IP address.

201311070447
• Symptom: Build Run displays that the content of ACL 5000 is too long.
• Condition: This symptom can be seen if ACL 5000 is user customized.

201311180232
• Symptom: OSPFv3 neighbors on a broadcast network might fail to reach Full state.
• Condition: This symptom might occur if more than five OSPFv3 neighbors exist on a broadcast network and they fail to elect a DR.

201312030363
• Symptom: BFD flapping occurs.
• Condition: This symptom can be seen when the following conditions exist:
  o The minimum intervals for sending and receiving single-hop BFD control packets are 100ms.
  o The BFD detection time multiplier is 3.
  o Large numbers of unknown IPv4 multicast packets are received.

201312170306
• Symptom: The SFP Plus interface on the front panel of A5800-48G-PoE+ might go down.
• Condition: This symptom might occur during the operation of A5800-48G-PoE+.

201312160087
• Symptom: The MAC addresses that a VPLS VSI learns cannot reach the configured upper limit.
• Condition: This symptom can be seen when a VPLS VSI is configured with an upper limit for MAC addresses to be learned.

201312050147
• Symptom: A walk on ifOutDiscards MIB returns a value of 0.
• Condition: This symptom can be seen during a walk on ifOutDiscards MIB.

201312230212
• Symptom: Switches in QinQ transparent transmission VLANs cannot establish OSPF neighbors.
• Condition: This symptom can be seen if switches are connected through ports configured with QinQ and transparent transmission VLANs.

201312170513
• Symptom: An interface bound to VPLS or VPWS cannot transparently transmit multicast protocol packets.
• Condition: This symptom can be seen when an interface is bound to VPLS or VPWS.
Resolved Problems in R1808P16

201311270239

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

Resolved Problems in R1808P15

201309160028

- Symptom: Some inter-AS traffic might fail to be forwarded in a domain where both L2VPN and L3VPN are running.
- Condition: This symptom might occur if the following conditions exist:
  - Both L2VPN and L3VPN are running in the domain.
  - All devices in the domain are rebooted.

201309170371

- Symptom: If some selected ports in a service loopback group are replaced with other ports, some multicast traffic cannot be forwarded through Switch-MDT.
- Condition: This symptom occurs if the following conditions exist:
  - Multicast VPN is enabled.
  - Multicast traffic has been switched from Share-MDT to Switch-MDT.
  - The number of selected ports in a service loopback group has reached the upper limit and some member ports are replaced with other ports.

201306060521

- Symptom: A port discards incoming ARP packets with two VLAN tags.
- Condition: This symptom occurs when the following conditions exist:
  - The port is a trunk or hybrid port and is enabled with QinQ.
  - The port is configured to permit VLANs where ARP detection or ARP snooping is enabled.

201309040090

- Symptom: The switch fails to create Share-MDT forwarding entries.
- Condition: This symptom occurs when the following conditions exist:
  - The switch is running multicast VPN.
  - The switch has created large numbers of MPLS TE tunnels.

201309160040

- Symptom: After the `reset bgp` command is executed on the ASBR in an inter-AS multicast VPN scenario, inter-AS PIM neighbors cannot be created.
- Condition: This symptom occurs after the `reset bgp` command is executed on the ASBR in an inter-AS multicast VPN scenario.

201309090133

- Symptom: After BGP receives two VPN routes that have the same attributes except for the RD and label, the system updates the BGP routing table but does not update the IP routing table.
- Condition: This symptom occurs after BGP receives two VPN routes that have the same attributes except for the RD and label.

201309090170
- Symptom: A memory exception occurs during a walk on OSPF LSDB MIB.
- Condition: This symptom occurs when a walk on OSPF LSDB MIB is performed.

Resolved Problems in R1808P13

201309020181
- Symptom: After a 10 G expansion interface card that is inserted with a 1 G fiber module has been removed and inserted multiple times, the 10G interface connected to the 1 G fiber module cannot go up.
- Condition: This symptom occurs after a 10 G fiber card that is inserted with a 1 G fiber module has been removed and inserted multiple times.

201306060521
- Symptom: The software discards multi-tagged ARP packets received from a QinQ-enabled interface.
- Condition: This symptom occurs when the following conditions exist:
  - The interface is a trunk or hybrid interface.
  - The interface permits a VLAN that is enabled with ARP detection or ARP snooping.

201305170423
- Symptom: OSPF fails to learn networks passing a separated subnet. For example, 192.168.1.1/24 and 192.168.1.2/24 in the same subnet reside in different locations.
- Condition: This symptom occurs if a network is separated.

201308300303
- Symptom: SNMP GET fails to get the value of a MIB variable if the following MIB variable is not supported.
- Condition: This symptom occurs if a MIB variable is not supported.

201308300172
- Symptom: After an SSH user passes authentication on a RADIUS server, the switch fails assign the user priority configured on the RADIUS server to the SSH user.
- Condition: This symptom occurs after an SSH user passes authentication on a RADIUS server.

Resolved problems in R1808P11

201308210368
- Symptom: The first interface of a 10 GE fiber interface subcard fails to go up or continually go up and down.
- Condition: This symptom occurs if the following conditions exist:
  - The `display device manuinfo slot <slot-number> subslot <subslot-number>` command is executed to display the electronic label information of the 10 GE fiber interface subcard.
  - The first interface of the subcard re-establishes the physical link two times.
**Symptom:** The switch unexpectedly reboots upon receiving SNMPv3 packets that are larger than the `globPDUSize` (defaults to 1500) and have a `contextName` field that is almost the `globPDUSize`.

**Condition:** This symptom occurs when the following conditions exist:
- The switch receives SNMPv3 packets that are larger than the `globPDUSize` (defaults to 1500) and have a `contextName` field that is almost the `globPDUSize`.
- SNMPv2, SNMPv3, SSH, DHCP, and OSPF attacks exist.

**Symptom:** A SmartOptics 10GBASE-ZR module inserted to an SFP+ interface is identified as 10GBASE-ER and the system prompts that the module is not supported.

**Condition:** This symptom can be seen if a SmartOptics 10GBASE-ZR module is inserted to an SFP+ interface.

**Symptom:** When a CRLSP used by an MPLS TE tunnel fails, the MPLS TE tunnel cannot establish a new CRLSP.

**Condition:** This symptom occurs when the following conditions exist:
- Two explicit paths are configured and the MPLS TE tunnel uses the higher-priority explicit path.
- A bypass tunnel is configured to protect the MPLS TE tunnel.
- The reoptimization frequency is set to a small value such as one second.

When the higher-priority explicit path fails, MPLS TE cannot establish a new CRLSP over the lower-priority explicit path because the reoptimization frequency is too short. After the reoptimization frequency is set to a larger value, MPLS TE still cannot establish a new CRLSP because the new value does not take effect.

**Symptom:** The switch unexpectedly reboots when a smart phone is connected to the USB interface of the switch.

**Condition:** This symptom occurs if a smart phone from specific vendors is connected to the USB interface of the switch.

**Symptom:** Multicast VPN fails to forward multicast packets.

**Condition:** This symptom occurs if the multicast packets is destined to a Share-Group address in which the second byte has a decimal value larger than 128, such as 239.129.1.1.

**Symptom:** System resources become insufficient when outbound QoS policies are applied to multiple interfaces.

**Condition:** This symptom occurs when the following conditions exist:
- The software is upgraded from R1211 to R1808P06.
- The `qos apply policy <policy-name> outbound` command is executed on multiple interfaces to match IPv4 header fields and Layer 2 frame header fields.

**Symptom:** Parity check errors might occur to the memory space for internal entries, and the affected internal entries become invalid, resulting in routing failures or device reboot.

**Condition:** This symptom might be seen when the following conditions exist:
The switch has run for a long time.
The ports on the switch are forwarding large amounts of traffic.

ZDD06122

- Symptom: On an IRF fabric, broadcast ARP packets received on a multi-chassis aggregate interface might be forwarded through other member ports of the aggregate interface.
- Condition: This symptom might occur if a member port in the multi-chassis aggregate interface goes up and down.

ZDD06109

- Symptom: When the switch receives large numbers of TC packets (for example, dozens of TC packets per second), the CPU usage is 100% for a long time.
- Condition: This symptom occurs when the following conditions exist:
  - PVST is enabled.
  - Lots of ARP entries exist.
  - The switch receives large numbers of TC packets (for example, dozens of TC packets per second).

ZDD06035

- Symptom: A user with a valid IP address fails to access the Web interface of the switch.
- Condition: This symptom occurs if `ip http acl` is configured and the referenced ACL is specified with a VPN instance.

LSD075268

- Symptom: When Internet Explorer 10 is used to access the Web interface of the switch, multiple functions cannot be configured.
- Condition: This symptom can be seen when Internet Explorer 10 is used to access the Web interface of the switch.

LSD074446

- Symptom: The master switch in a cluster unexpectedly reboots when the `cluster switch-to` command is executed.
- Condition: This symptom occurs when the `cluster switch-to` command is executed on the master switch in a cluster.

LSD075442

- 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.

LSD075619

- Symptom: An IRF member switch's internal interface that connects to an IPS card fails to forward packets.
- Condition: This symptom occurs when the following conditions exist:
  - The `port connection-mode extend` command is configured on the IRF member switch's internal interface.
  - The IRF member switch connects to another member switch through an aggregate interface, and some member ports in the aggregate interface are deleted.
Resolved problems in R1808P08

LSD075006
- Symptom: The switch fails to start up if the NAND flash's area that stores runtime information is corrupted.
- Condition: This symptom occurs if the NAND flash's area that stores runtime information is corrupted.

LSD074507
- Symptom: The switch fails to communicate with a device from another vendor through IPv6 VRRPv3.
- Condition: This symptom occurs because the IPv6 VRRPv3 packet format used by the switch contains a redundant authentication field, which does not comply with RFC 5798.

LSD074987
- Symptom: After an IRF master/subordinate switchover, OSPF fails to learn routes although OSPF neighbor relationships have been established.
- Condition: This symptom occurs if the following conditions exist before the master/subordinate switchover:
  - OSPF neighbor relationships are established on the subordinate switch.
  - The undo irf mac-address persistent command is configured on the IRF fabric.

LSD075013
- Symptom: When a VRRP backup device is rebooted, it becomes the VRRP master within a short time.
- Condition: This symptom occurs if the VRRP backup device's interface that is enabled with VRRP is a Layer 3 interface.

ZDD06135
- Symptom: A switch connected to a device from another vendor unexpectedly reboots during IKE negotiation.
- Condition: This symptom occurs if the IKE proposal adopts RSA signature authentication and a domain is referenced for the IKE peer.

LSD075095/LSD075382
- Symptom: An IRF fabric continually reboots if a member switch sends incorrect IRF packets because of a packet buffer hardware fault.
- Condition: This symptom occurs if a member switch sends incorrect IRF packets because of a packet buffer hardware fault.

LSD074644
- Symptom: A switch unexpectedly reboots when a user logs in to the Web interface.
- Condition: This symptom occurs if the character string specified in the snmp-agent sys-info location or snmp-agent sys-info contact command exceeds 200 characters.
Resolved problems in R1808P06

LSD074198

• Symptom: As shown in the following figure, if the import-route static and undo import-route static commands are repeatedly executed on Dev C where multiple static routes exist, Dev B might reboot.

• Condition: This symptom might occur if the import-route static and undo import-route static commands are repeatedly executed on Dev C where multiple static routes exist.

![Diagram](image)

LSD074638

• Symptom: A configuration file larger than 17K bytes fails to be uploaded to IMC BIMS when the authentication method is username and password.

• Condition: This symptom might occur when a configuration file larger than 17K bytes is uploaded to IMC BIMS and the authentication method is username and password.

LSD074434/LSD074711

• Symptom: When an IRF fabric that has a dynamic link aggregation group with multiple member ports splits, LACP MAD cannot quickly detect the IRF split, resulting in 10-second packet loss.

• Condition: This symptom might occur during an IRF split because a large number of LACP packets are sent when the IRF fabric splits, which disables LACP MAD from quickly detecting the failure.

LSD074354

• Symptom: The output from the display ipv6 dhcp snooping user-binding dynamic command does not show DHCP snooping entries for users that have obtained IP addresses in a VLAN if DHCP relay is enabled on the VLAN interface and DHCP snooping is enabled on the VLAN.

• Condition: This symptom occurs in a VLAN if DHCP relay is enabled on the VLAN interface and DHCP snooping is enabled on the VLAN.

LSD073944

• Symptom: After the ip https enable command and then the undo ip https enable command are executed, TCP port 443 is not shut down.

• Condition: This symptom occurs after the ip https enable command and then the undo ip https enable command are executed.

LSD073683

• Symptom: No prompt information is given upon failure of executing the ip https enable command.

• Condition: This symptom occurs if you first execute the portal local-server https server-policy sslsvr command and then execute the ip https enable command. The ip https enable command fails to be executed because the server policy needed by HTTP has been used by portal.

LSD074749

• Symptom: In the output from the display current-configuration command, the snmp-agent sys-info contact and location fields only have four characters.

• Condition: This symptom occurs if the contact and location information is configured in the Web interface.
Resolved problems in R1808P02

LSD074224

- Symptom: The 3Com 3CNJ2000 device that is attached to the switch fails to supply power to PDs.
- Condition: This symptom might occur if the switch runs R1805P02 and the 3Com 3CNJ2000 PD device is attached to the switch as a PD.

LSD074325

- Symptom: After the software is upgraded from R1211P04 to Feature 1805P02, ping operations fail.
- Condition: This symptom occurs when the following conditions exist:
  - HPE 5800 is connected to a Cisco device, which does not use split horizon.
  - The Cisco device assigns labels for direct routes, and HPE 5800 assigns Swap attribute for the LSPs.

LSD074473

- Symptom: LDP packets not destined for the switch are delivered to the CPU. If large numbers of such LDP packets are delivered to the CPU, the CPU usage is high, affecting normal LDP sessions especially when link down/up events occur.
- Condition: This symptom occurs when the switch resides between two other devices and receives LDP packets destined for one of those two devices.

LSD074048

- Symptom: ARP reply messages with Trailer field error are blocked by some firewalls when VLAN-tagged ARP replies are sent out of the trunk port of the DUT.
- Condition: This symptom occurs when the VLAN-tagged ARP replies are sent out of the trunk port of the DUT. The following figure shows the network diagram.

ZDD05904

- Symptom: The configuration file cannot be uploaded to the ACS through CWMP.
Condition: This symptom occurs if CWMP uploads the configuration file by using the HTTP put or HTTPS put method, and the ACS requires file transfer authentication in addition to the authentication performed during CWMP connection setup.

NOTE:
If IMC is used as the ACS, you must also update IMC to the BIMS 5.2 (E0401) version to solve the problem.

LSD070383

Symptom: An SNMP walk on the dot3OamUniqueEventNotificationTx and dot3OamDuplicateEventNotificationTx nodes returns a value of 0.

Condition: This symptom might occur if you use MIB Browser or other network management tools to access the dot3OamUniqueEventNotificationTx and dot3OamDuplicateEventNotificationTx nodes.

LSD072339

Symptom: The STP status of the link is wrong on the MSTIs except CIST.

Condition: This symptom occurs when you perform the following operations:
- Connect the neighboring MSTP devices through an aggregate link that allows packets from multiple VLANs to pass through.
- Delete all VLANs that are mapped to MSTIs on the aggregate link, and configure the VLANs again.

ZDD05659

Symptom: MSDP peers cannot go up.

Condition: This symptom might be seen when route flapping frequently occurs on the network and CPUs of the MSDP peers are busy.

ZDD05804

Symptom: If the egress interface cost of the IS-IS route that is optimal among IS-IS routes destined for the same network is modified twice, route calculation error occurs, and the optimal route is not selected.

Condition: This symptom occurs if the egress interface cost of the IS-IS route that is optimal among IS-IS routes destined for the same network is modified twice.

ZDD05830

Symptom: If the switch receives Type-4 LSAs from multiple areas, it advertises the most recently received Type-4 LSA to other area, rather than the optimal one.

Condition: This symptom occurs if the switch receives Type-4 LSAs from multiple areas.

LSD073884

Symptom: The configuration of the esp encryption-algorithm aes-cbc-192 command is changed to the esp encryption-algorithm aes-cbc-128 command.

Condition: This symptom occurs when you perform the following operation:

In FIPS mode, execute the esp encryption-algorithm aes-cbc-192 command, and then the transform ah-esp command in IPsec transform set view. In the current-configuration, the esp encryption-algorithm aes-cbc-192 command is changed to the esp encryption-algorithm aes-cbc-192 aes-cbc-128 command.

Save the configuration and reboot the device.
LSD073943

- **Symptom:** In FIPS mode, if you execute the `authorization-attribute work-directory` command that includes an invalid parameter in local user view, the following messages that appear still include FTP information, although FTP is not supported in FIPS mode:
  - Warning: Wrong FTP path or nonexistent directory.
  - Warning: The directory for FTP must be an absolute path!

- **Condition:** This symptom can be seen if you execute the `authorization-attribute work-directory` command that includes an invalid parameter in local user view in FIPS mode.

LSD074084

- **Symptom:** Memory leaks occur when the `public-key local create dsa` command or the `public-key local create rsa` command is used in FIPS mode to generate key pairs.

- **Condition:** This symptom occurs when the `public-key local create dsa` command or the `public-key local create rsa` command is used in FIPS mode to generate key pairs.

LSD073993

- **Symptom:** When the log file is full, if you do not enter `y` at the prompt "Warning: All port will be shutdown when the logfile is full. Are you sure? [Y/N]:" that appears after you execute the `info-center log file overwrite-protection all-port-powerdown` command, all service ports are shut down.

- **Condition:** This symptom occurs if you do not enter `y` at the prompt "Warning: All port will be shutdown when the logfile is full. Are you sure? [Y/N]:" that appears after you execute the `info-center log file overwrite-protection all-port-powerdown` command when the log file is full.

LSD074012

- **Symptom:** The log host records two identical logs for each command executed on the switch.

- **Condition:** This symptom occurs when the following conditions exist:
  - The log host is specified using the `info-center log host vpn-instance vpn1 ip address` command on the switch.
  - The VPN instance `vpn1` does not exist and the specified IP address is a public address.

LSD074011

- **Symptom:** The display current-configuration command displays the default SNMP configurations while SNMP is disabled.

- **Condition:** This symptom might occur if you specify SNMPv1 and SNMPv2c on the Web interface and then disable SNMP while the device is operating in FIPS mode and SNMP is not configured for the device.

LSD074104

- **Symptom:** If you enter `n`, or do not enter `y` before the confirmation timeout timer expires at the prompt that appears after you execute the `info-center log file overwrite-protection all-port-powerdown` command, the system displays incorrect messages. It displays "Log file directory cannot be more than 19 characters" after the confirmation timeout timer expires, or "Non-support language mode" after you enter `n`.

- **Condition:** This symptom occurs if you enter `n`, or do not enter `y` before the confirmation timeout timer expires at the prompt that appears after you execute the `info-center log file overwrite-protection all-port-powerdown` command.

ZDD05611

- **Symptom:** When an IRF fabric in an L3VPN network can’t create BGP peer successfully, BGP GR process will takes four minutes. Under that condition, ping operations to a device connected to the IRF fabric fail.
• Condition: This symptom can be seen if a ping operation is performed to a device connected to an IRF fabric when the IRF fabric is performing BGP GR. The master device is rebooting.

**LSD074037**

• Symptom: Traffic that matches a deny-mode routing policy node might be handled by a permit-mode routing policy node.
• Condition: This symptom might occur if the following conditions exist:
  o Too many ACL resources are used.
  o Both a deny-mode node and a permit-mode node are configured for a routing policy, and the deny-mode node has a higher priority.

The following configuration is for reference:
```
policy-based-route proxy deny node 5
  if-match acl 3001

policy-based-route proxy permit node 10
  if-match acl 3002
  apply ip-address next-hop 192.168.3.2
```

**ZDD05791**

• 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.

**LSD074015**

• Symptom: The **shutdown** command executed for the log file overwrite protection function (configured by **info-center logfile overwrite-protection all-port-powerdown**) that is triggered by log saving failure is not saved into the running configuration file.
• Condition: This symptom can be seen when the switch performs the log file overwrite protection function (configured by **info-center logfile overwrite-protection all-port-powerdown**).

**LSD073914**

• Symptom: A user cannot change the login password and the following error message appears:
  
  Failed to write the password records to file.
  Error: Something wrong in writing the password history records. Failed to set password.
• Condition: This symptom might occur if a user with the security-audit user role logs in for the first time while the device is operating in FIPS mode.

**LSD074301**

• Symptom: The switch reboots after it receives an incorrect DHCP packet.
• Condition: This symptom might occur if the length of Option 82 in the DHCP packet exceeds the agent information field length.

**LSD074266**

• Symptom: The numbers in the packet statistics are random and cannot be cleared by using the **reset counters** command.
• Condition: This symptom might occur when you use the **display interface** command to display the statistics of a Layer 3 aggregate interface.

**LSD073946**

• Symptom: A high CPU usage (even nearly 100%) occurs.
• Condition: This symptom might occur if there are multiple PVST instances on the device and TC snooping is enabled. With TC snooping enabled, the device actively updates the MAC address table entries and ARP entries upon receiving TC-BPDUs. Because multiple PVST instances have abundant MAC address table entries and ARP entries, TC snooping may overburden the system.
LSD074438

- Symptom: The MAC address of a user is not removed from the Auth-Fail VLAN after a successful 802.1X re-authentication.
- Condition: This symptom occurs when the following conditions exist:
  - The same VLAN is specified as the critical VLAN and the PVID of the hybrid port.
  - The auth-fail VLAN is assigned to the user who fails the 802.1X authentication on the MAC-based access control port. Then, the user passes the 802.1X authentication at the second try.

LSD074514

- Symptom: A MIB node returns wrong value.
- Condition: This symptom might occur if you use MIB Browser or other network management tools to access the hh3cDevMSlotEnvironmentValue, hh3cDevMSlotEnvironmentUpperLimit, and hh3cDevMSlotEnvironmentLowerLimit nodes.

LSD072197

- Symptom: A secondary IP address can be assigned to the network management port that does not allow any secondary IP address configuration.
- Condition: This symptom occurs when the secondary IP address is assigned to the network management port M-GigabitEthernet 0/0/0 through IMC.

LSD074440/LSD074455

- Symptom: The switch drops IGMP reports.
- Condition: This symptom might be seen when the following conditions exist:
  - The switch is enabled with 802.1X authentication and MAC authentication.
  - The source MAC address of the IGMP report has passed MAC authentication.

Resolved problems in R1807P02

LSD074034

- 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.

LSD073959

- Symptom: Roll back the software from the version F1807P01 or later to a version before F1807P01 using ISSU compatible mode, the operation will fail.
- Condition: Roll back the software from the version F1807P01 or later to a version before F1807P01 using ISSU compatible mode.

Resolved problems in F1807P01

None
Resolved problems in F1805P02

LSD072808
- Symptom: Disabling and enabling MPLS operation after a master/subordinate switchover, MPLS function fails.
- Condition: This symptom occurs by disabling and enabling MPLS operation after a master/subordinate switchover.

LSD072882
- Symptom: Traffic passing IPS card cannot be forwarded.
- Condition: This symptom occurs if the mirroring mode is configured for IPS card on A5820X device.

Resolved problems in F1805P01

LSD72321
- 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.

LSD50222
- Symptom: A CE connected to a subordinate switch in an IRF fabric cannot communicate with the remote CE over a CCC connection.
- Condition: This symptom might occur if the CE connects to a subordinate switch in an IRF fabric that acts as a PE.

LSD62489
- Symptom: The Summary -> Network -> VLAN -> Select VLAN Web page displays incorrect information about VLAN members.
- Condition: This symptom might occur if VLAN member ports are configured on the switch.

LSD65783
- Symptom: Packet loss occurs during Layer 2 forwarding over a cross-chassis aggregate link.
- Condition: This symptom might occur if the following conditions exist:
  - The link-aggregation traffic redirection is enabled.
  - All traffic forwarding occurs on the master device.
  - The master device is rebooted.

LSD68838
- Symptom: An aggregate group port on an IRF member switch is down after the member switch is rebooted.
- Condition: This symptom might occur if the aggregate group comprises ports on different IRF member switches, and the port is a PVLAN promiscuous port.

LSD68704
- Symptom: MAC addresses that should be added to SVLAN are added to PVLAN when packets whose PVID is SVLAN are received.
- Condition: This symptom might occur if you configure isolater-user-vlan, and then cancel the PVLAN and SVLAN mapping.
ZDD04834
- Symptom: Software loading during an incompatible ISSU on a subordinate switch has multiple errors.
- Condition: This symptom might occur if the **issu rollback slot 1** command is executed repeatedly when an incompatible ISSU is loading software on a subordinate switch.

LSD071681
- Symptom: The fans of the 5820AF-24XG or 5800AF-48G run at the highest speed continuously.
- Condition: This symptom occurs after the switch has started for five minutes.

LSD071159
- Symptom: BFD flapping occurs on a sub card and BFD fails to establish a session over the sub card.
- Condition: This symptom might occur if you configure BFD and then insert the sub card.

LSD070899
- Symptom: The undo silent-interface configuration on the master gets lost after a master/subordinate switchover.
- Condition: This symptom occurs after a master/subordinate switchover is performed.

LSD68981
- Symptom: Memory leaks occur to the CWMP module, resulting in a system reboot.
- Condition: This symptom might occur if saving configuration fails because of insufficient Flash space when CWMP is running.

LSD071085
- Symptom: ACL description information gets lost after a master/subordinate switchover.
- Condition: This symptom occurs after a master/subordinate switchover is performed.

LSD69468
- Symptom: The switch reboots after long-time routing flapping.
- Condition: This symptom might occur if route flapping occurs for a long time then MPLS LDP is running.

LSD69541
- Symptom: A Cisco IP phone connected to the switch switches between voice VLAN and data VLAN.
- Condition: This symptom occurs when the device is connected to a Cisco IP phone that runs DHCP.

LSD67870
- Symptom: The CPU usage of the master switch in an IRF fabric is 100%.
- Condition: This symptom might occur after the subordinate switch has an ACFP policy assigned and then gets rebooted.

LSD68952
- Symptom: The console port is unresponsive.
- Condition: This symptom might occur when diagnosis information is saved to the subordinate switch.
LSD070280

- Symptom: The switch cannot respond to Tracert requests.
- Condition: This symptom occurs when the switch is running VRRP and is in backup state.

LSD071657

- Symptom: An error occurs to the MAC address table, resulting in a system reboot.
- Condition: This symptom might occur after a long-time operation.

LSD071662

- Symptom: IPv6 ACLs in hardware cannot be deleted.
- Condition: This symptom occurs if you assign IPv6 ACLs to a VLAN interface and then delete the ACLs.

LSD071306

- Symptom: CPU resources cannot be released, resulting in a system reboot.
- Condition: This symptom might be seen on a specific switch if overtime PCIE access occurs.

LSD071184

- Symptom: The switch cannot transparently transmit LSP echo packets.
- Condition: This symptom occurs when the switch is performing Layer 2 forwarding.

LSD071871

- Symptom: The port Ten-GigabitEthernet1/0/52 of 5800AF-48G goes up and down.
- Condition: This symptom might occur when the port is connected to a transceiver module that has digital diagnostic function.

Resolved problems in F1803L03

LSD69494

- Symptom: Some protocols on the switch cannot run properly.
- Condition: This symptom might occur when the CPU receives a large number of IP multicast packets within a short time.

LSD070281

- Symptom: FTP/TFTP download speeds on the HPE 5800 switch are slow.
- Condition: This symptom might occur during FTP/TFTP file downloads.

LSTB005616

- Symptom: A system reboot occurs when a copy operation is performed through a specific U disk.
- Condition: This symptom might occur during a copy operation through a specific U disk.

Resolved problems in F1803L01

LSD69190

- Symptom: The GMT time zone offset value of Caracas (capital of Venezuela) is not correct on the System Time page.
- Condition: None.
LSD69697
- Symptom: The IMC fails to perform topology calculation for a switch.
- Condition: This symptom might occur if the network management interface of the switch is connected to the IMC.

LSD69259
- Symptom: An SNMP walk on hh3cSysBootType MIB returns no values.
- Condition: This symptom might occur if the walk operation is performed after the switch reboots.

LSD070470
- Symptom: IRF protocols fail to exchange messages and CLI configurations fail, and BFD MAD cannot work and BFD is in an unstable state.
- Condition: An IRF fabric runs multiple protocols simultaneously for a long time.

Resolved problems in F1305P01

LSD66095
- Symptom: A port inserted with a non-HPE transceiver module cannot come up.
- Condition: This symptom might occur if the port connects to a non-HPE transceiver module with a fiber cable.

LSD63957
- Symptom: A switch that runs LLDP fails to display information about an LLDP neighbor after receiving an LLDP packet that contains an unknown organizationally-defined TLV longer than 500 bytes from the neighbor.
- Condition: This symptom occurs if the switch receives from an LLDP neighbor an LLDP packet that contains an unknown organizationally-defined TLV longer than 500 bytes.

LSD63958
- Symptom: A switch that runs LLDP fails to display information about an LLDP neighbor after receiving an LLDP packet in which the Location Identification TLV has an LCI value of 0.
- Condition: This symptom occurs if the switch receives from a neighbor an LLDP packet in which the Location Identification TLV has an LCI value of 0.

LSD65589
- Symptom: Memory leaks occur to the HTTP module, and the switch reboots.
- Condition: This symptom might occur if the switch receives non-standard HTTP packets (for example, the HTTP packets have the same domain).

LSD64596
- Symptom: The switch reboots when a user Telnets to the switch.
- Condition: This symptom might occur if the following conditions exist:
  o VTY debugging is enabled on the switch.
  o The Telnet Binary option is negotiated.

LSD64756
- Symptom: Result in DISMAN-PING-MIB::pingResultsOperStatus Failed and cannot be restore, the device reboot occasionally.
- Condition: Get or set RPINGMib to operate NQA through SNMP.
LPD12677
- Symptom: RX alarm information is incorrect in transceiver alarm information.
- Condition: This symptom might occur when both TX and RX power alarms exist on the same port.

LSD64709
- Symptom: 10G port in sub card cannot go up after it comes down normally.
- Condition: For the first time, 10G port in sub card is up, use ‘dis device manuinfo slot 1 subslot’ command to get the series number of sub card.

LSD64788
- Symptom: Outbound BPDU packets on a source port cannot be mirrored.
- Condition: This symptom might occur if the source port is configured with bidirectional mirroring and enabled with BPDU tunneling.

Resolved problems in R1211P04

LSD65853
- Symptom: The switch reboots when you configure a very log password for a Web user by using the cluster command.
- Condition: This symptom might occur when you configure a very log password for a Web user by using the cluster command.

ZDD04769
- Symptom: The switch reboots when it acts as the source DR.
- Condition: This symptom might occur when a downstream switch is enabled and disabled with PIM-SM continuously.

ZDD04754
- Symptom: The CPU usage is high when the switch acts as the DHCP server.
- Condition: This symptom might occur if many clients use conflict addresses.

ZDD04724
- Symptom: The switch reboots when LDP flapping occurs on a port.
- Condition: This symptom might occur when LDP flapping occurs on an unstable port.

LSD64220
- Symptom: The sFlow ifInOctet and ifOutOctet values should be 64-bit long, but the values displayed are 32-bit long.
- Condition: This symptom exists in displayed sFlow port statistics.

LSD65092
- Symptom: The switch reboots if fast and continuous NQA ping operations are performed.
- Condition: This symptom might occur if fast and continuous NQA ping operations are performed.

ZDD04358
- Symptom: LDP flapping occurs when the switch has established Martini MPLS L2VPN with a Cisco device.
- Condition: This symptom might be seen if a primary PW/backup PW switchover occurs on the Cisco device.
LSD64598
- Symptom: The switch reboots if you execute the `free user vty` command when VTY debugging is enabled.
- Condition: This symptom might occur if you execute the `free user vty` command when VTY debugging is enabled.

LSD66815
- Symptom: An error message appears after 24 ACL rules for matching TCP/UDP ports are assigned.
- Condition: This symptom might occur if more than 25 ACL rules for matching TCP/UDP ports are assigned.

LSD66490
- Symptom: Loopback detection logs show information different from the actual configuration.
- Condition: This symptom might occur if you change the loopback detection action from shutdown to semi-block when a loop has been detected.

LSD65841
- Symptom: A 1-second interruption occurs to Layer 2 forwarding during an IRF master/subordinate switchover.
- Condition: This symptom might occur if an IRF master/subordinate switchover is performed when enable link aggregation traffic redirection to the master.

LSD68572
- Symptom: The wireless card LSWM1WCM10 or IPS card LSDM1IPS10 might be identified as the firewall card LSWM1FW10.
- Condition: Upgrade the system software to R1211L01, R1211P02, R1211P03, F1305, or F1305P01.

LSD65758
- Symptom: A checksum error message appears when an SFP transceiver module is inserted.
- Condition: This symptom occurs if you insert an old 3Com SFP transceiver.

LSD65746
- Symptom: A BFD session on a port is not removed after the port goes down.
- Condition: This symptom might occur if you configure IRF member ID 10 for the switch.

HWD35697
- Symptom: POE function fails.
- Condition: When the switch of HPE TAA power up, insert the POE sub-card without firmware.

LSD68690
- Symptom: The link state of a 10GE port on the front panel is not stable.
- Condition: This symptom might occur if a voltage dip occurs and results in input clock noise on the 10GE port on the front panel.

LSD67497
- Symptom: The switch cannot learn PIM RP and NBR information in a VPN when it acts as a PE.
- Condition: This symptom might occur when the switch acts as a PE that resides in the same position as Dev B in the following network. In this network, multicast VPN is enabled. For network Private 1, Dev A is a PE device. For network Private 2 and Dev B, Dev A is a P device.
Dev A can receive VPN PIM RP and NBR information from the upstream device but it does not advertise the information to Dev B.

Resolved problems in R1211P02

LSD63054
- Symptom: The switch that acts as the sFlow agent sends both sampled_ipv4 and sampled_ethernet data in a sFlow packet.
- Condition: This symptom occurs when the switch sends a sFlow packet with a sampled_header.

LSD63203
- Symptom: The remark service-vlan-id command fails to take effect in the inbound direction on the customer-side port.
- Condition: This symptom occurs when two-to-two VLAN mapping is configured.

ZDD04235
- Symptom: The remark service-vlan-id command fails to take effect in the inbound direction on the customer-side port.
- Condition: This symptom occurs when two-to-two VLAN mapping is configured.

LSD61915
- Symptom: The ports of the AC card LSWM1WCM20 installed on a switch cannot start up after the switch starts up. This problem is solved after the AC card is hot swapped.
- Condition: This symptom occurs when a switch installed with the AC card LSWM1WCM20 starts up.

LSD62780
- Symptom: Pack forwarding errors occur, resulting in NLB failure.
- Condition: This symptom might occur when NLB is used on MCE.

LSD62622
- Symptom: An SNMP Get operation to the sflow sampler of a port fails.
- Condition: This symptom might occur when you use SNMP to get the sflow sampler of a specific port.

LSD62416
- Symptom: The save force command in the configuration file obtained through auto-configuration does not take effect, and the configuration file cannot be specified as the startup configuration file.
- Condition: This symptom occurs if the configuration file obtained through auto-configuration contains the save force command.
LSD59864
- Symptom: The BIMS management interface shows an IRF fabric as multiple switches.
- Condition: This symptom occurs if you use BIMS to manage an IRF fabric.

ZDD04271
- Symptom: The switch fails to establish usable LSPs.
- Condition: This symptom might occur in a specific network where the switch establishes many useless LSPs and has no resources to establish usable LSPs.

ZDD04176
- Symptom: When ARP attack protection is enabled, ARP entries on an interface are changed by ARP attack packets that are sourced from the same MAC address but have a sender IP address on a subnet different from the receiving interface.
- Condition: This symptom occurs if the interface receives ARP attack packets that are sourced from the same MAC address but have a sender IP address on a different subnet from the receiving interface.

ZDD04163
- Symptom: Chassis IDs in the displayed LLDP information contain garbled characters.
- Condition: This symptom occurs when the switch is connected to a specific IP Phone.

Resolved problems in R1211
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](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:

- HPE 5820X & 5800 Switch Series Installation Guide
- HPE 5820X & 5800 Switch Series Command References-Release 1810
- HPE 5820X & 5800 Switch Series Configuration Guides-Release 1810
- HPE PSR150-A & PSR150-D Power Supplies User Guide
- HPE PSR300-12A & PSR300-12D1 Power Supplies User Guide
- HPE PSR750-A Power Supply User Guide
- HPE LSW1FAN & LSW1BFAN Fan Assembly Installation
- HPE LSWM1FANSC & LSWM1FANSCB Fan Assembly Installation
- HPE OAP Cards User Guide
- HPE LSW148POEM PoE Module User Guide
- HPE 5820X & 5800 Switch Series Interface Cards User Guide
- HPE A58x0AF 650W AC (JC680A) & 650W DC (JC681A) Power Supplies User Guide

Documentation feedback

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

Hardware features

5800

Switch models and technical specifications

Table 5 lists the models in the HPE 5800 Switch Series and their alias names used in this document. Table 6 describes the technical specifications.

Table 5 Models in the HPE 5800 Switch Series

<table>
<thead>
<tr>
<th>Product code</th>
<th>HPE description</th>
<th>Alias</th>
</tr>
</thead>
<tbody>
<tr>
<td>JC101A</td>
<td>5800-48G-PoE+ Switch with 2 Interface Slots</td>
<td>5800-48G-PoE+ (2 slots)</td>
</tr>
<tr>
<td>JG242A</td>
<td>5800-48G-PoE+ TAA Switch with 2 Interface Slots</td>
<td>5800-48G-PoE+ TAA (2 slots)</td>
</tr>
<tr>
<td>JC105A</td>
<td>5800-48G Switch with 1 Interface Slot</td>
<td>5800-48G (1 slot)</td>
</tr>
<tr>
<td>JG258A</td>
<td>5800-48G TAA Switch with 1 Interface Slot</td>
<td>5800-48G TAA (1 slot)</td>
</tr>
<tr>
<td>JC104A</td>
<td>5800-48G-PoE+ Switch with 1 Interface Slot</td>
<td>5800-48G-PoE+ (1 slot)</td>
</tr>
<tr>
<td>JG257A</td>
<td>5800-48G-PoE+ TAA Switch with 1 Interface Slot</td>
<td>5800-48G-PoE+ TAA (1 slot)</td>
</tr>
<tr>
<td>JC100A</td>
<td>5800-24G Switch</td>
<td>5800-24G</td>
</tr>
<tr>
<td>JG255A</td>
<td>5800-24G TAA Switch</td>
<td>5800-24G TAA</td>
</tr>
<tr>
<td>JC099A</td>
<td>5800-24G-PoE+ Switch</td>
<td>5800-24G-PoE+</td>
</tr>
<tr>
<td>JG254A</td>
<td>5800-24G-PoE+ TAA Switch</td>
<td>5800-24G-PoE+ TAA</td>
</tr>
<tr>
<td>JC103A</td>
<td>5800-24G-SFP Switch with 1 Interface Slot</td>
<td>5800-24G-SFP (1 slot)</td>
</tr>
<tr>
<td>JG256A</td>
<td>5800-24G-SFP TAA Switch with 1 Interface Slot</td>
<td>5800-24G-SFP TAA (1 slot)</td>
</tr>
<tr>
<td>JG225A</td>
<td>5800AF-48G Switch</td>
<td>5800AF-48G</td>
</tr>
<tr>
<td>JC101B</td>
<td>5800-48G-PoE+ Switch with 2 Interface Slots</td>
<td>5800-48G-PoE+ (2 slots)</td>
</tr>
<tr>
<td>JG242B</td>
<td>5800-48G-PoE+ TAA Switch with 2 Interface Slots</td>
<td>5800-48G-PoE+ TAA (2 slots)</td>
</tr>
<tr>
<td>JC105B</td>
<td>5800-48G Switch with 1 Interface Slot</td>
<td>5800-48G (1 slot)</td>
</tr>
<tr>
<td>JG258B</td>
<td>5800-48G TAA Switch with 1 Interface Slot</td>
<td>5800-48G TAA (1 slot)</td>
</tr>
<tr>
<td>JC104B</td>
<td>5800-48G-PoE+ Switch with 1 Interface Slot</td>
<td>5800-48G-PoE+ (1 slot)</td>
</tr>
<tr>
<td>JG257B</td>
<td>5800-48G-PoE+ TAA Switch with 1 Interface Slot</td>
<td>5800-48G-PoE+ TAA (1 slot)</td>
</tr>
<tr>
<td>JC100B</td>
<td>5800-24G Switch</td>
<td>5800-24G</td>
</tr>
<tr>
<td>JG255B</td>
<td>5800-24G TAA Switch</td>
<td>5800-24G TAA</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Dimensions (H × W × D)</td>
<td>86.1 × 440 × 465 mm (3.39 × 17.32 × 18.31 in)</td>
<td>43.6 × 440 × 367 mm (1.72 × 17.32 × 14.45 in)</td>
</tr>
<tr>
<td>Weight</td>
<td>≤ 18 kg (39.68 lb)</td>
<td>≤ 6.5 kg (14.33 lb)</td>
</tr>
<tr>
<td>Console ports</td>
<td>1, on the front panel</td>
<td>1, covered by the logo plate on the front panel</td>
</tr>
<tr>
<td>Management Ethernet ports</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>USB ports (full speed)</td>
<td>1, on the front panel</td>
<td>1, covered by the logo plate on the front panel</td>
</tr>
<tr>
<td>10/100/1000 Base-T Ethernet ports</td>
<td>48, PoE</td>
<td>48</td>
</tr>
<tr>
<td>100/1000Base-X SFP ports</td>
<td>4</td>
<td>N/A</td>
</tr>
<tr>
<td>SFP+ ports</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

You can plug an SFP+ transceiver module, SFP transceiver module or SFP+ cable into an SFP port. An SFP port plugged in with an SFP+ cable can be used to connect IRF devices.
<table>
<thead>
<tr>
<th>Expansion interface card slots</th>
<th>2, on the front panel</th>
<th>1, on the rear panel</th>
<th>1, on the rear panel</th>
<th>N/A</th>
<th>1, on the rear panel</th>
<th>1, on the front panel</th>
</tr>
</thead>
<tbody>
<tr>
<td>OAP card slots</td>
<td>1</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Fan tray slots</td>
<td>1, hot swapping</td>
<td>N/A</td>
<td>N/A</td>
<td>2, hot swapping</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>PoE module slots</td>
<td>1</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Power supply slots</td>
<td>2, hot swapping</td>
<td>N/A</td>
<td>N/A</td>
<td>2, hot swapping</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>AC-input voltage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DC-input voltage</td>
<td>Rated voltage: 100 VAC to 240 VAC, 50 or 60 Hz</td>
<td>Rated voltage: 90 VAC to 264 VAC, 47 or 63 Hz</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RPS DC-input voltage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minimum power consumption</td>
<td>DC: 94 W</td>
<td>102 W</td>
<td>DC: 107 W</td>
<td>105 W</td>
<td>67 W</td>
<td>DC: 64 W</td>
</tr>
<tr>
<td></td>
<td>AC: 96 W</td>
<td></td>
<td>AC: 131 W</td>
<td></td>
<td>AC: 85 W</td>
<td>AC: 67 W</td>
</tr>
</tbody>
</table>

**Rated voltage:**
- **AC:**
  - Rated voltage: 100 VAC to 240 VAC, 50 or 60 Hz
  - Max voltage: 90 VAC to 264 VAC, 47 or 63 Hz

**DC:**
- Rated voltage: 300 W at –48 VDC to –60 VDC
- Rated voltage: 750 W at –54 VDC to –57 VDC

**RPS DC-input voltage:**
- Rated voltage: –52 VDC to –55 VDC
- Rated voltage: 10.8 VDC to 13.2 VDC
- Rated voltage: –52 VDC to –55 VDC

**Minimum power consumption:**
- DC: 94 W
- AC: 96 W
- 102 W
- DC: 107 W
- AC: 131 W
- 105 W
- 67 W
- DC: 64 W
- AC: 85 W
- DC: 58 W
- AC: 67 W
### Maximum power consumption

|-----------------------------|-------------------------|------------------------|-----------------------------------------------|------------------------------------------------|

| Operating temperature        | 0°C to 45°C (32°F to 113°F) |
| Operating humidity           | 10% to 90%, non condensing |

### Hardware compatibility matrixes

Interface cards, OAP cards, PoE modules, power supplies, and redundant power systems (RPSs) must be purchased separately. When you purchase or install these components, check that they are compatible with the switch.

You must separately purchase two fan trays for the 5800AF-48G switch. All other 5800 switches come with fixed fans or a fan tray installed.

### Table 7 Pluggable component (except the OAP cards) compatibility matrix

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>HPE 5830/5820/5800 650W AC power supply (JC680A)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>HPE</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Hot swappable power supply options

<table>
<thead>
<tr>
<th>Power supply</th>
<th>5800AF-48G</th>
<th>5800-24G-PoE+</th>
<th>5800-24G-SFP</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSR300-12A</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>PSR300-12D1</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>PSR750-A</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>HPE 5830/5820/5800 650W AC power supply (JC680A)</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>HPE</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>5830/5820/5800 650W DC power supply (JC681A)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>PSR150-A (JD362A) No No No No No No Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSR150-D (JD366A) No No No No No No Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Hot swappable fan tray options**

<table>
<thead>
<tr>
<th>LSW1FAN (JC096A)</th>
<th>Yes No No No No No No</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSWM1FANSC (JC682A)</td>
<td>No No No Yes No No No</td>
</tr>
<tr>
<td>LSWM1FANSCB (JC683A)</td>
<td>No No No Yes No No No</td>
</tr>
<tr>
<td>LSW1BFAN (JC098A)</td>
<td>No No No No No No Yes</td>
</tr>
</tbody>
</table>

**Interface card options**

<table>
<thead>
<tr>
<th>LSW1SP4P0 (JC091A)</th>
<th>Yes Yes Yes No Yes Yes Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSW1SP2P0 (JC092B)</td>
<td>Yes Yes Yes No Yes Yes Yes</td>
</tr>
<tr>
<td>LSW1GP16P0 (JC095A)</td>
<td>Yes Yes Yes No Yes Yes Yes</td>
</tr>
<tr>
<td>LSW1GT16P (JC094A)</td>
<td>Yes Yes Yes No Yes Yes Yes</td>
</tr>
</tbody>
</table>

**Hot swappable PoE module options**

<table>
<thead>
<tr>
<th>LSW148POEM (JC097B)</th>
<th>Yes only for the 5800-48 G-PoE+ (2 slots) No No No No No No</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSW148POEM (JG260A)</td>
<td>Yes only for the 5800-48 G-PoE+ TAA (2 slots) No No No No No No</td>
</tr>
</tbody>
</table>

**NOTE:**

The HPE 5830/5820/5800 650W AC power supply and the HPE 5830/5820/5800 650W DC power supply are referred to as the 650W AC power supply and the 650W DC power supply throughout this installation guide.
### Table 8 OAP card compatibility matrix

<table>
<thead>
<tr>
<th>Switch</th>
<th>LSWM1FW10 (JD255A)</th>
<th>LSWM1WCM10 (JD441A)</th>
<th>LSWM1WCM10 (JG261A)</th>
<th>LSWM1WCM20 (JD443A)</th>
<th>LSWM1WCM20 (JG262A)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5800-48G (1 slot)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>5800-48G-PoE+ (1 slot)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>5800-48G-PoE+ (2 slots)</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>5800AF-48G</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>5800-24G</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>5800-24G-PoE+</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>5800-24G-SFP (1 slot)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>5800-48G-PoE+ TAA (1 slot)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>5800-48G-PoE+ TAA (2 slots)</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>5800-48G TAA (1 slot)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>5800-24G-PoE+ TAA</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>5800-24G-SFP TAA (1 slot)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>5800-24G TAA</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**NOTE:**
You install the LSWM1WCM20 (JD443A, JG262A) card in the expansion interface card slot and all other OAP cards in the OAP card slot.

### Table 9 RPS compatibility matrix

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A-RPS1600 (JG136A)</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
5820X

Switch models and technical specifications

Table 10 lists the models in the HPE 5820X Switch Series and the alias that they are referred to in this document. Table 11 describes the technical specifications.

**Table 10 Models in the HPE 5820X Switch Series**

<table>
<thead>
<tr>
<th>Product code</th>
<th>HPE description</th>
<th>Alias</th>
</tr>
</thead>
<tbody>
<tr>
<td>JG219A</td>
<td>HP 5820AF-24XG Switch</td>
<td>5820AF-24XG</td>
</tr>
<tr>
<td>JC102A</td>
<td>HP 5820X-24XG-SFP+ Switch</td>
<td>5820X-24XG-SFP+</td>
</tr>
<tr>
<td>JG243A</td>
<td>HP 5820X-24XG-SFP+ TAA-compliant Switch</td>
<td>5820X-24XG-SFP+ TAA</td>
</tr>
<tr>
<td>JC106A</td>
<td>HP 5820X-14XG-SFP+ Switch with 2 Interface Slots</td>
<td>5820X-14XG-SFP+ (2 slots)</td>
</tr>
<tr>
<td>JG259A</td>
<td>HP 5820X-14XG-SFP+ TAA Switch with 2 Interface Slots</td>
<td>5820X-14XG-SFP+ TAA (2 slots)</td>
</tr>
</tbody>
</table>

**Table 11 The HPE 5820X Switch Series technical specifications**

<table>
<thead>
<tr>
<th>Item</th>
<th>5820AF-24XG</th>
<th>5820X-24XG-SFP+/5820X-24XG-SFP+ TAA</th>
<th>5820X-14XG-SFP+ (2 slots)/5820X-14XG-SFP+ TAA (2 slots)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dimensions (H × W × D)</td>
<td>43.6 × 440 × 660 mm (1.72 × 17.32 × 25.98 in)</td>
<td>43.6 × 440 × 427 mm (1.72 × 17.32 × 16.8 in)</td>
<td>86 × 440 × 467 mm (3.39 × 17.32 × 18.39 in)</td>
</tr>
<tr>
<td>Weight</td>
<td>≤ 11.2 kg (24.69 lb)</td>
<td>≤ 8.5 kg (18.74 lb)</td>
<td>≤ 17 kg (37.48 lb)</td>
</tr>
<tr>
<td>Console ports</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Management Ethernet ports</td>
<td>1</td>
<td>1</td>
<td>N/A</td>
</tr>
<tr>
<td>USB ports</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>10/100/1000Base-T Ethernet ports</td>
<td>2</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>SFP+ ports</td>
<td>24</td>
<td>24</td>
<td>14</td>
</tr>
<tr>
<td>Expansion interface card slots</td>
<td>N/A</td>
<td>N/A</td>
<td>2, front panel</td>
</tr>
<tr>
<td>OAP card slots</td>
<td>N/A</td>
<td>N/A</td>
<td>1, rear panel</td>
</tr>
<tr>
<td>Fan tray slots</td>
<td>2, rear panel</td>
<td>1, rear panel</td>
<td>1, rear panel</td>
</tr>
<tr>
<td>Power supply slots</td>
<td>2, rear panel</td>
<td>2, rear panel</td>
<td>2, rear panel</td>
</tr>
<tr>
<td>AC-input voltage</td>
<td>Rated voltage: 100 VAC to 240 VAC, 50 or 60 Hz</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Max voltage: 90 VAC to 264 VAC, 47 or 63 Hz

|------------------|-----------------------------------|-----------------------------------|-----------------------------------|-----------------------------------|

Operating temperature 0ºC to 45ºC (32°F to 113°F)
Operating humidity 10% to 90%, noncondensing

### Hardware compatibility matrix

Interface cards, OAP cards, power supplies, and RPSs must be purchased separately. When you purchase or install these components, check that they are compatible with the switch.

You must separately purchase two fan trays for the 5820AF-24XG switch. All other 5820X switches come with a fan tray installed.

**Table 12 Pluggable components (except the OAP cards) compatibility matrix**

<table>
<thead>
<tr>
<th>Cards/modules</th>
<th>5820AF-24XG</th>
<th>5820X-24XG-SFP+/5820X-24XG-SFP+ TAA</th>
<th>5820X-14XG-SFP+ (2 slots)/5820X-14XG-SFP+ TAA (2 slots)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hot swappable power supply options</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HPE 5830/5820/5800 650W AC power supply (JC680A)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>HPE 5830/5820/5800 650W DC power supply (JC681A)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>PSR300-12A (JC087A)</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PSR300-12D1 (JC090A)</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Fan tray options</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LSW1BFAN (JC098A)</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>LSW1FAN (JC096A)</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>LSWM1FANSC (JC682A)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>LSWM1FANSCB (JC683A)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Interface card options</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LSW1SP4P0 (JC091A)</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>LSW1SP2P0 (JC092B)</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**NOTE:**
The HPE 5830/5820/5800 650W AC power supply and the HPE 5830/5820/5800 650W DC power supply are referred to as the 650W AC power supply and the 650W DC power supply throughout this installation guide.
Table 13 OAP card compatibility matrix

<table>
<thead>
<tr>
<th>Switch</th>
<th>LSWM1FW 10 (JD255A)</th>
<th>LSWM1WCM 10 (JD441A)</th>
<th>LSWM1WCM 10 (JG261A)</th>
<th>LSWM1WCM 20 (JD443A)</th>
<th>LSWM1WCM 20 (JG262A)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5820AF-24XG</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>5820X-24XG-SFP+</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>5820X-24XG-SFP+ TAA</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>5820X-14XG-SFP+ (2 slots)</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>5820X-14XG-SFP+ TAA (2 slots)</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

NOTE:
You install the LSWM1WCM20 (JD443A or JG262A) card in the expansion interface card slot and all other OAP cards in the OAP card slot.

Table 14 RPS compatibility matrix

<table>
<thead>
<tr>
<th>RPS</th>
<th>5820AF-24XG</th>
<th>5820X-24XG-SFP+/5820X-24XG-SFP+ TAA</th>
<th>5820X-14XG-SFP+ (2 slots)/5820X-14XG-SFP+ TAA (2 slots)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A-RPS800 (JD183A)</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>A-RPS1600 (JG136A)</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Software features

Table 15 Software features of the 5800 series

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Switching capacity (full duplex)</td>
<td>284 Gbps</td>
<td>256 Gbps</td>
<td>208 Gbps</td>
<td>256 Gbps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Packet forwarding rate (whole system)</td>
<td>211.3 Mpps</td>
<td>190.5 Mpps</td>
<td>154.8 Mpps</td>
<td>190.5 Mpps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forwarding mode</td>
<td>Store and forward</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IRF</td>
<td>Ring topology</td>
<td>Chain topology</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Link aggregation</strong></td>
<td>- Aggregation of GE ports&lt;br&gt;- Aggregation of 10 GE ports&lt;br&gt;- Static link aggregation&lt;br&gt;- Dynamic link aggregation&lt;br&gt;An IRF fabric supports up to 128 aggregation groups, and each group supports up to eight GE ports or eight 10 GE ports.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Flow control</strong></td>
<td>IEEE 802.3x flow control and back pressure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Jumbo frame</strong></td>
<td>With a maximum size of 10000 bytes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>MAC address table</strong></td>
<td>- 32K MAC addresses&lt;br&gt;- 1K static MAC addresses&lt;br&gt;- Blackhole MAC addresses&lt;br&gt;- Limit to the number of MAC addresses learned on a port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>VLAN</strong></td>
<td>- Port-based VLANs (4094 VLANs)&lt;br&gt;- QinQ and selective QinQ&lt;br&gt;- Voice VLAN&lt;br&gt;- Protocol-based VLANs&lt;br&gt;- MAC-based VLANs&lt;br&gt;- IP subnet-based VLANs&lt;br&gt;- GVRP&lt;br&gt;- Super VLAN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>VLAN mapping</strong></td>
<td>- One-to-one VLAN mapping&lt;br&gt;- Many-to-one VLAN mapping&lt;br&gt;- Two-to-two VLAN mapping</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ARP</strong></td>
<td>- 16K entries&lt;br&gt;- 1K static entries&lt;br&gt;- Gratuitous ARP&lt;br&gt;- Standard proxy ARP and local proxy ARP&lt;br&gt;- ARP source suppression&lt;br&gt;- ARP detection (based on DHCP snooping entries/802.1X security entries/static IP-to-MAC bindings)&lt;br&gt;- Multicast ARP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ND</strong></td>
<td>- 8K entries&lt;br&gt;- 1K static entries</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>VLAN virtual interface</strong></td>
<td>1K</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DHCP</strong></td>
<td>- DHCP client&lt;br&gt;- DHCP snooping&lt;br&gt;- DHCP relay agent&lt;br&gt;- DHCP server&lt;br&gt;- DHCPv6 client&lt;br&gt;- DHCPv6 snooping&lt;br&gt;- DHCPv6 relay agent&lt;br&gt;- DHCPv6 server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Details</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDP helper</td>
<td>Supported</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td>Dynamic domain name resolution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dynamic domain name resolution client</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IPv4/IPv6 addresses</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv4 route</td>
<td>4K static routes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RIP v1/2: up to 4K IPv4 routes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OSPF v1/v2: up to 16K IPv4 routes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>BGP: up to 16K IPv4 routes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISIS: up to 16K IPv4 routes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>256 equal-cost routes, each having 8 next hops at most</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Routing policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VRRP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Policy based routing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IRDP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 route</td>
<td>2K static routes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RIPng: up to 2K IPv6 routes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OSPF v3: up to 8K IPv6 routes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>BGP4+ for IPV6: up to 8K IPv6 routes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISIS for IPV6: up to 8K IPv6 routes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>256 equal-cost routes, each having 8 next hops</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Routing policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VRRP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Policy routing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URPF</td>
<td>Reverse route check strict mode and loose mode</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MCE</td>
<td>IPv4/IPv6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BFD</td>
<td>OSPF/OSPFv3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>BGP/BGP4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IS-IS/IS-ISv6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PIM/IPM for IPv6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Static route</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MAD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tunnel</td>
<td>IPv4 over IPv4 tunnel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IPv4 over IPv6 tunnel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IPv6 over IPv4 manual tunnel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IPv6 over IPv4 6to4 tunnel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IPv6 over IPv4 ISATAP tunnel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IPv6 over IPv6 tunnel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>GRE tunnel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPLS</td>
<td>MPLS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VPLS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv4 multicast</td>
<td>IGMP snooping v1/v2/v3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Multicast VLAN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Multicast VLAN+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IGMP v1/v2/v3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PIM-DM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Details</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIM-SM</td>
<td>PIM-SM, PIM-SSM, MSDP, MBGP, PIM BI-DIR, Multicast VPN, Multicast over MCE, Multicast over MCE over tunnel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 multicast</td>
<td>MLD snooping v1/v2, PIM-DM/SM/SSM/BI-DIR for IPv6, IPv6 multicast VLAN, IPv6 multicast VLAN+, MBGP for IPv6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Broadcast/multicast/unicast storm control</td>
<td>in port rate percentage, in pps, in bps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MSTP</td>
<td>STP/RSTP/MSTP, STP root guard, BPDU guard, STP TC snooping</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RRPP</td>
<td>RRPP protocol, Multi-instance RRPP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smart Link</td>
<td>Up to 26 groups, Multi-instance Smart Link</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitor link</td>
<td>Supported</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QoS/ACL</td>
<td>Restriction of the rates at which a port sends and receives packets, with a granularity of 8 kbps. Packet redirection, CAR, with a granularity of 8 kbps. Global CAR (including aggregation CAR and hierarchical CAR). Eight output queues for each port. Per-port and per-queue Queue scheduling algorithms, including SP, WDRR, WFQ, and SP + WDRR. 802.1p and DSCP re-mark. Packet filtering at Layer 2 through 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 WRED Traffic shaping User profile COPP HQoS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mirroring</td>
<td>Traffic mirroring, Port mirroring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote mirroring</td>
<td>Multiple mirror observing ports</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Remote port mirroring (RSPAN/ERSPAN)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>Hierarchical management and password protection of users</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AAA authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RADIUS authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HWTACACS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SSH 2.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Port isolation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Port security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MAC address authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP-MAC-port binding</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP source guard</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HTTPS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SSL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PKI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Portal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EAD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Boot ROM access control (set Boot ROM password recovery)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>OAA</strong></td>
<td>OAA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IPS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Firewall</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anti virus</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wireless access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>802.1X</strong></td>
<td>Up to 2,048 users</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Port-based and MAC address-based authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Guest VLAN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Trunk port authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>802.1X-based dynamic QoS/ACL/VLAN assignment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Traffic Management</strong></td>
<td>IPFIX (NetStream)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>sFlow</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Software download and upgrade</strong></td>
<td>XModem</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FTP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TFTP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Management
- Configuration at the command line interface
- Remote configuration through Telnet
- Configuration through Console port
- SNMP
- RMON alarm, event and history recording
- IMC NMS
- Web-based network management
- System log
- Hierarchical alarms
- HGMPv2
- NTP
- PoE
- Power supply alarm function
- Fan and temperature alarms
- BIMS zero configuration

### Maintenance
- Debug information output
- Ping and Tracert
- NQA
- Track
- Remote maintenance through Telnet
- Virtual cable test
- 802.1ag
- 802.3ah
- DLDP
- File download and upload through USB port
- Auto power down
- EEE

<table>
<thead>
<tr>
<th>Feature</th>
<th>5820X-14XG-SFP+ (2 slots)/5820X-14XG-SFP+ TAA (2 slots)</th>
<th>5820X-24XG-SFP+/5820X-24XG-SFP+ TAA</th>
<th>5820AF-24XG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switching capacity</td>
<td>488 Gbps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(full duplex)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Packet forwarding rate</td>
<td>363 Mbps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(whole system)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forwarding mode</td>
<td>Store-forward and cut-through</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IRF</td>
<td>Ring topology</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Chain Topology</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MAD of BFD/LACP/ARP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISSU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Link aggregation</td>
<td>Aggregation of GE ports</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aggregation of 10-GE ports</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Static link aggregation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dynamic link aggregation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 16: Software features of the 5820X series
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>An IRF fabric</td>
<td>Supports up to 128 aggregation groups, and each group supports up to eight GE ports or eight 10-GE ports</td>
</tr>
<tr>
<td>Flow control</td>
<td>IEEE 802.3x flow control and back pressure</td>
</tr>
<tr>
<td>Jumbo Frame</td>
<td>Supports a maximum frame size of 10000 bytes</td>
</tr>
<tr>
<td>MAC address table</td>
<td>32K MAC addresses, 1K static MAC addresses, Blackhole MAC addresses, Limit to the number of MAC addresses learned on a port</td>
</tr>
<tr>
<td>VLAN</td>
<td>Port-based VLANs (4094 VLANs), QinQ and selective QinQ, Voice VLAN, Protocol-based VLANs, MAC-based VLANs, IP subnet-based VLANs, GVRP, Super VLAN</td>
</tr>
<tr>
<td>VLAN mapping</td>
<td>One-to-one VLAN mapping, Many-to-one VLAN mapping, Two-to-two VLAN mapping</td>
</tr>
<tr>
<td>ARP</td>
<td>8K entries, 1K static entries, Gratuitous ARP, Standard proxy ARP and local proxy ARP, ARP source suppression, ARP detection (based on DHCP snooping entries/802.1x security entries/static IP-to-MAC bindings), Multicast ARP</td>
</tr>
<tr>
<td>ND</td>
<td>4K entries, 1K static entries</td>
</tr>
<tr>
<td>VLAN virtual interface</td>
<td>1K</td>
</tr>
<tr>
<td>DHCP</td>
<td>DHCP client, DHCP snooping, DHCP relay agent, DHCP server, DHCPv6 client, DHCPv6 snooping, DHCPv6 relay agent, DHCPv6 server</td>
</tr>
<tr>
<td>UDP Helper</td>
<td>Supported</td>
</tr>
<tr>
<td>DNS</td>
<td>Dynamic domain name resolution, Dynamic domain name resolution client, IPv4/IPv6 addresses</td>
</tr>
<tr>
<td>IPv4 route</td>
<td>4K static routes, RIP v1/2: up to 4K IPv4 routes</td>
</tr>
<tr>
<td>Feature</td>
<td>Details</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>IPv4 routes</td>
<td>OSPF v1/v2: up to 12K IPv4 routes</td>
</tr>
<tr>
<td></td>
<td>BGP: up to 12K IPv4 routes</td>
</tr>
<tr>
<td></td>
<td>ISIS: up to 12K IPv4 routes</td>
</tr>
<tr>
<td></td>
<td>256 equal-cost routes, each having 8 next hops at most</td>
</tr>
<tr>
<td>Routing policy</td>
<td>VRRP</td>
</tr>
<tr>
<td></td>
<td>Policy based routing</td>
</tr>
<tr>
<td></td>
<td>IRDP</td>
</tr>
<tr>
<td>IPv6 routes</td>
<td>2K static routes</td>
</tr>
<tr>
<td></td>
<td>RIPng: up to 2K IPv6 routes</td>
</tr>
<tr>
<td></td>
<td>OSPFv3: up to 6K IPv6 routes</td>
</tr>
<tr>
<td></td>
<td>BGP4+: up to 6K IPv6 routes</td>
</tr>
<tr>
<td></td>
<td>ISISv6: up to 6K IPv6 routes</td>
</tr>
<tr>
<td></td>
<td>256 equal-cost routes, each having 8 next hops at most</td>
</tr>
<tr>
<td>Routing policy</td>
<td>VRRP</td>
</tr>
<tr>
<td></td>
<td>Policy based routing</td>
</tr>
<tr>
<td>URPF</td>
<td>Strict mode and loose mode</td>
</tr>
<tr>
<td>MCE</td>
<td>IPv4/IPv6</td>
</tr>
<tr>
<td>BFD</td>
<td>OSPF/OSPFv3</td>
</tr>
<tr>
<td></td>
<td>BGP/BGP4</td>
</tr>
<tr>
<td></td>
<td>IS-IS/IS-ISv6</td>
</tr>
<tr>
<td></td>
<td>PIM/IPM for IPv6</td>
</tr>
<tr>
<td></td>
<td>Static route</td>
</tr>
<tr>
<td></td>
<td>MAD</td>
</tr>
<tr>
<td>Tunnel</td>
<td>IPv4 over IPv4 tunnel</td>
</tr>
<tr>
<td></td>
<td>IPv4 over IPv6 tunnel</td>
</tr>
<tr>
<td></td>
<td>IPv6 over IPv4 manual tunnel</td>
</tr>
<tr>
<td></td>
<td>IPv6 over IPv4 6to4 tunnel</td>
</tr>
<tr>
<td></td>
<td>IPv6 over IPv4 ISATAP Tunnel</td>
</tr>
<tr>
<td></td>
<td>IPv6 over IPv6 tunnel</td>
</tr>
<tr>
<td></td>
<td>GRE tunnel</td>
</tr>
<tr>
<td>IPv4 multicast</td>
<td>IGMP snooping v1/v2/v3</td>
</tr>
<tr>
<td></td>
<td>Multicast VLAN</td>
</tr>
<tr>
<td></td>
<td>Multicast VLAN+</td>
</tr>
<tr>
<td></td>
<td>IGMP v1/v2/v3</td>
</tr>
<tr>
<td></td>
<td>PIM-DM</td>
</tr>
<tr>
<td></td>
<td>PIM-SM</td>
</tr>
<tr>
<td></td>
<td>PIM-SSM</td>
</tr>
<tr>
<td></td>
<td>MSDP</td>
</tr>
<tr>
<td></td>
<td>MBGP</td>
</tr>
<tr>
<td></td>
<td>PIM BI-DIR</td>
</tr>
<tr>
<td></td>
<td>Multicast over MCE</td>
</tr>
<tr>
<td></td>
<td>Multicast over MCE over Tunnel</td>
</tr>
<tr>
<td>IPv6 multicast</td>
<td>MLD snooping v1/v2</td>
</tr>
<tr>
<td>Feature</td>
<td>Details</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MLD v1/v2</td>
<td></td>
</tr>
<tr>
<td>PIM-DM/SM/SSM/BI-DIR for IPv6</td>
<td></td>
</tr>
<tr>
<td>IPv6 multicast VLAN</td>
<td></td>
</tr>
<tr>
<td>IPv6 multicast VLAN+</td>
<td></td>
</tr>
<tr>
<td>MBGP for IPv6</td>
<td></td>
</tr>
<tr>
<td>Broadcast/multicast/unicast storm control</td>
<td>In port rate percentage</td>
</tr>
<tr>
<td></td>
<td>In pps</td>
</tr>
<tr>
<td></td>
<td>In bps</td>
</tr>
<tr>
<td>MSTP</td>
<td>STP/RSTP/MSTP</td>
</tr>
<tr>
<td></td>
<td>STP root guard</td>
</tr>
<tr>
<td></td>
<td>BPDU guard</td>
</tr>
<tr>
<td></td>
<td>STP TC snooping</td>
</tr>
<tr>
<td>RRPP</td>
<td>RRPP protocol</td>
</tr>
<tr>
<td></td>
<td>Multi-instance RRPP</td>
</tr>
<tr>
<td>Smart link</td>
<td>Up to 26 groups</td>
</tr>
<tr>
<td></td>
<td>Multi-instance Smart Link</td>
</tr>
<tr>
<td>Monitor link</td>
<td>Supported</td>
</tr>
<tr>
<td>QoS/ACL</td>
<td>Restriction of the rates at which a port sends and receives packets, with a granularity of 8 kbps.</td>
</tr>
<tr>
<td></td>
<td>Packet redirection</td>
</tr>
<tr>
<td></td>
<td>CAR, with a granularity of 8 kbps.</td>
</tr>
<tr>
<td></td>
<td>Global CAR (including aggregation CAR and hierarchical CAR)</td>
</tr>
<tr>
<td></td>
<td>Eight output queues for each port</td>
</tr>
<tr>
<td></td>
<td>Per-port and per-queue queue scheduling algorithms, including SP, WDRR, WFQ, and SP + WDRR</td>
</tr>
<tr>
<td></td>
<td>802.1p and DSCP re-mark</td>
</tr>
<tr>
<td></td>
<td>Packet filtering at Layer 2 through Layer 4; flow classification based on source MAC address, destination MAC address, source IPv4/IPv6 address, destination IPv4/IPv6 address, port, protocol, and VLAN.</td>
</tr>
<tr>
<td></td>
<td>Time range</td>
</tr>
<tr>
<td></td>
<td>WRED</td>
</tr>
<tr>
<td></td>
<td>Traffic shaping</td>
</tr>
<tr>
<td></td>
<td>User profile</td>
</tr>
<tr>
<td></td>
<td>COPP</td>
</tr>
<tr>
<td>Mirroring</td>
<td>Traffic mirroring</td>
</tr>
<tr>
<td></td>
<td>Port mirroring</td>
</tr>
<tr>
<td></td>
<td>Multiple mirror observing ports</td>
</tr>
<tr>
<td>Remote mirroring</td>
<td>Remote port mirroring (RSPAN/ERSPAN)</td>
</tr>
<tr>
<td>Security</td>
<td>Hierarchical management and password protection of users</td>
</tr>
<tr>
<td></td>
<td>AAA authentication</td>
</tr>
<tr>
<td></td>
<td>RADIUS authentication</td>
</tr>
<tr>
<td></td>
<td>HWTACACS</td>
</tr>
<tr>
<td></td>
<td>SSH 2.0</td>
</tr>
<tr>
<td></td>
<td>Port isolation</td>
</tr>
<tr>
<td></td>
<td>Port security</td>
</tr>
<tr>
<td></td>
<td>MAC address authentication</td>
</tr>
<tr>
<td>IP-MAC-port binding</td>
<td>Data Center Feature</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>IP source guard</td>
<td>PFC</td>
</tr>
<tr>
<td>HTTPS</td>
<td>DCBX</td>
</tr>
<tr>
<td>SSL</td>
<td></td>
</tr>
<tr>
<td>PKI</td>
<td></td>
</tr>
<tr>
<td>Portal</td>
<td></td>
</tr>
<tr>
<td>EAD</td>
<td></td>
</tr>
<tr>
<td>Boot ROM access control (Set Boot ROM password recovery)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OAA</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS</td>
<td></td>
</tr>
<tr>
<td>Firewall</td>
<td></td>
</tr>
<tr>
<td>Anti virus</td>
<td></td>
</tr>
<tr>
<td>Wireless access</td>
<td></td>
</tr>
<tr>
<td>FC</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>802.1X</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 2,048 users</td>
<td></td>
</tr>
<tr>
<td>Port-based and MAC address–based authentication</td>
<td></td>
</tr>
<tr>
<td>Guest VLAN</td>
<td></td>
</tr>
<tr>
<td>Trunk port authentication</td>
<td></td>
</tr>
<tr>
<td>802.1X-based dynamic QoS/ACL/VLAN assignment</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Software download and upgrade</th>
<th>Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>XModem</td>
<td>Configuration at the command line interface</td>
</tr>
<tr>
<td>FTP</td>
<td>Remote configuration through Telnet</td>
</tr>
<tr>
<td>TFTP</td>
<td>Configuration through Console port</td>
</tr>
<tr>
<td></td>
<td>SNMP</td>
</tr>
<tr>
<td></td>
<td>RMON alarm, event and history recording</td>
</tr>
<tr>
<td></td>
<td>IMC NMS</td>
</tr>
<tr>
<td></td>
<td>Web-based network management</td>
</tr>
<tr>
<td></td>
<td>System log</td>
</tr>
<tr>
<td></td>
<td>Hierarchical alarms</td>
</tr>
<tr>
<td></td>
<td>HGMPv2</td>
</tr>
<tr>
<td></td>
<td>NTP</td>
</tr>
<tr>
<td></td>
<td>Power supply alarm function</td>
</tr>
<tr>
<td></td>
<td>Fan and temperature alarms</td>
</tr>
<tr>
<td></td>
<td>BIMS zero configuration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Maintenance</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Debug information output</td>
<td></td>
</tr>
<tr>
<td>Ping and Tracert</td>
<td></td>
</tr>
<tr>
<td>NQA</td>
<td></td>
</tr>
<tr>
<td>Track</td>
<td></td>
</tr>
<tr>
<td>Remote maintenance through Telnet</td>
<td></td>
</tr>
<tr>
<td>Virtual cable test</td>
<td></td>
</tr>
<tr>
<td>802.1ag</td>
<td></td>
</tr>
<tr>
<td>802.3ah</td>
<td></td>
</tr>
<tr>
<td>DLDP</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td></td>
</tr>
<tr>
<td>File download and upload through USB port</td>
<td></td>
</tr>
<tr>
<td>Auto power down</td>
<td></td>
</tr>
</tbody>
</table>
Appendix B Upgrading software

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

Table 17 Software upgrade methods

<table>
<thead>
<tr>
<th>Approach</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrading at the Boot menu</td>
<td>Using XMODEM to upgrade software through the console port</td>
</tr>
<tr>
<td></td>
<td>Using TFTP to upgrade software through an Ethernet port</td>
</tr>
<tr>
<td></td>
<td>Using FTP to upgrade software through an Ethernet Port</td>
</tr>
<tr>
<td>Upgrading at the CLI</td>
<td>Loading software through the USB interface</td>
</tr>
<tr>
<td></td>
<td>Loading software with FTP</td>
</tr>
<tr>
<td></td>
<td>Loading software with TFTP</td>
</tr>
</tbody>
</table>

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 5800AF-48G, 5800-24G-SFP (1 slot), 5800-24G-SFP TAA (1 slot), 5820AF-24XG, 5820X-24XG-SFP+ and 5820X-24XG-SFP+ TAA switches, HPE 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 extended 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 heavy memory test
   
   ********************************************************************************
   *                                                                              *
   *       HPE 5800-48G Switch with 1 Interface Slot BOOTROM, Version 303        *
   *                                                                              *
   ********************************************************************************
   Copyright (c) 2010-2015 Hewlett Packard Enterprise Development LP
   
   Creation Date   : Nov 10 2015,15:09:38
   CPU Clock Speed : 750MHz
   Memory Size     : 1024MB
   Flash Size      : 512MB
   CPLD Version    : 003
   PCB Version     : Ver.B
   Mac Address     : C4CAD9D5E686
   
   Press Ctrl-B to enter Extended Boot menu...0

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

**Table 18 Shortcut keys**

<table>
<thead>
<tr>
<th>Shortcut keys</th>
<th>Prompt message</th>
<th>Function</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl+B</td>
<td>Press Ctrl-B to enter Extended Boot menu...</td>
<td>Accesses the extended Boot menu.</td>
<td>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</td>
</tr>
</tbody>
</table>
Accessing the basic Boot menu

To access the basic Boot menu:

1. Press Ctrl+D within 1 seconds 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 303

**Table 19 Basic Boot ROM menu options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Update full BootRom</td>
<td>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 Using XMODEM to upgrade software through the console port.</td>
</tr>
<tr>
<td>2. Update extended BootRom</td>
<td>Update the extended Boot ROM segment. To do so, you must use XMODEM and the console port. For more information, see Using XMODEM to upgrade software through the console port.</td>
</tr>
<tr>
<td>3. Update basic BootRom</td>
<td>Update the basic Boot ROM segment. To do so, you must use XMODEM and the console port. For more information, see Using XMODEM to upgrade software through the console port.</td>
</tr>
</tbody>
</table>
Option | Task
--- | ---
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 20).

### Table 20 BASIC-ASSISTANT menu options

<table>
<thead>
<tr>
<th>Option</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. RAM Test</td>
<td>Perform a RAM self-test.</td>
</tr>
<tr>
<td>2. Reserved</td>
<td>Reserved option field.</td>
</tr>
<tr>
<td>3. Reserved</td>
<td>Reserved option field.</td>
</tr>
<tr>
<td>4. Reserved</td>
<td>Reserved option field.</td>
</tr>
<tr>
<td>0. Return to boot menu</td>
<td>Return to the basic Boot menu.</td>
</tr>
</tbody>
</table>

### 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 3). For more information about password recovery capability, see *HPE 5820X & 5800 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
Table 21 Extended Boot ROM menu options

<table>
<thead>
<tr>
<th>Option</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Download application file to flash</td>
<td>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 R1807P02 version (or higher) for upgrade.</td>
</tr>
<tr>
<td>2. Select application file to boot</td>
<td>&lt;ul&gt; &lt;li&gt;Specify the main and backup system software images for the next startup:&lt;/li&gt; &lt;li&gt;• If password recovery capability is enabled, you can specify a system software image of any version.&lt;/li&gt; &lt;li&gt;• If password recovery capability is disabled, the system software image version must be R1807P02 or higher.&lt;/li&gt; &lt;li&gt;Specify the main and backup configuration files for the next startup. This task can be performed only if password recovery capability is enabled.&lt;/li&gt; &lt;/ul&gt;</td>
</tr>
<tr>
<td>3. Display all files in flash</td>
<td>Display files on the flash.</td>
</tr>
<tr>
<td>4. Delete file from flash</td>
<td>Delete files to free storage space.</td>
</tr>
<tr>
<td>5. Restore to factory default configuration</td>
<td>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 220 or higher.</td>
</tr>
<tr>
<td>6. Enter BootRom upgrade menu</td>
<td>Load the next-startup configuration file with all user privilege passwords configured with the <strong>super password</strong> 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.</td>
</tr>
<tr>
<td>7. Skip current system configuration</td>
<td>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.</td>
</tr>
<tr>
<td>8. Reserved</td>
<td>Reserved option field.</td>
</tr>
<tr>
<td>9. Set switch startup mode</td>
<td>Set the startup mode to fast startup mode or full startup mode.</td>
</tr>
<tr>
<td>0. Reboot</td>
<td>Reboot the switch.</td>
</tr>
<tr>
<td>Ctrl+F: Format File System</td>
<td>Format the current storage medium.</td>
</tr>
<tr>
<td>Ctrl+P: Skip Super Password</td>
<td>Load the next-startup configuration file with all user privilege passwords configured with the <strong>super password</strong> 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.</td>
</tr>
</tbody>
</table>
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 4.

Table 22 EXTEND-ASSISTANT menu options

<table>
<thead>
<tr>
<th>Option</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Display Memory</td>
<td>Display data in the memory.</td>
</tr>
<tr>
<td>2. Search Memory</td>
<td>Search the memory for a specific data segment.</td>
</tr>
<tr>
<td>0. Return to boot menu</td>
<td>Return to the extended Boot ROM menu.</td>
</tr>
</tbody>
</table>

Using XMODEM to upgrade software through the console port

Setting terminal parameters

1. Start the PC and run the terminal emulation program, for example, HyperTerminal.
2. Select Start > Programs > Accessories > Communications > HyperTerminal to enter the HyperTerminal window. The Connection Description dialog box appears.

Figure 1 Connection description of the HyperTerminal

3. Type the name of the new connection in the Name text box and click OK. The following dialog box appears. Select the serial port to be used from the Connect using drop-down list.
4. Click OK after selecting a serial port. The following dialog box appears. Set Bits per second to 9600, Data bits to 8, Parity to None, Stop bits to 1, and Flow control to None.

5. Click OK after setting the serial port parameters. The HyperTerminal window appears.
6. Click Properties in the HyperTerminal window to enter the Switch Properties dialog box. Click the Settings tab, set the emulation to VT100, and then click OK.
Figure 5 Set terminal emulation in Switch Properties dialog box

Complete the following tasks to update the Boot ROM program with XMODEM through the console port (For details about the HyperTerminal, refer to Setting terminal):

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter 6 or press Ctrl + U in the extended Boot menu to access the Boot ROM update menu.</td>
<td>Required. Log in to the switch through the HyperTerminal and then configure the protocol used for loading files.</td>
</tr>
<tr>
<td>Enter 1 to update the entire Boot ROM. The file transfer protocol menu appears.</td>
<td></td>
</tr>
<tr>
<td>Enter 3 to choose</td>
<td>Required. Log in to the switch through the HyperTerminal and then set the download rate of the console port on the switch.</td>
</tr>
<tr>
<td>Choose an appropriate download rate. For example, enter 5 to choose 115200 bps.</td>
<td>Required. Log in to the switch through the HyperTerminal and then set the download rate of the console port on the switch.</td>
</tr>
<tr>
<td>Change the baud rate setting on the terminal</td>
<td>Optional. Set the baud rate of the serial port on the terminal to be consistent with that of the console port on the switch.</td>
</tr>
<tr>
<td>Press Enter to establish a connection between the terminal and the switch for downloading the file</td>
<td>Optional.</td>
</tr>
<tr>
<td>Upload the software file from the terminal to the switch</td>
<td>Required. Transmit a file from the terminal to the switch using XMODEM.</td>
</tr>
</tbody>
</table>
switch | the changed connection rate.
---|---
Update the Boot ROM file on the switch | Required.
Update the Boot ROM file on the switch.
---|---
Restore the download rate to 9600 bps (the default) | Optional.
Set the baud rate of the serial port on the terminal to be consistent with the default rate of the console port on the switch.
---|---
Press any key to return to the Boot ROM update menu. | Required.

7. Enter 6 or press Ctrl + U in the extended Boot menu to access the Boot ROM update menu.

   Enter your choice(0-9): 6

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

   Enter your choice(0-3):

   Table 23 Boot ROM update menu options

<table>
<thead>
<tr>
<th>Option</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Update full BootRom</td>
<td>Update the complete Boot ROM file.</td>
</tr>
<tr>
<td>2. Update extended BootRom</td>
<td>Update the extended Boot ROM segment.</td>
</tr>
<tr>
<td>3. Update basic BootRom</td>
<td>Update the basic Boot ROM segment.</td>
</tr>
<tr>
<td>0. Return to boot menu</td>
<td>Return to the previous menu.</td>
</tr>
</tbody>
</table>

8. Enter 1 to update the entire Boot ROM. The file transfer protocol menu appears.

   NOTE:
   All the Boot ROM files used for upgrade are complete Boot ROM files.

   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):

   Table 24 File transfer protocol menu options

<table>
<thead>
<tr>
<th>Option</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Set TFTP protocol parameter</td>
<td>Set TFTP parameters.</td>
</tr>
<tr>
<td>2. Set FTP protocol parameter</td>
<td>Set FTP parameters.</td>
</tr>
</tbody>
</table>
3. Set XMODEM protocol parameter | Set XMODEM parameters.

0. Return to boot menu | Return to the Boot ROM menu.

9. Enter 3 to choose Xmodem. The baud rate menu appears.
   Please select your download baudrate:
   1.* 9600
   2. 19200
   3. 38400
   4. 57600
   5. 115200
   0. Return
   Enter your choice (0-5):

10. Choose an appropriate download rate. For example, enter 5 to choose 115200 bps.
    Download baud rate is 115200 bps
    Please change the terminal's baud rate 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 update takes tens of minutes.

11. Change the baud rate setting on the terminal to be the same as on the switch:
    a. Select Call > Disconnect in the HyperTerminal window to disconnect the terminal from the switch.

Figure 6 Disconnecting the terminal from the switch

b. Select File > Properties. In the Properties dialog box, click Configure (as shown in Figure 7), and then select 115200 from the Bits per second drop-down list box (as shown in Figure 8).
c. Select **Call > Call** to reestablish the connection.
NOTE:
The new settings can take effect only after you reestablish the connection.

12. Press Enter to establish a connection between the terminal and the switch for downloading the file.
    Now please start transfer file with XMODEM protocol.
    If you want to exit, Press <Ctrl+X>.
    Loading ...CCCCCCCCCC

NOTE:
Press Ctrl + X to quit downloading files; otherwise, proceed as follows.

13. Upload the software file from the terminal to the switch:
    a. Select Transfer > Send File in the HyperTerminal window (as shown in Figure 10). Click Browse in the pop-up dialog box (as shown in Figure 11) to select the software image file to be downloaded (for example, update.bin), and select Xmodem from the Protocol drop-down list.

Figure 10 Transfer menu

Figure 11 File transmission dialog box

b. Click Send. The following dialog box appears:
14. Update the Boot ROM file on the switch:
   After the Boot ROM file is downloaded, the terminal displays the following information:
   Loading ...CCCC Done!
   Will you Update Basic BootRom? (Y/N): Y
   The system asks you whether you want to update the basic Boot ROM segment. Click Y and then the system displays the following information after the update is completed.
   Updating Basic BootRom...........Done!
   Updating extended BootRom? (Y/N): Y
   The system asks you whether you want to update the extended Boot ROM segment. Click Y. Then the system displays the following information after the update is completed:
   Updating extended BootRom.........Done!
   Please change the terminal's baudrate to 9600 bps, press ENTER when ready.

15. Restore the download rate to 9600 bps (the default). See Change the baud rate setting on the terminal.

16. Press any key to return to 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):

17. Enter 0 to return to the extended Boot menu.
18. Enter 0 in the extended Boot menu to restart the device.

After the restart is complete, the updated Boot ROM file becomes effective.
Loading a system software image file

To load the system software image file of the switch, enter 1 in the extended Boot menu. The system displays the following information:

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

Select an appropriate protocol in Table 24 to load the file.

The procedure of loading a system software image file is the same as upgrading Boot ROM.

After the file is loaded, set the file attribute to main, backup, or none at the prompt.

Writing flash.................................................................
.............Done!

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

NOTE:
If a system software image file with a specific attribute already exists when you set a new file with the attribute, the attribute of the existing file becomes none after the new file becomes effective.

Using TFTP to upgrade software through an Ethernet port

Upgrading the Boot ROM program

Complete the following tasks to upgrade the Boot ROM program using TFTP through an Ethernet port (For details about the HyperTerminal, refer to Setting terminal):

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set up the configuration environment</td>
<td>Required. Connect the switch to the TFTP server through an Ethernet port, and to a PC through the console port. The PC and the TFTP server can be the same device.</td>
</tr>
<tr>
<td>Run the TFTP Server program on the sever</td>
<td>Required.</td>
</tr>
<tr>
<td>Run the terminal emulation program on the PC connected with the switch's console port. Start the switch and enter the Boot ROM menu. Then enter the protocol parameter setting menu.</td>
<td>Required. Log in to the switch through the HyperTerminal and configure the protocol for uploading the Boot ROM file.</td>
</tr>
<tr>
<td>Enter 1 to update the entire Boot ROM. The file transfer protocol menu appears.</td>
<td></td>
</tr>
<tr>
<td>Enter 1 to choose TFTP. The TFTP</td>
<td></td>
</tr>
<tr>
<td>Update the Boot ROM file on the switch</td>
<td>Required. Update the Boot ROM file on the switch.</td>
</tr>
<tr>
<td>Press any key to return to the Boot ROM update menu.</td>
<td>Required. Restart the switch to make the updated Boot ROM file effective.</td>
</tr>
</tbody>
</table>
1. Set up the configuration environment:
   Connect an Ethernet port (GigabitEthernet 1/0/25, for example) of the switch to the server
   (whose IP address is available) that provides the file (usually the .bin file) to be downloaded,
   and connect the console port of the switch to a PC, as shown in Figure 13.

   Figure 13 Load software using TFTP/FTP through Ethernet port

   ![Figure 13 Load software using TFTP/FTP through Ethernet port](image)

   **CAUTION:**
   - The PC and the TFTP/FTP server can be the same device.
   - Each 5800-24G-SFP switch with 1 Interface Slot provides a management Ethernet port, which can work
   even when a switching chip problem causes all regular Ethernet ports to stop working. To guarantee an
   upgrade success, HPE recommends using the management Ethernet port for software upgrade.
   - The TFTP/FTP server program is not provided with the HPE 5800 series. Make sure one TFTP/FTP server
   program is available yourself.

2. Run the TFTP Server program on the server:
   Run TFTP Server on the server connected with the switch's Ethernet port, and specify the path
   of the application file to be downloaded.

3. Run the terminal emulation program on the PC connected with the switch's console port. Start
   the switch and enter the Boot ROM menu. Then enter the protocol parameter setting menu.
   If you want to load the Boot ROM file, enter 6 in the extended Boot menu after the system
   displays "Enter your choice(0-9):" 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):

4. Enter 1 to update the entire Boot ROM. The file transfer protocol menu appears.
   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 choose TFTP. The TFTP settings menu appears.
   Load File Name :update.bin
   Server IP Address :10.10.10.2
   Local IP Address :10.10.10.3
   Gateway IP Address :
Table 25 TFTP parameter settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load File Name</td>
<td>Name of the file to be downloaded (for example, update.bin).</td>
</tr>
<tr>
<td>Server IP Address</td>
<td>IP address of server (for example, 10.10.10.2).</td>
</tr>
<tr>
<td>Local IP Address</td>
<td>IP address of the switch (for example, 10.10.10.3).</td>
</tr>
<tr>
<td>Gateway IP Address</td>
<td>IP address of the gateway (suppose it is not specified).</td>
</tr>
</tbody>
</table>

**NOTE:**
- Enter the file name and IP addresses based on the actual condition.
- If the switch and the server are on the same network segment, you can specify any unused IP address of the network for the switch without specifying the gateway's IP address; if they are not on the same segment, you need to specify the gateway's IP address so that the switch can communicate with the server.

6. Update the Boot ROM file on the switch:
   Enter the corresponding parameters based on the actual condition. The system displays the following information:
   ```
   Loading........................................................................
   ...............................................................................
   ................................Done!
   Will you Update Basic BootRom? (Y/N):Y
   ```
   The system asks you whether you want to update the basic Boot ROM segment. Click Y. Then the system displays the following information after the update is complete:
   ```
   Updating Basic BootRom...........Done!
   Updating extended BootRom? (Y/N):Y
   ```
   The system asks you whether you want to update the extended Boot ROM segment. Click Y. Then the system displays the following information after the update is complete:
   ```
   Updating extended BootRom.........Done!
   ```

7. Press any key to return to the Boot ROM update menu.
   ```
   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):
   ```

8. Enter 0 to return to the extended Boot menu.
9. Enter 0 in the extended Boot menu to restart the device.
   After the restart is complete, the updated Boot ROM file becomes effective.

**Loading a system software image file**

To load the system software image file of the switch, enter 1 in the extended Boot menu. The system displays the following information:

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

You can enter 1 to load the file.

The procedure of loading a system software image file is the same as upgrading Boot ROM.

After the file is loaded, set the file attribute to main, backup, or none at the prompt.

Writing flash. ............................................................. Done!

Please input the file attribute (Main/Backup/None) M

Done!

NOTE:

If a system software image file with a specific attribute already exists when you set a new file with the attribute, the attribute of the existing file becomes none after the new file becomes effective.

Using FTP to upgrade software through an Ethernet Port

Upgrading the Boot ROM program

NOTE:

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

Complete the following tasks to upgrading the Boot ROM program using FTP through an Ethernet port (For details about the HyperTerminal, refer to Setting terminal:

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| Set up the configuration environment | Required  
Connect the switch to the TFTP server through an Ethernet port, and to a PC through the console port. The PC and the TFTP server can be the same device. |
| Run the FTP Server program on the server | Required |
| Run the terminal emulation program on the PC connected with the switch's console port. Start the switch and enter the Boot ROM menu, and then enter the protocol parameter setting menu. | Required |
| Enter 1 to update the entire Boot ROM. The file transfer protocol menu appears. | Log in to the switch through the HyperTerminal and configure the protocol for uploading the Boot ROM file. |
| Enter 2 to choose FTP. The FTP settings menu appears. | |
| Update the Boot ROM file on the switch | Required  
Update the Boot ROM file on the switch. |
| Press any key to return to the Boot ROM update menu. | Required  
Restart the switch to make the updated Boot ROM file effective. |

1. Set up the configuration environment:

Connect an Ethernet port (GigabitEthernet 1/0/25, for example) of the switch to the server (whose IP address is available) that provides the file (usually the .bin file) to be downloaded, and connect the console port of the switch to a PC, as shown in Figure 13.
2. Run the FTP Server program on the server:
   Run FTP Server on the server connected with the switch's Ethernet port, configure the FTP username and password, and specify the path of the software image file to be downloaded.

3. Run the terminal emulation program on the PC connected with the switch’s console port. Start the switch and enter the Boot ROM menu, and then enter the protocol parameter setting menu.
   If you want to load the Boot ROM file, enter 6 in the Boot ROM menu after the system displays "Enter your choice(0-9):" 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):

4. Enter 1 to update the entire Boot ROM. The file transfer protocol menu appears.
   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 choose FTP. The FTP settings menu appears.
   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 : 5800
   FTP User Password : 123

   Table 26 FTP parameter settings
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load File Name</td>
<td>Name of the file to be downloaded</td>
</tr>
<tr>
<td>Server IP Address</td>
<td>IP address of the PC</td>
</tr>
<tr>
<td>Local IP Address</td>
<td>IP address of the switch</td>
</tr>
<tr>
<td>Gateway IP Address</td>
<td>IP address of the gateway</td>
</tr>
<tr>
<td>FTP User Name</td>
<td>Username for logging in to the FTP server, which should be consistent with that configured on the FTP server.</td>
</tr>
<tr>
<td>FTP User Password</td>
<td>Password for logging in to the FTP server, which should be consistent with that configured on the FTP server.</td>
</tr>
</tbody>
</table>

   NOTE:
   - Enter the file name and IP addresses based on the actual condition.
   - If the switch and the server are on the same network segment, you can specify any unused IP address of the network for the switch without specifying the gateway's IP address; if they are not on the same segment, you need to specify the gateway's IP address so that the switch can communicate with the server.

6. Update the Boot ROM file on the switch:
Enter the corresponding parameters based on the actual condition. The system displays the following information:
Will you Update Basic BootRom? (Y/N): Y
The system asks you whether you want to update the basic Boot ROM segment. Click Y. The system displays the following information after the update is complete:
Updating Basic BootRom...........Done!
Updating extended BootRom? (Y/N): Y
The system asks you whether you want to update the extended Boot ROM segment. Click Y and then the system displays the following information after the update is complete:
Updating extended BootRom.........Done!
7. Press any key to return to the Boot ROM update menu.

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):
8. Enter 0 to return to the extended Boot menu.
9. Enter 0 in the extended Boot menu to restart the device.
After the restart is complete, the updated Boot ROM file becomes effective.

Loading a system software image file
To load the system software image file of the switch, enter 1 in the extended Boot menu. The system displays the following information:
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 load the file through FTP.
The procedure of loading a system software image file is the same as upgrading Boot ROM.
After the file is loaded, set the file attribute to main, backup, or none at the prompt.

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

NOTE:
If a system software image file with a specific attribute already exists when you set a new file with the attribute, the attribute of the existing file becomes none after the new file becomes effective.

Upgrading software from CLI
You can upgrade software or download files remotely from CLI.
Loading software through the USB interface

Each HPE 5800 series switch provides a USB interface on its front panel. You can download software files to a removable storage device (such as a USB flash disk), and load the file through the USB interface.

To load a software file (for example, update.bin) from the USB flash disk:
1. Plug the USB flash disk containing the update.bin file in the USB interface of the switch.
2. Copy the update.bin file to the flash memory of the switch.
   ```
   <HPE> cd flash:
   <HPE> copy usba:/update.bin update.bin
   ```
3. Remove the USB flash disk, and then load the Boot ROM file.
   ```
   <HPE> 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...
   ```
4. Load the file, and specify the file as the main program file.
   ```
   <HPE> 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!
   <HPE> 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
   ```
   ```
   <HPE> reboot
   ```

**NOTE:**
- After loading the file, use the reboot command to restart the switch to make the update take effect (make sure you have saved other configurations before restart).
- If the built-in flash does not have enough space, load the Boot ROM file first, and then delete unused files (for example, unused system software image files) from the built-in flash, and then load the new system software image file.
- Avoid power failure during the loading process.

Loading software with FTP

As shown in Figure 14, run FTP Server on the local host, configure username admin and the password, and specify the path of the file to be downloaded (suppose the IP address of the FTP server is 202.10.10.53). Then, telnet to the switch and send the host program file to the switch using FTP.

**Figure 14 Load software through FTP**
To download a software file (for example, update.bin) from an FTP server and upgrade software:

1. **Download the file to the switch by using FTP.**
   
   ```
   <HPE> 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  
   [ftp] bye  
   ```

2. **Upgrade the Boot ROM program.**

   ```
   <HPE> 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 file, and specify the file as the main system software image file.**

   ```
   <HPE> 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!  
   ```

   ```
   <HPE> 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  
   <HPE> reboot  
   ```

**NOTE:**

- After loading the application file, use the **reboot** command to restart the switch to make the update take effect (make sure you have saved other configurations before restart).

- If the built-in flash does not have enough space, load the Boot ROM file first, and then delete unused files (for example, unused system software image files) from the built-in flash, and then load the new system software image file.

- Avoid any power failure during the loading process.

**Loading software with TFTP**

Loading a file through TFTP is similar to loading a file through FTP. The switch can serve only as a TFTP client that downloads the file from the TFTP server to its flash memory. The procedure after download is the same as loading the file remotely through FTP.
Contents

A5800_5820X-CMW520-R1810P16 ............................................................... 1
New feature: ITU channel number for a transceiver module ................... 1
  Specifying an ITU channel number for a transceiver module ................... 1
  Command reference ............................................................................. 1
    New command: itu-channel ............................................................... 1
    New command: display transceiver itu-channel .................................... 2
    Modified command: display transceiver alarm ..................................... 3
    Modified command: display transceiver diagnosis ................................ 4
A5800_5820X-CMW520-R1810P12 ............................................................... 5
New feature: Transparent transmission for protocol packets in a VPN ....... 5
Enabling transparent transmission for protocol packets in a VPN .......... 5
  Command reference ............................................................................. 5
    bpdu-tunnel l2vpn-transport ............................................................ 5
A5800_5820X-CMW520-R1810P11 ............................................................... 7
A5800_5820X-CMW520-R1810P10 ............................................................... 8
A5800_5820X-CMW520-R1810P07 ............................................................... 9
Modified feature: NTP support for ACL .................................................. 9
  Feature change description ............................................................... 9
    Modified command: ntp-service authentication-keyid .......................... 9
A5800_5820X-CMW520-R1810P06 ............................................................... 10
A5800_5820X-CMW520-R1810P03 ............................................................... 11
New feature: Default settings configuration for prefixes advertised in RA messages ......................................................... 11
  Configuring the default settings for prefixes advertised in RA messages ................................................................. 11
    Command reference ............................................................................. 11
      ipv6 nd ra prefix default ............................................................... 11
Modified feature: Prefix information configuration in RA messages .......... 12
  Feature change description ............................................................... 12
  Command changes ............................................................................. 12
    Modified command: ipv6 nd ra prefix ............................................... 12
Modified feature: Configuring the description of a VLAN .................... 13
  Feature change description ............................................................... 13
  Command changes ............................................................................. 13
    Modified command: description ....................................................... 13
A5800_5820X-CMW520-R1810P01 ............................................................... 14
Modified feature: Displaying VLAN interface information .................... 14
  Feature change description ............................................................... 14
  Command changes ............................................................................. 14
    Modified command: display interface vlan-interface .......................... 14
Modified feature: Member device brand name

Feature change description

Command changes

Modified command: brand

New feature: Route summarization on an ASBR

Configuring route summarization on an ASBR

Command reference

Modified feature: Specifying multiple secondary HWTACACS servers

Feature change description

Command changes

Modified command: primary accounting

Modified command: primary authentication

Modified command: primary authorization

Modified command: secondary accounting

Modified command: secondary authentication

Modified command: secondary authorization

Modified feature: Disabling advertising prefix information in RA messages

Feature change description

Command changes

Modified command: ipv6 nd ra prefix

New feature: VLAN-specific DHCP snooping

Configuring DHCP snooping in a VLAN

Command reference

Modified feature: link aggregation management VLANs and management port

Specifying link aggregation management VLANs and management port

Command reference

link-aggregation management-vlan

link-aggregation management-port
New feature: Disabling SSL 3.0

  Disabling SSL 3.0 ........................................................................................................ 32
  Command reference ................................................................................................... 32
  ssl version ssl3.0 disable ...................................................................................... 32

Modified feature: DLDP hybrid shutdown mode ......................................................... 33

  Feature change description ..................................................................................... 33
  Command changes .................................................................................................. 33
  Modified command: dldp unidirectional-shutdown ................................................ 33

Modified feature: Configuring MTU on a Layer 3 interface ....................................... 33

  Feature change description ..................................................................................... 33
  Command changes .................................................................................................. 33
  Modified command: mtu .......................................................................................... 33

New feature: SNMP notifications for PVST topology changes ................................ 35

  Enabling SNMP notifications for PVST topology changes ..................................... 35
  Command reference .............................................................................................. 35
  snmp trap enable stp .............................................................................................. 35

New feature: Configuring the applicable scope of packet filtering on a VLAN interface 36

  Configuring the applicable scope of packet filtering on a VLAN interface ................ 36
  Command reference .............................................................................................. 36
  packet-filter filter ................................................................................................. 36

New feature: DHCPv6 snooping entry backup ............................................................ 37

  Configuring DHCPv6 snooping entry backup ......................................................... 37
  Command reference .............................................................................................. 38
  display ipv6 dhcp snooping binding database ...................................................... 38
  ipv6 dhcp snooping binding database filename ................................................... 39
  ipv6 dhcp snooping binding database update interval ......................................... 39
  ipv6 dhcp snooping binding database update now ............................................. 40

New feature: Displaying brief VLAN information ....................................................... 41

  Displaying brief VLAN information ...................................................................... 41
  Command reference .............................................................................................. 41
  display vlan brief ................................................................................................. 41

Modified feature: Enhanced CC authentication feature .......................................... 42

  Feature change description ................................................................................... 42
  Command changes ............................................................................................... 42
  New command: display public-key local ecdsa public ......................................... 42
  New command: public-key local export ecdsa ..................................................... 43
  Modified command: authentication-algorithm .................................................... 43
  Modified command: ciphersuite .......................................................................... 44
  Modified command: dh ......................................................................................... 44
  Modified command: pfs ....................................................................................... 44
  Modified command: prefer-cipher ...................................................................... 45
  Modified command: pre-shared-key ................................................................... 45
  Modified command: public-key local create ...................................................... 45
  Modified command: scp ...................................................................................... 46
  Modified command: sftp ...................................................................................... 46
  Modified command: ssh2 ..................................................................................... 47
New feature: Generic flow control check for Ethernet interfaces

Enabling generic flow control check for Ethernet interfaces
Command reference
flow-control-check enable

New feature: Remote flow mirroring

Configuring remote flow mirroring
Command reference
mirror-to

Modified feature: File signature verification in software upgrade (including ISSU)

Feature change description
Command changes

Modified feature: Executing interactive commands in interface range view

Feature change description
Command changes

Modified feature: Configuring physical state change suppression on an Ethernet interface

Feature change description
Command changes
Modified command: link-delay

Modified feature: Configuring a tag and description for an IPv6 static route

Feature change description
Command changes
Modified command: ipv6 route-static

Modified feature: BGP support for IPv6 link-local address for peer relationship establishment

Feature change description
Command changes
Modified command: peer connect-interface

New feature: Route addition for assigned prefixes on the DHCPv6 relay agent

Configuring route addition for assigned prefixes on the DHCPv6 relay agent
Command reference
display ipv6 dhcp relay prefix
ipv6 dhcp relay iapd-route-add
reset ipv6 dhcp relay prefix

New feature: Telnet/SSH user connection control

Configuring Telnet/SSH user connection control
Configuration prerequisites
Configuration procedure
Command reference
ssh server acl
ssh server ipv6 acl
telnet server acl
telnet server ipv6 acl
New feature: Advertising the COMMUNITY attribute through BGP VPN-IPv6/VPNv6 routes

Advertising the COMMUNITY attribute through BGP VPN-IPv6/VPNv6 routes

Command reference

peer advertise-community (IPv6 BGP-VPN instance view)

peer advertise-community (BGP-VPNv6 subaddress family view)

Modified feature: BGP support for IPv6 link-local address for peer relationship establishment

Feature change description

Command changes

Modified command: peer connect-interface

Modified feature: BPDU tunneling

Feature change description

Command changes

Modified command: bpdu-tunnel dot1q

New feature: 802.1X voice VLAN

Configuring an 802.1X voice VLAN

Configuration guidelines

Configuration prerequisites

Configuration procedure

Command reference

dot1x voice vlan

New feature: Sending EAPOL frames untagged on a port

Configuring a port to send EAPOL frames untagged

Command reference
dot1x eapol untag

New feature: TCP fragment attack protection

Enabling TCP fragment attack protection

Command reference

attack-defense tcp fragment enable

New feature: Tracert packet source IPv6 address configuration

Specifying the source IPv6 address for tracert packets

Command changes

Modified command: tracert ipv6

Modified feature: Auto status transition of dynamic secure MAC addresses

Feature change description

Command changes

Modified feature: IPv6 address with a 127-bit prefix length

Feature change description

Command changes

A5800_5820X-CMW520-R1808P25

New feature: Discarding IPv6 packets that contain extension headers

Enabling a device to discard IPv6 packets that contain extension headers

Command reference
New feature: Configuring switch-MDT .............................................................. 90
New feature: Multicast across VPNs ................................................................. 74
Configuring multicast across VPNs ................................................................. 74
Overview ............................................................................................................. 74
Specifying the source IP address for multicast across VPNs ............................. 76
Configuration example (Source-side PE configuration) .................................. 77
Configuration example (Receiver-side PE configuration) ............................... 79
Command reference ......................................................................................... 81
multicast extra-vpn ............................................................................................ 81
New feature: Configuring the expected bandwidth of an interface ................. 82
Configuring the expected bandwidth of an interface ....................................... 82
Command reference ......................................................................................... 82
bandwidth ......................................................................................................... 82
New feature: Configuring DHCPv6 relay on an MCE ..................................... 83
Configuring DHCPv6 relay on an MCE .......................................................... 83
Command reference ......................................................................................... 83
Modified feature: Customizing DHCP options .............................................. 83
Feature change description .................................................................. 83
Command changes ......................................................................................... 83
Modified command: option ........................................................................... 83
A5800_5820X-CMW520-R1808P17 ................................................................. 85
Modified feature: ACL-based packet filtering on a VLAN interface ............... 85
Feature change description .................................................................. 85
Command changes ......................................................................................... 85
Modified command: packet-filter .................................................................. 85
A5800_5820X-CMW520-R1808P15 ................................................................. 87
Modified feature: Setting the device name .................................................... 87
Feature change description .................................................................. 87
Command changes ......................................................................................... 87
Modified command: sysname ........................................................................ 87
Modified feature: BGP load balancing ......................................................... 87
Feature change description .................................................................. 87
Command changes ......................................................................................... 87
Modified command: balance ......................................................................... 87
Modified feature: Multicast BGP load balancing ......................................... 88
Feature change description .................................................................. 88
Command changes ......................................................................................... 88
Modified command: balance ......................................................................... 88
A5800_5820X-CMW520-R1808P13 ................................................................. 90
New feature: Configuring switch-MDT .............................................................. 90
Configuring switch-MDT ................................................................................. 90
Overview ............................................................................................................. 90
Configuring switch-MDT .................................................................................. 92
Displaying and maintaining switch-MDT ......................................................... 93
Command reference ......................................................................................... 94
display multicast-domain vpn-instance switch-group receive ...................... 94
display multicast-domain vpn-instance switch-group send ......................... 96
multicast-domain holddown-time .................................................................. 97
New feature: Configuring multicast VPN inter-AS option B .......................... 100
  Configuring multicast VPN inter-AS option B .................................. 100
  Share-MDT establishment by using RPF proxy vector on public networks .......... 100
  Upstream neighbor address check by using BGP connector on a private network ... 102
  Configuration example ....................................................................... 102
  Command reference ........................................................................... 109
  New command: multicast rpf proxy vector ........................................... 109
  New command: multicast rpf-proxy-vector compatible .............................. 110
  Modified command: display pim routing-table ..................................... 110
  Modified command: display pim neighbor ......................................... 112

A5800_5820X-CMW520-R1808P11 ............................................................... 113
A5800_5820X-CMW520-R1808P08 ............................................................... 114
New feature: Enabling MAC authentication multi-VLAN mode .................. 114
  Overview ......................................................................................... 114
  Configuration procedure ................................................................... 114
  Command reference ......................................................................... 114
  mac-authentication host-mode multi-vlan ............................................. 114

A5800_5820X-CMW520-R1808P06 ............................................................... 116
New feature: Supporting multicast routing and forwarding based on secondary IP addresses .............................................................. 116
  Multicast routing and forwarding based on secondary IP addresses ............ 116
  Command reference ......................................................................... 116
  Modified command: display pim neighbor ......................................... 116

A5800_5820X-CMW520-R1808P02 ............................................................... 119
New feature: Configuring a criterion to match the packet length ............... 119
  Configuring a criterion to match the packet length ................................ 119
  Command reference ......................................................................... 120
  if-match packet-length ................................................................... 120
New feature: Configuring a multiport ARP entry ...................................... 121
  Configuring a multiport ARP entry .................................................... 121
  Command reference ......................................................................... 121
New feature: Configuring a multiport unicast MAC address entry .............. 122
  Configuring a multiport unicast MAC address entry ................................ 122
  Configuring a multiport unicast MAC address entry on the specified interfaces 122
  Displaying multiport unicast MAC address entries ................................ 123
  Command reference ......................................................................... 123
  display mac-address multiport ......................................................... 123
  mac-address multiport (interface view) .............................................. 124
  mac-address multiport (system view) ................................................ 125
New feature: Configuring LLDP to advertise a specific voice VLAN .......... 126
  Configuration guidelines ................................................................... 126
  Configuration procedure ................................................................... 126
  Dynamically advertising server-assigned VLANs through LLDP ................ 127
  Command reference ......................................................................... 127
  lldp voice-vlan .............................................................................. 127
Modified feature: Looped-port status processing mechanism

- Feature change description
- Command changes

Modified feature: Portal redirection

- Feature change description
- Command changes

Modified feature: Implementing ACL-based IPsec

- Feature change description
  - IPsec configuration example
  - IKE configuration example
- Command changes

Modified feature: Executing a batch file

- Feature change description
- Command changes
  - Modified command: execute

Modified feature: Configuring system information for the SNMP agent

- Feature change description
- Command changes
  - Modified command: snmp-agent sys-info

A5800_5820X-CMW520-R1807P02

New feature: FIPS

- Overview
- FIPS self-tests
  - Power-up self-test
  - Conditional self-tests
  - Triggering a self-test
- Configuring FIPS
  - Enabling the FIPS mode
  - Triggering a self-test
- Displaying and maintaining FIPS
- FIPS configuration example
- Command reference
  - fips mode enable
  - display fips status
  - fips self-test

New feature: Configuring ACL-based IPsec

- Configuring ACL-based IPsec
- ACL-based IPsec configuration task list
- Configuring ACLs
- Configuring an IPsec transform set
- Configuring an IPsec policy
- Applying an IPsec policy group to an interface
- Configuring the IPsec session idle timeout
- Enabling ACL checking of de-encapsulated IPsec packets
- Configuring the IPsec anti-replay function
- Configuring packet information pre-extraction
- Enabling invalid SPI recovery
- Configuring IPsec RRI
- Displaying and maintaining IPsec
- IPsec configuration examples
  - IKE-based IPsec tunnel for IPv4 packets configuration example
- Command reference
  - Modified command: ah authentication-algorithm
  - New command: connection-name
New feature: Disabling password recovery capacity .................................. 214
  Disabling password recovery capacity ................................................. 214
  Command reference ............................................................................. 214
  password-recovery enable .................................................................. 214
New feature: Verifying the correctness and integrity of the file ................. 215
  Verifying the correctness and integrity of the file .................................. 215
  Command reference ............................................................................. 215
  crypto-digest ....................................................................................... 215
New feature: Enabling MAC address migration log notifying ....................... 215
  Command reference ............................................................................. 216
  mac-flapping notification enable .......................................................... 216
New feature: Configuring packet capture ............................................... 217
  Configuring the packet capture function ................................................. 217
  Displaying and maintaining packet capture ......................................... 218
  Packet capture configuration example .................................................. 218
  Packet capture configuration commands .............................................. 219
  display packet capture buffer ............................................................... 219
  display packet capture status ............................................................... 220
  packet capture .................................................................................... 220
  packet capture buffer save ................................................................. 221
  packet capture schedule ..................................................................... 222
  packet capture start ............................................................................ 223
  packet capture stop ............................................................................ 224
  reset packet capture buffer ................................................................ 225
New feature: Enabling log file overwrite-protection .................................. 226
  Enabling log file overwrite-protection .................................................. 226
  Command reference ............................................................................. 226
  info-center logfile overwrite-protection .............................................. 227
New feature: Setting the MTU of the VPLS instance ................................ 228
  Setting the MTU of the VPLS instance .................................................. 228
  Command reference ............................................................................. 228
  mtu ....................................................................................................... 228
New feature: Configuring an OSPFv3 NSSA area .............................................. 229

Configuring an OSPFv3 NSSA area ................................................................. 229
Command reference ......................................................................................... 229
nssa (OSPFv3 area view) .................................................................................... 229

Modified feature: Modifying CLI configuration commands executed in FIPS mode for CC evaluation ................................................................. 230

Feature change description ............................................................................. 230
Command changes ............................................................................................ 230
Modified command: display snmp-agent community ....................................... 245
Modified command: prefer-cipher ................................................................. 244
Modified command: ciphersuite ...................................................................... 243
Modified command: sftp .................................................................................. 242
Modified command: ssh2 .................................................................................. 241
Modified command: ssh user .......................................................................... 240
Modified command: scp ................................................................................. 239
Modified command: public-key local create ................................................. 239
Modified command: password-control super length .................................... 239
Modified command: password-control super composition ......................... 238
Modified command: secondary authentication (RADIUS scheme view) ....... 237
Modified command: primary accounting (RADIUS scheme view) ............... 237
Modified command: primary authentication (RADIUS scheme view) .......... 237
Modified command: secondary accounting (RADIUS scheme view) .......... 237
Modified command: password-control composition ..................................... 236
Modified command: password-control length .............................................. 236
Modified command: key (RADIUS scheme view) .......................................... 235
Modified command: key (HWTACACS scheme view) .................................... 235
Modified command: set authentication password ....................................... 234
Modified command: password ................................................................. 233
Modified command: protocol inbound ........................................................... 233
Modified command: authentication-mode ..................................................... 232
Modified command: protocol inbound ........................................................... 232
Modified command: set authentication password ....................................... 231
Modified feature: Modifying login management commands executed in FIPS mode for CC evaluation ................................................................. 232

Feature change description ............................................................................. 232
Command changes ............................................................................................ 232

Modified Feature: Modifying software upgrade commands executed in FIPS mode for CC evaluation ................................................................. 234

Feature change description ............................................................................. 234
Command changes ............................................................................................ 234

Modified Feature: Modifying configuration file management commands executed in FIPS mode for CC evaluation ......................................................... 235

Feature change description ............................................................................. 235
Command changes ............................................................................................ 235

Modified Feature: Modifying security commands executed in FIPS mode for CC evaluation ................................................................. 235

Feature change description ............................................................................. 235
Command changes ............................................................................................ 235

Modified feature: Modifying SNMP commands executed in FIPS mode for CC evaluation ................................................................. 245

Feature change description ............................................................................. 245
Command changes ............................................................................................ 245
Modified command: display snmp-agent community ....................................... 245
Modified command: snmp-agent community .................................................. 245
Modified command: snmp-agent group .......................... 245
Modified command: snmp-agent usm-user { v1 | v2c } .......... 246
Modified command: snmp-agent calculate-password .......... 246
Modified command: snmp-agent sys-info ......................... 246
Modified command: snmp-agent target-host ..................... 247
Modified command: snmp-agent usm-user v3 .................... 247

Modified feature: Displaying RPS status information .......... 248
Feature change description ........................................ 248
Command changes .................................................. 248
Modified command: display rps ................................... 248

New feature: Disabling MAC entry aging timer refresh based on destination MAC address .......... 249
Disabling MAC entry aging timer refresh based on destination MAC address ........................................... 249
Application example .............................................. 249
Command reference ................................................. 250
mac-address destination-hit disable .............................. 250

Modified feature: Support for MD5 authentication key rollover ...... 250
Feature change description ........................................ 250
Configuring OSPF authentication ................................ 250
Modified command: authentication-mode ......................... 250

Modified feature: Offline detect timer .......................... 252
Feature change description ........................................ 252
Command changes .................................................. 252
Modified command: mac-authentication timer .................. 253

Modified feature: Configuring the frequency with which the log file is saved .......... 253
Feature change description ........................................ 253
Command changes .................................................. 253
Modified command: info-center logfile frequency .............. 253

New feature: Configuring the VPN instance of the sFlow collector ...... 257
Configuring the VPN instance of the sFlow collector .......... 257
Command reference ................................................. 258
New feature: Setting the subnet mask length to be 31 ........................................ 258
  Setting the subnet mask length to be 31 ............................................................ 258
  Command reference ....................................................................................... 258
  Modified command: ip address ..................................................................... 258
New Feature: Displaying per-port queue-based traffic statistics .................... 258
  Displaying per-port queue-based traffic statistics ........................................ 258
  Command reference ..................................................................................... 259
  display qos queue-statistics ..................................................................... 259
New feature: Specifying a fixed verification code for Web login .................... 260
  Specifying a fixed verification code for Web login ...................................... 260
  Command reference .................................................................................... 260
New feature: Specifying the authentication mode for users trying to log in to the
device through HTTPS ..................................................................................... 260
  Specifying the authentication mode for users trying to log in to the device through HTTPS ............................................................. 260
  Command reference .................................................................................... 260
New feature: Setting the Web user connection timeout time ....................... 260
  Setting the Web user connection timeout time ........................................ 260
  Command reference .................................................................................... 261
New feature: Setting the size of the buffer for Web login logging ............... 261
  Setting the size of the buffer for Web login logging .................................. 261
  Command reference .................................................................................... 261
New feature: Configuring and displaying brand information ....................... 261
  Configuring and displaying brand information ........................................ 261
  Command reference .................................................................................... 261
New feature: Displaying the software and hardware copyright statements 261
  Displaying the software and hardware copyright statements .................. 261
  Command reference .................................................................................... 262
New feature: Creating a bidirectional MPLS TE tunnel ............................... 262
  Creating a bidirectional MPLS TE tunnel .................................................. 262
  Command reference .................................................................................... 262
New feature: Configuring DM ................................................................. 262
  Configuring DM .......................................................................................... 262
  Command reference .................................................................................... 262
New feature: Configuring static VPLS .......................................................... 262
  Configuring static VPLS ............................................................................ 262
  Command reference .................................................................................... 262
New feature: Configuring traffic policing for VPLS ..................................... 263
  Configuring traffic policing for VPLS ......................................................... 263
  Command reference .................................................................................... 263
New feature: Enabling VPLS statistics .......................................................... 263
  Enabling VPLS statistics ........................................................................... 263
  Command reference .................................................................................... 263
New feature: Configuring SVC MPLS L2VPN for a service instance or on a
Layer 3 interface .............................................................................................. 263
  Configuring SVC MPLS L2VPN for a service instance or on a Layer 3 interface ................................................................. 263
  Command reference .................................................................................... 264
New feature: Configuring traffic policing for an AC ........................................... 264
Configuring traffic policing for an AC ................................................................. 264
Command reference ......................................................................................... 264
New feature: Enabling traffic statistics for an AC .............................................. 264
Enabling traffic statistics for an AC ................................................................. 264
Command reference ......................................................................................... 264
New feature: Configuring a user-defined ACL .................................................. 264
Configuring a user-defined ACL ...................................................................... 264
Command reference ......................................................................................... 264
New feature: Configuring ECN for a queue ....................................................... 265
Configuring ECN for a queue ........................................................................... 265
Command reference ......................................................................................... 265
New feature: Configuring IPv6 portal .............................................................. 265
Configuring IPv6 portal .................................................................................. 265
Command reference ......................................................................................... 265
New feature: Specifying an ISP domain for users with unknown domain names .................................................. 265
Specifying an ISP domain for users with unknown domain names .................. 265
Command reference ......................................................................................... 265
New feature: MVRP ............................................................................................ 266
Configuring MVRP .......................................................................................... 266
Command reference ......................................................................................... 266
New feature: Enabling sending ICMPv6 redirect messages ............................ 266
Enabling sending ICMPv6 redirect messages ................................................. 266
Command reference ......................................................................................... 266
New feature: Configuring DHCPv6 snooping to support Option 18 and Option 37 .................................................. 266
Configuring DHCPv6 snooping to support Option 18 and Option 37 ............... 266
Command reference ......................................................................................... 266
New feature: Configuring the DHCPv6 server to assign IPv6 addresses to DHCPv6 clients .................................................. 267
Configuring the DHCPv6 server to assign IPv6 addresses to DHCPv6 clients .................................................. 267
Command reference ......................................................................................... 267
New feature: Specifying a destination server for a private network ................. 267
Specifying a destination server for a private network ....................................... 267
Command reference ......................................................................................... 267
New feature: Configuring the uplink port to permit multiple isolate-user-VLANs .................................................. 268
Configuring the uplink port to permit multiple isolate-user-VLANs ................. 268
Overview ......................................................................................................... 268
Configuration procedure ............................................................................... 268
Configuration example .................................................................................. 270
Command reference ......................................................................................... 272
port isolate-user-vlan trunk promiscuous ....................................................... 272
Modified feature: Displaying information about static CR-LSPs on a node 275
Feature change description ............................................................................. 275
Command changes ......................................................................................... 275
New Feature: Setting the DSCP value for multiple types of protocol packets

Setting the DSCP value for BGP protocol packets
Setting the DSCP value for IPv6 BGP protocol packets
Setting the DSCP value for OSPF protocol packets
Setting the DSCP value for RIP protocol packets
Setting the DSCP value for DHCPv6 protocol packets
Setting the DSCP value for DHCP protocol packets
Setting the DSCP value for DNS protocol packets
Setting the DSCP value for IPv6 DNS protocol packets
Setting the DSCP value for packets sent by the Telnet server
Setting the ToS value for packets sent by the TCP/UDP listening service on the NQA server
Setting the ToS value for packets sent by the TCP/UDP listening service on the NQA server
Setting the DSCP value for packets sent by the FTP server
Setting the DSCP value for outgoing RSVP packets
Setting the DSCP value for outgoing LDP packets
Setting the DSCP value for IPv4 packets sent by the FTP server
Setting the DSCP value for packets sent by the FTP client
Setting the DSCP value for packets sent by the TFTP client
Setting the DSCP value for IPv6 packets sent by the NQA server
Setting the DSCP value for IPv6 PIM protocol packets
Setting the DSCP value for MLD protocol packets
Setting the DSCP value for MLD protocol packets sent by MLD snooping
Setting the DSCP value for PIM protocol packets
Setting the DSCP value for IGMP protocol packets
Setting the DSCP value for IGMP protocol packets sent by IGMP snooping
Setting the DSCP value for IGMP protocol packets
Setting the DSCP value for IPv6 PIM protocol packets
Setting the DSCP value for IPv6 BGP protocol packets
Setting the DSCP value for IPv6 DNS protocol packets
Setting the DSCP value for DNS protocol packets
Setting the DSCP value for SNMP trap packets
Setting the DSCP value for SNMP response packets
Setting the DSCP value for the protocol packets sent to the log host
Setting the DSCP value for VRRP protocol packets
Setting the DSCP value for IGMP protocol packets
Setting the DSCP value for IPv6 packets sent by IGMP snooping
Setting the DSCP value for IPv6 packets sent by IGMP snooping
Setting the DSCP value for DHCP protocol packets
Setting the DSCP value for DHCPv6 protocol packets
Setting the DSCP value for IPv6 packets sent by the NQA server
Setting the DSCP value for packets sent by the Telnet server
Setting the DSCP value for packets sent by the Telnet client

Added commands

dhcp client dscp

dhcp dscp
dns dscp
dns ipv6 dscp
dscp (IGMP view)
dscp (IGMP-Snooping view)
dscp (IPv6 PIM view)
dscp (MLD view)
dscp (MLD-Snooping view)
dscp (MPLS LDP view)
dscp (OSPF view)
dscp (PIM view)
dscp (RIP view)
ftp client dscp
ftp client ipv6 dscp
ftp server dscp
ip http dscp
ipv6 dhcp client dscp
ipv6 dhcp dscp
ipv6 http dscp
mpls rsvp-te dscp
nqa server tos
peer dscp (BGP/BGP-VPN instance view)
peer dscp (IPv6 address family view)
radius dscp ................................................................. 304
radius ipv6 dscp .......................................................... 304
sftp client dscp ......................................................... 305
sftp client ipv6 dscp .................................................... 305
snmp-agent packet response dscp ................................. 306
ssh client dscp .......................................................... 306
ssh client ipv6 dscp ...................................................... 307
ssh server dscp ........................................................ 307
ssh server ipv6 dscp ...................................................... 308
telnet client dscp ......................................................... 308
telnet client ipv6 dscp .................................................... 309
telnet server dscp ........................................................ 309
telnet server ipv6 dscp .................................................... 310
tftp client dscp .......................................................... 310
tftp client ipv6 dscp ...................................................... 311
tos (DHCP operation type view) ..................................... 311
vrrp dscp ................................................................. 312
vrrp ipv6 dscp ........................................................... 312
Modified commands .................................................... 313
info-center loghost ..................................................... 313
ping ipv6 ................................................................. 313
snmp-agent target-host .............................................. 313
tracert ................................................................. 314
tracert ipv6 ............................................................. 314

New feature: Setting a DSCP value for an ISP domain .......... 314
Setting a DSCP value for an ISP domain .......................... 314
Command reference ................................................... 315
dscp (ISP domain view) ............................................... 315
display domain ......................................................... 316

New feature: Delaying the MAC authentication ................... 318
Configuring the MAC authentication delay ......................... 318
Command reference ................................................... 318
mac-authentication timer auth-delay ............................... 318
Modified feature: tunnel bandwidth ................................ 319
Feature change description ......................................... 319
Command changes ..................................................... 319
Modified command: tunnel bandwidth ............................. 319

Modified feature: Establishing a connection to an SCP server to transfer files with the server ......................... 319
Feature change description ......................................... 319
Command changes ..................................................... 319
Modified command: SCP .............................................. 319

Modified feature: Configuring the maximum number of routes in a VPN instance ............................................. 320
Feature change description ......................................... 320
Command changes ..................................................... 320
Modified command: routing-table limit ............................ 320

Modified feature: Configuring PBR to support next hops in VPN instances 320
Feature change description ......................................... 320
Command changes ..................................................... 320
Modified command: apply ip-address default next-hop ........ 320
Modified command: apply ip-address next-hop .................... 321

Modified feature: Commands related to password .................. 321
Feature change description ......................................... 321
Modified feature: Setting the IRF link down report delay .......................... 335

Feature change description .......................................................... 335
Command changes ........................................................................ 335
Modified command: irf link-delay .................................................. 335

A5800_5820X-CMW520-F1803L01 ...................................................... 336

New feature: M6VPE ................................................................. 336
Configuring M6VPE ..................................................................... 336
Command reference .................................................................... 336

New feature: Disabling the USB port ............................................. 336
Configuring the Disabling the USB port ........................................ 336
Command reference .................................................................... 336
usb disable .................................................................................. 336

Removed feature: Setting the password display mode for all local users · 337
Feature change description .......................................................... 337
Removed commands .................................................................... 337
local-user password-display-mode ................................................................. 337
A5800_5820X-CMW520-F1305P01 ............................................................... 338
New feature: Displaying information about the patch package ................. 340
  Displaying information about the patch package ........................................ 340
  Command reference .................................................................................... 340
New feature: Displaying alarm information ................................................. 340
  Displaying alarm information ...................................................................... 340
  Command reference .................................................................................... 340
New feature: Configuring LDP NSR ............................................................... 341
  Configuring LDP NSR ................................................................................ 341
  Command reference .................................................................................... 341
New feature: Configuring protection switching ............................................ 341
  Configuring protection switching ................................................................ 341
  Command reference .................................................................................... 341
New feature: Configuring byte-count or packet-based WFQ queuing ......... 341
  Configuring byte-count or packet-based WFQ queuing: ......................... 341
  Command reference .................................................................................... 341
New feature: Configuring SP+WFQ queuing ............................................... 342
  Configuring SP+WFQ queuing .................................................................. 342
  Command reference .................................................................................... 342
New feature: Configuring the service type as SCP for SSH users ............ 342
  Configuring the service type as SCP for SSH users .................................... 342
  Command reference .................................................................................... 342
New feature: Configuring the device as an SCP client ................................ 342
  Configuring the device as an SCP client ..................................................... 342
  Command reference .................................................................................... 342
New feature: Enabling SSL client weak authentication ............................. 342
  Enabling SSL client weak authentication .................................................. 342
  Command reference .................................................................................... 342
New feature: Configuring a user validity check rule ................................... 343
  Configuring a user validity check rule ......................................................... 343
  Command reference .................................................................................... 343
New feature: SAVI ......................................................................................... 343
  Configuring SAVI ...................................................................................... 343
  Command reference .................................................................................... 343
New feature: Blacklist ................................................................................... 343
  Configuring blacklist .................................................................................. 343
  Command reference .................................................................................... 343
New feature: Configuring BFD to detect the indirect next hop of a static route
........................................................................................................................ 344
  Configuring BFD to detect the indirect next hop of a static route ............... 344
  Command reference .................................................................................... 344
New feature: Enabling OSPF ISPF ................................................................. 344
  Enabling OSPF ISPF .................................................................................. 344
  Command reference .................................................................................... 344
<table>
<thead>
<tr>
<th>New feature</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigning a high priority to IS-IS routes</td>
<td>344</td>
</tr>
<tr>
<td>Configuring IPv6 IS-IS MTR</td>
<td>344</td>
</tr>
<tr>
<td>Enabling 4-byte AS number suppression</td>
<td>345</td>
</tr>
<tr>
<td>Setting the maximum number of IGMP snooping &amp; MLD snooping forwarding entries</td>
<td>345</td>
</tr>
<tr>
<td>Enabling the IGMP snooping &amp; MLD snooping host tracking function</td>
<td>345</td>
</tr>
<tr>
<td>PIM snooping &amp; IPv6 PIM snooping</td>
<td>346</td>
</tr>
<tr>
<td>Setting the maximum number of forwarding entries for multicast VLANs</td>
<td>346</td>
</tr>
<tr>
<td>Setting the maximum number of forwarding entries for IPv6 multicast VLANs</td>
<td>347</td>
</tr>
<tr>
<td>Enabling multicast optimization</td>
<td>347</td>
</tr>
<tr>
<td>Enabling the IGMP &amp; MLD host tracking function</td>
<td>347</td>
</tr>
<tr>
<td>Configuring a password for MD5 authentication used by both MSDP peers to establish a TCP connection</td>
<td>348</td>
</tr>
<tr>
<td>BGP MDT</td>
<td>348</td>
</tr>
<tr>
<td>Configuring IPv6 multicast routing and forwarding in a VPN instance</td>
<td>348</td>
</tr>
</tbody>
</table>
New feature: IPv6 PIM support for VPNs .................................................. 349
  Configuring IPv6 PIM in a VPN instance ........................................... 349
  Command reference ........................................................................ 349
New feature: SNMP support for IPv6 ACLs ......................................... 349
  Using IPv6 ACLs with SNMP ........................................................... 349
  Command reference ........................................................................ 349
New feature: SNMP PIM traps .............................................................. 349
  Enabling SNMP PIM traps globally ................................................... 349
  Command reference ........................................................................ 349
New feature: Configuring the source IP address of sFlow packets ........ 350
  Configuring the source IP address of sFlow packets ......................... 350
  Command reference ........................................................................ 350
New feature: Bulk interface configuration ........................................... 350
  Bulk interface configuration ............................................................. 350
  Command reference ........................................................................ 350
New feature: Configuring a Layer 3 aggregation group ....................... 350
  Configuring a Layer 3 aggregation group ......................................... 350
  Command reference ........................................................................ 350
New feature: Configuring the MTU of a Layer 3 aggregate interface ...... 351
  Configuring the MTU of a Layer 3 aggregate interface ...................... 351
  Command reference ........................................................................ 351
New feature: Assigning a port an aggregation priority ......................... 351
  Assigning a port an aggregation priority .......................................... 351
  Command reference ........................................................................ 351
New feature: Configuring MPLS labels as the load sharing criteria for a link aggregation group ............................................................. 351
  Configuring MPLS labels as the load sharing criteria for a link aggregation group ............................................................. 351
  Command reference ........................................................................ 351
New feature: Setting the guest attribute for a user group ...................... 352
  Setting the guest attribute for a user group ....................................... 352
  Command reference ........................................................................ 352
New feature: Setting the validity time of a local user ........................... 352
  Setting the validity time of a local user ............................................ 352
  Command reference ........................................................................ 352
New feature: Specifying the local user as a guest or guest manager ....... 352
  Specifying the local user as a guest or guest manager ....................... 352
  Command reference ........................................................................ 352
New feature: Authorizing a local user to use the Web service ................ 353
  Authorizing a local user to use the Web service ................................ 353
  Command reference ........................................................................ 353
New feature: Configuring status detection for RADIUS authentication/authorization servers ............................................................. 353
  Configuring status detection for RADIUS authentication/authorization servers ............................................................. 353
  Command reference ........................................................................ 353
New feature: Specifying the VPN for the source IPv6 address of outgoing RADIUS packets

Specifying the VPN for the source IPv6 address of outgoing RADIUS packets
Command reference

New feature: Specifying the VPN for the IPv6 address of a RADIUS server

Specifying the VPN for the IPv6 address of a RADIUS server
Command reference

New feature: Configuring 802.1X critical VLAN

Configuring 802.1X critical VLAN
Command reference

New feature: Specifying supported domain name delimiters

Specifying supported domain name delimiters
Command reference

New feature: Configuring an 802.1X VLAN group

Configuring an 802.1X VLAN group
Command reference

New feature: Configuring a MAC authentication critical VLAN

Configuring a MAC authentication critical VLAN
Command reference

New feature: Enabling inactivity aging

Enabling inactivity aging
Command reference

New feature: Enabling the dynamic secure MAC function

Enabling the dynamic secure MAC function
Command reference

New feature: PVST

Configuring PVST
Command reference

New feature: Configuring an MTU for a VLAN interface

Configuring an MTU for a VLAN interface
Command reference

New feature: Enabling LLDP to automatically discover IP phones

Enabling LLDP to automatically discover IP phones
Command reference

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
Command reference

Modified command: display lldp local-information
Modified command: display lldp neighbor-information

New feature: Configuring the VF tracking function to monitor an AVF

Configuring the VF tracking function to monitor an AVF
Command reference

New feature: Enabling client offline detection

Enabling client offline detection
New feature: Configuring DHCP snooping support for sub-option 9 in Option 82

New feature: Specifying the source interface for DNS packets

New feature: Configuring TCP path MTU discovery

New feature: Configuring the interface as an uplink interface and disabling it from learning ND snooping entries

New feature: Specifying the AFTR address

New feature: Enabling GRE keepalive and setting the keepalive parameters

Modified feature: Configuring the password for switching from the current user privilege level to a higher one

Modified feature: Displaying files and folders

Modified feature: Activating/stopping/deleting/confirming patches

Modified feature: Loading/installing and running patches
Modified feature: Configuring IP source guard .......................................................... 373
Feature change description ..................................................................................... 373
Command changes .................................................................................................. 373
Modified command: display ip source binding ....................................................... 373
Modified command: display ipv6 source binding ..................................................... 373
Modified command: ip source binding (system view) ............................................. 374
Modified command: ipv6 source binding (system view) ........................................ 374
Modified command: ip source binding (interface view) ......................................... 374
Modified command: ipv6 source binding (interface view) ...................................... 375
Modified command: ip verify source ..................................................................... 375
Modified command: ipv6 verify source ................................................................ 376

Modified feature: Configuring the maximum number of routes for the VPN instance .......................................................... 367
Feature change description ..................................................................................... 367
Command changes .................................................................................................. 367
Modified command: routing-table limit ................................................................. 367

Modified feature: Configuring SVC MPLS L2VPN .................................................. 367
Feature change description ..................................................................................... 367
Command changes .................................................................................................. 367
Modified command: mpls l2vc ............................................................................. 367

Modified feature: Configuring traffic policing ....................................................... 370
Feature change description ..................................................................................... 370
Command changes .................................................................................................. 370
Modified command: car ......................................................................................... 370

Modified feature: Configuring aggregate CAR .................................................... 371
Feature change description ..................................................................................... 371
Command changes .................................................................................................. 371
Modified command: qos car aggregative .............................................................. 371

Modified feature: Configuring hierarchical CAR .................................................. 371
Feature change description ..................................................................................... 371
Command changes .................................................................................................. 371
Modified command: qos car aggregative .............................................................. 371

Modified feature: Configuring the idle cut function .............................................. 372
Feature change description ..................................................................................... 372
Command changes .................................................................................................. 372
Modified command: idle-cut enable ..................................................................... 372

Modified feature: Setting the quiet timer for RADIUS servers .............................. 372
Feature change description ..................................................................................... 372
Command changes .................................................................................................. 372
Modified command: timer quiet .......................................................................... 372

Modified feature: Specifying a community list name to match BGP VPNv4 routing information .......................................................... 368
Feature change description ..................................................................................... 368
Command changes .................................................................................................. 368
Modified command: display bgp vpnv4 all routing-table .................................... 368
Modified command: display bgp vpnv4 route-distinguisher routing-table .......... 369
Modified command: display bgp vpnv4 vpn-instance routing-table .................... 369

Modified feature: LACP MAD ............................................................................ 366
Feature change description ..................................................................................... 366
Command changes .................................................................................................. 366
Modified command: mad enable ........................................................................... 366

Modified feature: Setting the quiet timer for RADIUS servers .............................. 372
Feature change description ..................................................................................... 372
Command changes .................................................................................................. 372
Modified command: timer quiet .......................................................................... 372
Modified feature: Configuring the ABR to advertise a default route to the stub area ........................................ 377

Feature change description ......................................................... 377
Command changes ................................................................ 377

Modified command: **stub** .................................................. 377

Modified feature: Setting BGP SoO extended community attribute for BGP routing information ........................................ 378

Feature change description ......................................................... 378
Command changes ................................................................ 378

Modified command: apply extcommunity ....................................... 378
Modified command: ip extcommunity-list ........................................ 378

Modified feature: RIPng IPsec command ........................................ 378

Feature change description ......................................................... 378
Command changes ................................................................ 379

Modified command: ipsec-policy ................................................... 379

Modified feature: OSPFv3 IPsec command ........................................ 379

Feature change description ......................................................... 379
Command changes ................................................................ 379

Modified command: ipsec-policy ................................................... 379

Modified feature: Setting the register suppression time for PIM/IPv6 PIM ......................................................... 379

Feature change description ......................................................... 379
Command changes ................................................................ 380

Modified command: register-suppression-timeout ................................ 380

Modified feature: Setting the maximum delay for sending a hello message in PIM/IPv6 PIM ......................................................... 380

Feature change description ......................................................... 380
Command changes ................................................................ 380

Modified command: pim triggered-hello-delay .................................... 380
Modified command: pim ipv6 triggered-hello-delay ................................ 380

Modified feature: Displaying MBGP&IPv6 MBGP routing information matching the specified BGP community list ........................................ 381

Feature change description ......................................................... 381
Command changes ................................................................ 381

Modified command: display bgp multicast routing-table community-list ......................................................... 381
Modified command: display bgp ipv6 multicast routing-table community-list ......................................................... 381

Modified feature: Support of voice VLAN for 128 OUI addresses .......... 382

Feature change description ......................................................... 382
Command changes ................................................................ 382

Modified command: voice vlan mac-address ....................................... 382

Modified feature: Configuring the protected VLANs for the RRPP domain ......................................................... 382

Feature change description ......................................................... 382
Command changes ................................................................ 382

Modified command: protected-vlan ................................................... 382

Modified feature: Configuring the protected VLANs for a smart link group ......................................................... 383

Feature change description ......................................................... 383
Command changes ................................................................ 383
This release has the following changes:

- New feature: ITU channel number for a transceiver module

**New feature: ITU channel number for a transceiver module**

Specifying an ITU channel number for a transceiver module

This feature is supported only on the HPE X130 10G SFP+ LC LH80 Tunable Transceiver (JL250A) module.

ITU numbers and identifies fiber signals by wavelength and frequency. A transceiver module sends signals of a specific wavelength and frequency based on the specified ITU channel number.

This feature is required in dense wavelength division multiplexing scenarios.

The ITU channel number setting is saved in a register on the transceiver module. It is not saved to the configuration file.

To specify an ITU channel number for a transceiver module:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>itu-channel channel-number</td>
<td>By default, the ITU channel number is 1.</td>
</tr>
</tbody>
</table>

**Command reference**

**New command: itu-channel**

Use **itu-channel** to set the ITU channel number for a transceiver module.

Use **undo itu-channel** to restore the default.

**Syntax**

itu-channel  
undo itu-channel

**Default**

The ITU channel number is 1.

**Views**

Ethernet interface view

**Default command level**

2: System level
Parameters

*channel-number*: Specifies the ITU channel number.

Usage guidelines

This command is supported only on the HPE X130 10G SFP+ LC LH80 Tunable Transceiver (JL250A) module.

The ITU channel number is saved in a register on the transceiver module. It is not saved to the configuration file.

Examples

# Set the ITU channel number to 2 for the transceiver module on Ten-GigabitEthernet 1/0/50.

```plaintext
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/50
[Sysname-Ten-GigabitEthernet1/0/50] itu-channel 2
Changing the channel number causes the service to be down for a while. Continue? [Y/N]:Y
```

New command: display transceiver itu-channel

Use `display transceiver itu-channel` to display ITU channel information for transceiver modules.

Syntax

```plaintext
display transceiver itu-channel interface [ interface-type interface-number ] [ supported-channel ] | [ begin | exclude | include ] regular-expression
```

Views

Any view

Default command level

2: System level

Parameters

*interface* [ *interface-type interface-number* ]: Specifies an interface by its type and number. If no interface is specified, this command displays ITU channel information for the transceiver modules on all interfaces.

*supported channel*: Specifies ITU channels supported on the interface. If this keyword is not specified, the command displays the ITU channel that is being used on the interface.

*: 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 on the HPE X130 10G SFP+ LC LH80 Tunable Transceiver (JL250A) module.

Examples

# Display ITU channels used by the transceiver module on Ten-GigabitEthernet 1/0/50.

```plaintext
<Sysname> display transceiver itu-channel interface ten-gigabitethernet 1/0/50
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Channel</th>
<th>Wavelength(nm)</th>
<th>Frequency(THz)</th>
</tr>
</thead>
<tbody>
<tr>
<td>XGE1/0/50</td>
<td>1</td>
<td>1566.72</td>
<td>191.35</td>
</tr>
</tbody>
</table>
Display ITU channels supported by the transceiver module on Ten-GigabitEthernet 1/0/50.

```
<Sysname> display transceiver itu-channel interface ten-gigabitethernet 1/0/50
```

ITU channel settings supported on Ten-GigabitEthernet1/0/50:

<table>
<thead>
<tr>
<th>Channel</th>
<th>Wavelength(nm)</th>
<th>Frequency(THz)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1566.72</td>
<td>191.35</td>
</tr>
<tr>
<td>2</td>
<td>1566.31</td>
<td>191.40</td>
</tr>
<tr>
<td>3</td>
<td>1565.90</td>
<td>191.45</td>
</tr>
<tr>
<td>4</td>
<td>1565.50</td>
<td>191.50</td>
</tr>
<tr>
<td>5</td>
<td>1565.09</td>
<td>191.55</td>
</tr>
<tr>
<td>6</td>
<td>1564.68</td>
<td>191.60</td>
</tr>
<tr>
<td>7</td>
<td>1564.27</td>
<td>191.65</td>
</tr>
<tr>
<td>8</td>
<td>1563.86</td>
<td>191.70</td>
</tr>
</tbody>
</table>

Table 1 Command output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| WaveLength(nm) | Wavelength of the channel in nm, accurate to 0.01 nm. This field displays a hyphen (-) in the following situations:  
• No transceiver module is installed on the interface.  
• The transceiver module does not support specifying an ITU channel number.  
• The command failed to obtain the ITU channel information.  
• The device does not support the ITU channel number stored on the transceiver module. |
| Frequency(THz) | Frequency of the channel in THz, accurate to 0.01 THz. This field displays a hyphen (-) in the following situations:  
• No transceiver module is installed on the interface.  
• The transceiver module does not support specifying an ITU channel number.  
• The command failed to obtain the ITU channel information.  
• The device does not support the ITU channel number stored on the transceiver module. |

Modified command: display transceiver alarm

Syntax

```
display transceiver alarm interface [ interface-type interface-number ] [ | { begin | exclude | include } regular-expression ]
```

Views

Any view

Change description

The following alarm messages were added for the HPE X130 10G SFP+ LC LH80 Tunable Transceiver (JL250A) module:

• TEC error
• Wavelength unlocked
• Tx is not ready due to tuning
• Requested ITU channel number is invalid
• Received an ITU channel number request
• Tx dither not supported

Modified command: display transceiver diagnosis

Syntax

display transceiver diagnosis interface [ interface-type interface-number ] [ | { begin | exclude | include } regular-expression ]

Views

Any view

Change description

The following fields were added to the command output: Wave.error and Freq.error for the HPE X130 10G SFP+ LC LH80 Tunable Transceiver (JL250A) module.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wave.error</td>
<td>Wavelength offset in nm, accurate to 0.001 nm.</td>
</tr>
<tr>
<td>Freq.error</td>
<td>Frequency offset in GHz, accurate to 0.1 GHz.</td>
</tr>
</tbody>
</table>
This release has the following changes:

- New feature: Transparent transmission for protocol packets in a VPN

**New feature: Transparent transmission for protocol packets in a VPN**

**Enabling transparent transmission for protocol packets in a VPN**

In an MPLS L2VPN network, for CEs on two ends to establish neighborship, you can enable this feature on the customer-facing interface on the PE. Then, LLDP, STP, or LACP protocol packets can be transparently transmitted. When the PE receives these protocol packets from a local CE, the PE will encapsulate the packets with VC labels and transparently transmits packets to the peer CE. Then, the two CEs can establish neighborship. For more information about MPLS L2VPN and VC labels, see MPLS L2VPN in *MPLS Configuration Guide*.

When this feature is not enabled, PEs cannot transparently transmit protocol packets from local CEs. Instead, the PEs terminate the protocol packets.

To enable this feature on an interface, you must disable the protocol whose packets need to be transparently transmitted.

For LACP protocol packets to be transparently transmitted successfully, you must enable transparent transmission for protocol packets in a VPN on both the incoming interface and outgoing interface of the protocol packets on the PE.

To enable transparent transmission for protocol packets in a VPN:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable transparent transmission for protocol packets in a VPN.</td>
<td>bpdu-tunnel l2vpn-transport</td>
</tr>
</tbody>
</table>

**Command reference**

*bapdu-tunnel l2vpn-transport*

*Use* **bpdu-tunnel l2vpn-transport** *to enable transparent transmission for protocol packets in a VPN.*

*Use* **undo bpdu-tunnel l2vpn-transport** *to disable transparent transmission for protocol packets in a VPN.*

**Syntax**

bpdu-tunnel l2vpn-transport
undo bpdu-tunnel l2vpn-transport

Default

Transparent transmission for protocol packets in a VPN is disabled.

Views

Layer 2 Ethernet interface view

Default command level

2: System level

Usage guidelines

In an MPLS L2VPN network, for CEs on two ends to establish neighborship, you can enable this feature on the customer-facing interface on the PE. Then, LLDP, STP, or LACP protocol packets can be transparently transmitted. When the PE receives these protocol packets from the local CE, the PE will add VC labels to the packets and transparently transmits packets to the peer CE. Then, the two CEs can establish neighborship. For more information about MPLS L2VPN and VC labels, see MPLS L2VPN in *MPLS Configuration Guide*.

When this feature is not enabled, PEs cannot transparently transmit protocol packets from the local CEs. Instead, the PEs terminate the protocol packets.

To enable this feature on an interface, you must disable the protocol whose packets need to be transparently transmitted.

For LACP protocol packets to be successfully transparently transmitted, you must enable transparent transmit for protocol packets in a VPN on both the incoming interface and outgoing interface of the protocol packets on the PE.

Examples

# Enable transparent transmission for protocol packets in a VPN on GigabitEthernet 1/0/1.

```
<Sysname> system
<Sysname> interface gigabitethernet 1/0/1
<Sysname-Gigabitethernet1/0/1] bpdu-tunnel l2vpn-transport
```
This release has no feature changes.
A5800_5820X-CMW520-R1810P10

This release has no feature changes.
This release has the following changes:

- **Modified feature: NTP support for ACL**

**Modified feature: NTP support for ACL**

Feature change description

Before modification: You cannot use an ACL to specify the peer device that can use the authentication ID.

After modification: You can use an ACL to specify the peer device that can use the authentication ID.

**Modified command: ntp-service authentication-keyid**

**Old syntax**

```plaintext
tcp-service authentication-keyid keyid authentication-mode md5 { cipher | simple } value
```

**New syntax**

```plaintext
tcp-service authentication-keyid keyid authentication-mode md5 { cipher | simple } value [ acl ipv4-acl-number ] *
```

**Views**

System view

**Change description**

The `acl ipv4-acl-number` and `ipv6 acl ipv6-acl-number` options were added to the command.

`acl ipv4-acl-number`: Specifies an IPv4 basic ACL by its number in the range of 2000 to 2999. Only the devices permitted by the ACL can use the authentication ID for authentication.
This release has no feature changes.
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
- **Modified feature:** Configuring the description of a VLAN

**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`, `no-autoconfig`, `off-link`, 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><strong>system-view</strong></td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td><strong>interface interface-type interface-number</strong></td>
</tr>
<tr>
<td>3.</td>
<td>Configure the default settings for prefixes advertised in RA messages.</td>
<td><code>ipv6 nd ra prefix default</code> [ valid-lifetime preferred-lifetime [ no-autoconfig</td>
</tr>
</tbody>
</table>

**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, no-autoconfig, off-link, and no-advertise) is configured in the `ipv6 nd ra prefix` command, the prefix uses the default settings.

Examples

```bash
# 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, no-autoconfig, off-link, 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

```bash
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

```bash
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 you use the `ipv6 nd ra prefix` command to configure the prefix information, you must configure parameters `valid-lifetime`, `preferred-lifetime`, `no-autoconfig`, `off-link`, and `no-advertise` for the prefix.

After modification: If you do not specify parameters `valid-lifetime`, `preferred-lifetime`, `no-autoconfig`, `off-link`, and `no-advertise`, the prefix uses the default settings configured by using the `ipv6 nd ra prefix default` command.

Modified feature: Configuring the description of a VLAN

Feature change description

From this release, the description of a VLAN was modified.

Command changes

Modified command: description

Syntax

```
description text
undo description
```

Views

VLAN view

Change description

Before modification: For a VLAN, this is a string of 1 to 32 characters.

After modification: For a VLAN, this is a string of 1 to 80 characters.
This release has the following changes:

- **Modified feature: Displaying VLAN interface information**

**Modified feature: Displaying VLAN interface information**

**Feature change description**

From this release, traffic statistics for VLAN interfaces are not displayed.

**Command changes**

**Modified command: display interface vlan-interface**

**Syntax**

```
display interface [ vlan-interface ] [ brief [ down ] ] [ | { begin | exclude | include } regular-expression ]
```

```
display interface vlan-interface vlan-interface-id [ brief ] [ | { begin | exclude | include } regular-expression ]
```

**Views**

Any view

**Change description**

The following fields were deleted from the command output:

- Last clearing of counters: Never
- Last 300 seconds input: 0 bytes/sec 0 packets/sec
- Last 300 seconds output: 0 bytes/sec 0 packets/sec
- 0 packets input, 0 bytes, 0 drops
- 0 packets output, 0 bytes, 0 drops
This release has the following changes:

- **Modified feature: Member device brand name**

## Modified feature: Member device brand name

### Feature change description

The `hp` brand name changed to `hpe`.

### Command changes

**Modified command: brand**

**Old syntax**

```
brand { hp | h3c } [ slot slot-number ]
```

**New syntax**

```
brand { hpe | h3c } [ slot slot-number ]
```

### Views

**User view**

**Change description**

Before modification: The brand name of a member device could be `hp` or `h3c`.

After modification: The brand name of a member device can be `hpe` or `h3c`. 
This release has the following changes:

- New feature: Route summarization on an ASBR

**New feature: Route summarization on an ASBR**

**Configuring route summarization on an ASBR**

Perform this task to enable an ASBR to summarize external routes within the specified address range into a single route.

An ASBR can summarize routes in the following LSAs:

- Type-5 LSAs.
- Type-7 LSAs in an NSSA area.
- Type-5 LSAs translated by the ASBR (also an ABR) from Type-7 LSAs in an NSSA area.

If the ASBR (ABR) is not a translator, it cannot summarize routes in Type-5 LSAs translated from Type-7 LSAs.

To configure route summarization on an ASBR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPFv3 view.</td>
<td>ospfv3 [ process-id ]</td>
</tr>
<tr>
<td>3.</td>
<td>Configure route summarization on an ASBR.</td>
<td>asbr-summary ipv6-address prefix-length [ cost cost-value</td>
</tr>
</tbody>
</table>

**Command reference**

**asbr-summary**

Use **asbr-summary** to configure route summarization on an ASBR.

Use **undo asbr-summary** to remove the configuration.

**Syntax**

```plaintext
asbr-summary ipv6-address prefix-length [ cost cost-value | not-advertise ] *
undo asbr-summary ipv6-address prefix-length
```

**Default**

Route summarization is not configured on an ASBR.

**Views**

OSPFv3 view

**Default command level**

2: System level
Parameters

- **ipv6-address**: Specifies the destination IPv6 address of the summary route.
- **prefix-length**: Specifies the prefix length in the range of 0 to 128.
- **cost cost-value**: Specifies the cost of the summary route, in the range of 1 to 16777214. If you do not specify this option, the largest cost among the summarized routes applies. If the routes in Type-5 LSAs translated from Type-7 LSAs are Type-2 external routes, the largest cost among the summarized routes plus 1 applies.
- **not-advertise**: Disables advertising the summary route. If you do not specify this keyword, the command advertises the route.

Usage guidelines

An ASBR can summarize routes in the following LSAs:

- Type-5 LSAs.
- Type-7 LSAs in an NSSA area.
- Type-5 LSAs translated by the ASBR (also an ABR) from Type-7 LSAs in an NSSA area.
  - If the ASBR (ABR) is not a translator, it cannot summarize routes in Type-5 LSAs translated from Type-7 LSAs.

To enable ASBR to advertise specific routes that have been summarized, use the `undo asbr-summary` command.

Examples

```
# Configure a summary route 2000::/16 and specify a cost of 100 for the summary route.
<Sysname> system-view
<Sysname> ospfv3 1
<Sysname-ospfv3-1] asbr-summary 2000:: 16 cost 100
```

```
display ospfv3 asbr-summary
```

Use `display ospfv3 asbr-summary` to display ASBR summary route information.

Syntax

```
display ospfv3 [ process-id ] asbr-summary [ ipv6-address prefix-length ] [ verbose ]
```

Views

Any view

Default command level

1: Monitor level

Parameters

- **process-id**: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays information about ASBR summary routes for all OSPFv3 processes.
- **ipv6-address prefix-length**: Specifies an IPv6 address. The **ipv6-address** argument specifies an IPv6 prefix. The **prefix-length** argument specifies a prefix length in the range of 0 to 128. If you do not specify this argument, the command displays information about all ASBR summary routes.
- **verbose**: Displays detailed ASBR summary route information. If you do not specify this keyword, the command displays brief ASBR summary route information.

Examples

```
# Display brief ASBR summary route information in OSPFv3 process 1.
<Sysname> display ospfv3 1 asbr-summary
```
OSPFv3 Process 1 with Router ID (2.2.2.2) (Process 1)

Total summary addresses: 1

Prefix : 1000:4::/32
Status : Advertise
NULL0 : Active
Cost : 1 (Configured)
Routes count: 2

Table 3 Command output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total summary addresses</td>
<td>Total number of summary routes.</td>
</tr>
<tr>
<td>Prefix</td>
<td>Prefix and prefix length of the summary route.</td>
</tr>
<tr>
<td>Status</td>
<td>Advertisement status of the summary route:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Advertise</strong>—The summary route has been advertised.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Not-advertise</strong>—The summary route has not been advertised.</td>
</tr>
<tr>
<td>NULL0</td>
<td>Status of the Null 0 route:</td>
</tr>
<tr>
<td></td>
<td>• Active.</td>
</tr>
<tr>
<td></td>
<td>• Inactive.</td>
</tr>
<tr>
<td>Cost</td>
<td>Cost of the summary route:</td>
</tr>
<tr>
<td></td>
<td>• Configured.</td>
</tr>
<tr>
<td></td>
<td>• Not configured.</td>
</tr>
<tr>
<td>Routes count</td>
<td>Number of summarized routes.</td>
</tr>
</tbody>
</table>

# Display detailed ASBR summary route information in OSPFv3 process 1.

<Sysname> display ospfv3 1 asbr-summary verbose

OSPFv3 Router with ID (2.2.2.2) (Process 1)

Total summary addresses: 1

Prefix : 1000:4::/32
Status : Advertise
NULL0 : Active
Cost : 1 (Configured)
Routes count: 2

<table>
<thead>
<tr>
<th>Destination</th>
<th>Protocol</th>
<th>Process</th>
<th>Type</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000:4:10:3::/96</td>
<td>Static</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>1000:4:11:3::/96</td>
<td>Static</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 4 Command output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Prefix and prefix length of the summarized route.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Routing protocol from which the route was redistributed.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Process</td>
<td>Process of the routing protocol from which the route was redistributed.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of the summarized route.</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric of the summarized route.</td>
</tr>
</tbody>
</table>
This release has the following changes:

- New feature: Disabling reactivation for edge ports shut down by BPDU guard
- Modified feature: Specifying multiple secondary HWTACACS servers
- Modified feature: Disabling advertising prefix information in RA messages

**New feature: Disabling reactivation for edge ports shut down by BPDU guard**

Disabling the device to reactivate edge ports shut down by BPDU guard

A device enabled with BPDU guard shuts down edge ports that have received configuration BPDUs and notifies the NMS of the shutdown event. After a port status detection interval, the device reactivates the shutdown ports. This task disables the device to reactivate the edge ports that are shut down by BPDU guard. For more information about the port status detection interval, see device management configuration in *Fundamentals Configuration Guide*.

This feature takes effect only on edge ports that are shut down by BPDU guard after the feature is configured.

To disable the device to reactivate edge ports shut down by BPDU guard:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Disable the device to reactivate edge ports shut down by BPDU guard.</td>
<td>stp port shutdown permanent</td>
</tr>
</tbody>
</table>

**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

Usage guidelines

This command takes effect only on edge ports that are shut down by BPDU guard after the command is executed.

You can use the `shutdown-interval time` command to set the port status detection interval after which the device reactivates the shutdown ports. For information about the `shutdown-interval time` command, see Fundamentals Command Reference.

Examples

```
# Disable a device to reactivate edge ports shut down by BPDU guard.
<Sysname> system-view
 [Sysname] stp port shutdown permanent
```

Modified feature: Specifying multiple secondary HWTACACS servers

Feature change description

In this release, you can specify one primary HWTACACS server and up to 16 secondary HWTACACS servers in the same HWTACACS scheme. When the primary HWTACACS server is unreachable, the device uses a secondary HWTACACS server to process AAA requests.

You can configure a shared key for each HWTACACS server, primary or secondary. The device uses the shared keys to ensure secure communication with HWTACACS servers.

Command changes

Modified command: primary accounting

Old syntax

```
primary accounting ip-address [ port-number | vpn-instance vpn-instance-name ] *
```

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**

```plaintext```
secondary accounting ip-address [ port-number | vpn-instance vpn-instance-name ] *
undo secondary accounting
```

**New syntax**

```plaintext```
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, upper case 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.
  o 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.
  o 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: 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.
This release has the following changes:

- New feature: VLAN-specific DHCP snooping

**New feature: VLAN-specific DHCP snooping**

**Configuring DHCP snooping in a VLAN**

Perform this task to configure DHCP snooping features, including DHCP snooping entry recording and trusted port, in a VLAN.

For the DHCP snooping features to take effect in a VLAN, you must enable DHCP snooping for all VLANs.

To configure DHCP snooping in a VLAN:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable DHCP snooping.</td>
<td>dhcp-snooping</td>
</tr>
<tr>
<td>3.</td>
<td>Enable DHCP snooping for all VLANs.</td>
<td>dhcp-snooping vlan enable</td>
</tr>
<tr>
<td>4.</td>
<td>Enter VLAN view.</td>
<td>vlan vlan-id</td>
</tr>
<tr>
<td>5.</td>
<td>Enable the recording of DHCP snooping entries.</td>
<td>dhcp-snooping binding record</td>
</tr>
<tr>
<td>6.</td>
<td>Configure DHCP snooping trusted ports.</td>
<td>dhcp-snooping trust interface { interface-type interface-number }&amp;&lt;1-8&gt;</td>
</tr>
</tbody>
</table>

**Command reference**

**dhcp-snooping binding record**

Use `dhcp-snooping binding record` to enable the recording of DHCP snooping entries in a VLAN.

Use `undo dhcp-snooping binding record` to disable the recording of DHCP snooping entries in a VLAN.

**Syntax**

```
dhcp-snooping binding record
undo dhcp-snooping binding record
```

**Default**

DHCP snooping entry recording is disabled in a VLAN.

**Views**

VLAN view
Default command level
2: System level

Examples

# Enable the recording of DHCP snooping entries in VLAN 1.
<Sysname> system-view
<Sysname> vlan 1
<Sysname-vlan1> dhcp-snooping binding record

dhcp-snooping trust interface

Use dhcp-snooping trust interface to configure DHCP snooping trusted ports in a VLAN.
Use undo dhcp-snooping trust interface to remove DHCP snooping trusted ports from a VLAN.

Syntax

dhcp-snooping trust interface { interface-type interface-number }&<1-8>
undo dhcp-snooping trust interface { { interface-type interface-number }&<1-8> }

Default
No DHCP snooping trusted port is configured in a VLAN.

Views
VLAN view

Default command level
2: System level

Parameters

{ interface-type interface-number }&<1-8>: Specifies a space-separated list of up to eight interfaces. The interface-type interface-number argument specifies an interface by its type and number.

Usage guidelines

You can configure a maximum of eight DHCP snooping trusted ports in a VLAN. If you configure more than eight trusted ports by using this command multiple times, only the first eight trusted ports take effect.

The specified interfaces must belong to the VLAN. Otherwise, the configuration does not take effect.

This command is configured in VLAN view and takes effect in the VLAN. The dhcp-snooping trust command is configured in interface view and takes effect on the interface.

Examples

# Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as DHCP snooping trusted ports in VLAN 1.
<Sysname> system-view
<Sysname> vlan 1
<Sysname-vlan1> dhcp-snooping trust interface gigabitethernet 1/0/1 gigabitethernet 1/0/2

dhcp-snooping vlan enable

Use dhcp-snooping vlan enable to enable DHCP snooping for all VLANs.
Use undo dhcp-snooping vlan enable to disable DHCP snooping for all VLANs.

Syntax

dhcp-snooping vlan enable
undo dhcp-snooping vlan enable

Default
DHCP snooping is disabled for all VLANs.

Views
System view

Default command level
2: System level

Examples
# Enable DHCP snooping for all VLANs.
<Sysname> system-view
[Sysname] dhcp-snooping
[Sysname] dhcp-snooping vlan enable
This release has added the link aggregation management VLANs and management port feature.

**New feature: link aggregation management VLANs and management port**

Specifying link aggregation management VLANs and management port

For an aggregation group to forward traffic of some VLANs through a specific port, specify the VLANs as management VLANs and the port as a management port.

To specify link aggregation management VLANs and management port for an aggregation group:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>link-aggregation management-vlan vlan-id1 [ vlan-id2 ]</td>
<td>By default, no link aggregation management VLAN is specified. You can specify a maximum of two management VLANs. If you execute this command multiple times, the most recent configuration takes effect.</td>
</tr>
<tr>
<td>3.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>4.</td>
<td>link-aggregation management-port</td>
<td>By default, a port does not act as a management port in its aggregation group. The management port must be a Selected port.</td>
</tr>
</tbody>
</table>

Command reference

**link-aggregation management-vlan**

Use `link-aggregation management-vlan` to specify link aggregation management VLANs.

Use `undo link-aggregation management-vlan` to remove link aggregation management VLANs.

**Syntax**

- `link-aggregation management-vlan vlan-id1 [ vlan-id2 ]`
- `undo link-aggregation management-vlan [ vlan-id1 [ vlan-id2 ] ]`

**Default**

No link aggregation management VLAN is specified.

**Views**

System view
Default command level
3: Manage level

Parameters

- `vlan-id1`: Specifies a management VLAN by its ID in the range of 1 to 4094.
- `vlan-id2`: Specifies another management VLAN by its ID in the range of 1 to 4094.

Usage guidelines
You can specify a maximum of two management VLANs. If you execute this command multiple times, the most recent configuration takes effect.

Examples

```
# Specify VLAN 2 and VLAN 3 as link aggregation management VLANs.
<Sysname> system-view
[Sysname] link-aggregation management-vlan 2 3
```

link-aggregation management-port

Use `link-aggregation management-port` to configure a management port for an aggregation group.

Use `undo link-aggregation management-port` to restore the default.

Syntax

```
link-aggregation management-port
undo link-aggregation management-port
```

Default
A port does not act as a management port.

Views
Layer 2 Ethernet interface view

Default command level
2: System level

Usage guidelines
This command takes effect only when you configure a Selected port as a management port. You can configure only one management port for an aggregation group.

Examples

```
# Configure GigabitEthernet 1/0/1 as a management port.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] link-aggregation management-port
```
This release has no feature changes.
This release has the following changes:

- New feature: Disabling SSL 3.0
- Modified feature: DLDP hybrid shutdown mode
- Modified feature: Configuring MTU on a Layer 3 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Disable SSL 3.0 on the device.</td>
<td>ssl version ssl3.0 disable</td>
</tr>
</tbody>
</table>

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.
Modified feature: DLDP hybrid shutdown mode

Feature change description

In hybrid shutdown mode, DLDP automatically shuts down a port when detecting a unidirectional link. The port requires manual startup when the link becomes bidirectional.

The hybrid shutdown mode can resolve the following problems of the auto and manual shutdown modes:

- **Auto shutdown mode**—Frequent port state changes typically in an unstable network.
- **Manual shutdown mode**—The faulty port cannot be immediately shut down.

Command changes

Modified command: dldp unidirectional-shutdown

Old syntax

```
dldp unidirectional-shutdown { auto | manual }
undo dldp unidirectional-shutdown
```

New syntax

```
dldp unidirectional-shutdown { auto | hybrid | manual }
undo dldp unidirectional-shutdown
```

Views

- System view

Change description

After modification, the hybrid mode is supported. In hybrid mode, DLDP automatically shuts down the faulty port when detecting a unidirectional link. The port requires manual startup when the link becomes bidirectional.

Modified feature: Configuring MTU on a Layer 3 interface

Feature change description

The maximum value of the Maximum Transmission Unit (MTU) was modified from 1500 to 9216.

Command changes

Modified command: mtu

Syntax

```
mtu size
```

Views

- Layer 3 Ethernet interface view, Layer 3 aggregate interface view, VLAN interface view
Change description

Before modification: The value range for the size argument is 46 to 1500.
After modification: The value range for the size argument is 46 to 9216.
This release has the following changes:
- New feature: SNMP notifications for PVST topology changes
- New feature: Applicable scope of packet filtering on a VLAN interface
- New feature: DHCPv6 snooping entry backup
- New feature: Displaying brief VLAN information
- Modified feature: Enhanced CC authentication feature

**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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable SNMP notifications for PVST topology changes.</td>
<td>snmp-agent trap enable stp [ tc ]</td>
</tr>
</tbody>
</table>

**Command reference**

`snmp trap enable stp`

Use `snmp-agent trap enable stp` to enable SNMP notifications for PVST topology changes. Use `undo snmp-agent trap enable stp` to disable SNMP notifications for PVST topology changes.

**Syntax**

```
snmp-agent trap enable stp [ tc ]
undo snmp-agent trap enable stp [ tc ]
```

**Default**

SNMP notifications are disabled for PVST topology changes on all VLANs.

**Views**

System view

**Predefined user roles**

3: Manage level
Parameters

**tc**: Specifies SNMP notifications for PVST topology changes.

Usage guidelines

This command configures SNMP notifications only for PVST topology changes whether you specify the tc keyword or not.

Examples

# Enable SNMP notifications for PVST topology changes.
<Sysname> system-view
[Sysname] snmp-agent trap enable stp tc

New feature: 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a VLAN interface and enter its view.</td>
<td>interface vlan-interface {vlan-interface-id}</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the applicable scope of packet filtering on the VLAN interface.</td>
<td>packet-filter filter { route</td>
</tr>
</tbody>
</table>

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

Default command level
2: System level

Parameters
route: Filters packets forwarded at Layer 3 by the VLAN interface.
all: Filters all packets, including packets forwarded at Layer 3 by the VLAN interface and packets forwarded at Layer 2 by the physical ports associated with the VLAN interface.

Examples
# Configure the packet filtering on VLAN-interface 2 to filter packets forwarded at Layer 3.
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] packet-filter filter route

New feature: DHCPv6 snooping entry backup

Configuring DHCPv6 snooping entry backup

This feature saves DHCPv6 snooping entries to a backup file, and allows the DHCPv6 snooping device to download the entries from the backup file at reboot. The entries on the DHCPv6 snooping device cannot survive a reboot. The backup helps the security features provide services if these features (such as IPv6 source guard) must use DHCPv6 snooping entries for user authentication.

⚠️ IMPORTANT:
If you disable DHCPv6 snooping with the undo ipv6 dhcp snooping enable command, the device deletes all DHCPv6 snooping entries, including those stored in the backup file.

To configure DHCPv6 snooping entry backup:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ipv6 dhcp snooping binding database filename filename</td>
<td>By default, the DHCPv6 snooping device does not back up the DHCPv6 snooping entries. With this command executed, the DHCPv6 snooping device backs up DHCPv6 snooping entries immediately.</td>
</tr>
<tr>
<td>3.</td>
<td>ipv6 dhcp snooping binding database update now</td>
<td>Optional.</td>
</tr>
<tr>
<td>4.</td>
<td>ipv6 dhcp snooping binding database update interval seconds</td>
<td>Optional. By default, the DHCPv6 snooping device does not periodically update the backup file. If the DHCPv6 snooping entries change during an interval, the snooping device updates the backup file at the end of the interval. If no entry changes, the device does not update the backup file.</td>
</tr>
</tbody>
</table>
Step | Command | Remarks
--- | --- | ---
5. Display information about DHCPv6 snooping entry auto backup. | display ipv6 dhcp snooping binding database [ | { begin | exclude | include } regular-expression ] | N/A

Command reference

display ipv6 dhcp snooping binding database

Use **display ipv6 dhcp snooping binding database** to display information about DHCPv6 snooping entry auto backup.

Syntax

display ipv6 dhcp snooping binding database [ | { 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.

Examples

# Display information about DHCPv6 snooping entry auto backup.
<Sysname> display ipv6 dhcp snooping binding database

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name</td>
<td>Name of the DHCPv6 snooping entry backup file.</td>
</tr>
<tr>
<td>Update interval</td>
<td>Waiting time in seconds after a DHCPv6 snooping entry change for the DHCPv6 snooping device to update the backup file.</td>
</tr>
<tr>
<td>Latest read time</td>
<td>Time of the latest reading.</td>
</tr>
<tr>
<td>Latest write time</td>
<td><strong>Time of the latest writing.</strong></td>
</tr>
<tr>
<td>Status</td>
<td>Status of the update:</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
• Writing — The backup file is being updated.
• Last write succeeded — The backup file was successfully updated.
• Last write failed — The backup file failed to be updated.

ipv6 dhcp snooping binding database filename

Use `ipv6 dhcp snooping binding database filename` to configure the DHCPv6 snooping device to back up DHCPv6 snooping entries to a file.

Use `undo ipv6 dhcp snooping binding database filename` to disable the auto backup and remove the backup file.

**Syntax**

```
ipv6 dhcp snooping binding database filename filename
undo ipv6 dhcp snooping binding database filename
```

**Default**

The DHCPv6 snooping device does not back up DHCPv6 snooping entries.

**Default command level**

2: System level

**Parameters**

`filename`: Specifies the name of a backup file. For information about the `filename` argument, see *Fundamentals Configuration Guide*.

**Usage guidelines**

This command enables the DHCPv6 snooping device to back up the snooping entries immediately. For the device to periodically update the backup file, set an update interval by using the `ipv6 dhcp snooping binding database update interval` command.

**Examples**

```
# Configure the DHCPv6 snooping device to back up DHCPv6 snooping entries to the file database.dhcp.
<Sysname> system-view
[Sysname] ipv6 dhcp snooping binding database filename database.dhcp
```

**Related commands**

ipv6 dhcp snooping binding database update interval

**ipv6 dhcp snooping binding database update interval**

Use `ipv6 dhcp snooping binding database update interval` to configure the DHCPv6 snooping device to update the backup file periodically.

Use `undo ipv6 dhcp snooping binding database update interval` to restore the default.

**Syntax**

```
ipv6 dhcp snooping binding database update interval seconds
undo ipv6 dhcp snooping binding database update interval
```

**Default**

The DHCPv6 snooping device does not periodically update the backup file.
Views

System view

Default command level

2: System level

Parameters

seconds: Sets the update interval in seconds, in the range of 60 to 864000.

Usage guidelines

If the DHCPv6 snooping entries change during an interval, the snooping device updates the backup file at the end of the interval. If no entry changes, the device does not update the backup file.

For this command to take effect, you must configure the `ipv6 dhcp snooping binding database filename` command.

Examples

# Configure the DHCPv6 snooping device to update the backup file every 600 seconds.

```bash
<Sysname> system-view
[Sysname] ipv6 dhcp snooping binding database update interval 600
```

Related commands

`ipv6 dhcp snooping binding database update now`

ipv6 dhcp snooping binding database update now

Use `ipv6 dhcp snooping binding database update now` to manually update the DHCPv6 snooping entry backup file.

Syntax

```
ipv6 dhcp snooping binding database update now
```

Views

System view

Default command level

2: System level

Parameters

None

Usage guidelines

For this command to take effect, you must configure the `ipv6 dhcp snooping binding database filename` command.

Examples

# Manually update the DHCPv6 snooping entry backup file.

```bash
<Sysname> system-view
[Sysname] ipv6 dhcp snooping binding database update now
```

Related commands

`ipv6 dhcp snooping binding database filename`
New feature: Displaying brief VLAN information

Displaying brief VLAN information

In this release, you can display brief VLAN information.

Command reference

display vlan brief

Use `display vlan brief` to display brief VLAN information.

Syntax

display vlan brief

Views

Any view

Default command level

1: Monitor level

Examples

# Display brief VLAN information.
<Sysname> display vlan brief

Brief information about all VLANs:
Supported Minimum VLAN ID: 1
Supported Maximum VLAN ID: 4094
Default VLAN ID: 1

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Name</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VLAN 0001</td>
<td>GE1/0/1   GE1/0/2   GE1/0/3   GE1/0/4   GE1/0/5   GE1/0/6   GE1/0/7   GE1/0/8   GE1/0/9   GE1/0/10  GE1/0/11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GE1/0/12  GE1/0/13  GE1/0/14</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GE1/0/15  GE1/0/16  GE1/0/17</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GE1/0/18  GE1/0/19  GE1/0/20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GE1/0/21  GE1/0/22  GE1/0/23</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GE1/0/24  XGE1/0/26  XGE1/0/27</td>
</tr>
<tr>
<td></td>
<td></td>
<td>XGE1/0/28</td>
</tr>
</tbody>
</table>

Table 6 Command output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default VLAN ID</td>
<td>System default VLAN ID.</td>
</tr>
<tr>
<td>Name</td>
<td>VLAN name.</td>
</tr>
<tr>
<td>Port</td>
<td>Port that allows packets from the VLAN to pass through.</td>
</tr>
</tbody>
</table>
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
9906FBDB9FBD274654CA84727710773176A88AD3960C7E7B17BA24F539EA146B20BFB2BA7951A90
553328190D34510A45D550E
```

Table 7 Command output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time of Key pair created</td>
<td>Date and time when the local ECDSA key pair was created.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key name</td>
<td>Name of the key.</td>
</tr>
<tr>
<td>Key type</td>
<td>Type of the key. <strong>ECDSA Encryption Key</strong> indicates the ECDSA key pair.</td>
</tr>
<tr>
<td>Key code</td>
<td>Public key data.</td>
</tr>
</tbody>
</table>

**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:
\[
\text{ciphersuite } \{ \text{dhe_rsa_aes_128_cbc_sha | dhe_rsa_aes_256_cbc_sha | rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha } \} *
\]

New syntax
In FIPS mode:
\[
\text{ciphersuite } \{ \text{rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha } \} *
\]

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
\[
\text{dh } \{ \text{group2 | group5 | group14 } \}
\]

New syntax
\[
\text{dh group14}
\]

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
\[
\text{pfs } \{ \text{dh-group1 | dh-group2 | dh-group5 | dh-group14 } \}
\]

New syntax
\[
\text{pfs dh-group14}
\]

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 } ] *
```

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 | 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:
```
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 } ] *
```

**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:
New syntax

In non-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 } ]*
```

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.
This release has the following changes:

- New feature: Generic flow control check for Ethernet interfaces
- New feature: Remote flow mirroring
- Modified feature: File signature verification in software upgrade (including ISSU)
- Modified feature: Executing interactive commands in interface range view
- Modified feature: Configuring physical state change suppression on an Ethernet interface
- Modified feature: Configuring a tag and description for an IPv6 static route
- Modified feature: BGP support for IPv6 link-local address for peer relationship establishment

**New feature: Generic flow control check for Ethernet interfaces**

**Enabling generic flow control check for Ethernet interfaces**

Generic flow control is implemented through sending and receiving pause frames on Ethernet interfaces. However, receiving too many pause frames might cause link congestion and forwarding failure on an Ethernet interface. To resolve this problem, you can enable generic flow control check for Ethernet interfaces.

To enable generic flow control check for Ethernet interfaces:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enable generic flow check for Ethernet interfaces.</td>
<td>flow-control-check enable</td>
<td>By default, generic flow control check is disabled for Ethernet interfaces.</td>
</tr>
</tbody>
</table>

**Command reference**

`flow-control-check enable`

Use `flow-control-check enable` to enable generic flow control check for Ethernet interfaces.

Use `undo flow-control-check enable` to disable generic flow control check for Ethernet interfaces.

**Syntax**

`flow-control-check enable`
`undo flow-control-check enable`

**Default**

Generic flow control check is disabled for Ethernet interfaces.

**Views**

System view
Default command level
1: Monitor level

Examples

# Enable generic flow control check for Ethernet interfaces.
<Sysname> system-view
[sysname] flow-control-check enable
Flow control check enabled!

New feature: Remote flow mirroring

Configuring remote flow mirroring

This feature allows you to mirror packets to a remote monitoring device.

To configure remote flow mirroring:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter traffic behavior view.</td>
<td>traffic behavior behavior-name</td>
</tr>
<tr>
<td>3.</td>
<td>Configure remote flow mirroring for the traffic behavior.</td>
<td>mirror-to { cpu</td>
</tr>
</tbody>
</table>

Command reference

mirror-to

Use mirror-to to configure a flow mirroring action for a traffic behavior.
Use undo mirror-to to delete a flow mirroring action from a traffic behavior.

Old syntax

mirror-to { cpu | interface interface-type interface-number }

New syntax

mirror-to { cpu | interface interface-type interface-number [ destination-ip destination-ip-address source-ip source-ip-address [ dscp dscp-value | vlan vlan-id | vpn-instance vpn-instance-name ] * ] }
Parameters

- **cpu**: Mirrors packets to the CPU of the IRF member device where the interface with flow mirroring configured resides.
- **interface interface-type interface-number**: Mirrors packets to an interface specified by its type and number.
- **destination-ip destination-ip-address**: Encapsulates packets with the destination IP address when the packets are mirrored to the specified interface.
- **source-ip source-ip-address**: Encapsulates packets with the source IP address when the packets are mirrored to the specified interface.
- **dscp dscp-value**: Encapsulates packets with the DSCP value when the packets are mirrored to the specified interface.
- **vpn-instance vpn-instance-name**: Encapsulates packets with the VPN instance when the packets are mirrored to the specified interface.
- **vlan vlan-id**: Encapsulates packets with the VLAN ID when the packets are mirrored to the specified interface. The value range for the `vlan-id` argument is 1 to 4094.

Usage guidelines

In a behavior, you can configure multiple flow mirroring actions to mirror packets to different interfaces.

Examples

```
# Create traffic behavior 1 and configure the action of mirroring packets to the CPU for the traffic behavior.
<Sysname> system-view
[Sysname] traffic behavior 1
[Sysname-behavior-1] mirror-to cpu

# Create traffic behavior 1 and configure the action of mirroring packets to interface GigabitEthernet 1/0/1 for the traffic behavior.
<Sysname> system-view
[Sysname] traffic behavior 1
[Sysname-behavior-1] mirror-to interface gigabitethernet 1/0/1

# Create traffic behavior 1. Configure the action of mirroring packets to interface GigabitEthernet 1/0/1 for the traffic behavior, and encapsulate the mirrored packets with the following parameters:
- Source IP address 1.1.1.1.
- Destination IP address 2.2.2.2.
- DSCP value 20.
<Sysname> system-view
[Sysname] traffic behavior 1
[Sysname-behavior-1] mirror-to interface gigabitethernet 1/0/1 destination-ip 1.1.1.1 source-ip 2.2.2.2 dscp 20
```

Modified feature: File signature verification in software upgrade (including ISSU)

Feature change description

As of this release, the device verifies the file signature when it executes upgrade commands in both FIPS and non-FIPS modes. To downgrade the software to a version earlier than R1807P02, you...
must first downgrade the software to a version between R1807P02 and R1809P01. Then, use the **boot-loader** or **issu load** command to downgrade the software to the target version.

This change applies to the following software upgrade commands:

- **boot-loader**
- **boot-loader update file**
- **bootrom**
- **patch install**
- **patch load**
- **issu load**

Before modification:

The device verifies the file signature of the upgrade file only in FIPS mode. The commands are executed only if the signature verification is passed or no file signatures exist.

After modification:

The device verifies the file signature of the upgrade file in both FIPS and non-FIPS modes. The commands are executed only when the signature verification is passed.

Command changes

None.

**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: Configuring physical state change suppression on an Ethernet interface**

Feature change description

Before modification:

- When you separately enable state change suppression for link-up and link-down events, the most recent configuration takes effect. 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 is disabled.

After modification:
• You can specify a physical state change suppression interval in milliseconds by specifying the **msec** keyword.
• You can enable the system to suppress both link-down and link-up events by specifying the **updown** keyword.
• When you separately enable state change suppression for link-up and link-down events, both configurations take effect. 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.
• 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.

**Command changes**

**Modified command: link-delay**

**Old syntax**

```plaintext
link-delay delay-time [ mode up ]
undo link-delay
```

**New syntax**

```plaintext
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 is disabled.

After modification:
• The `link-delay delay-time [ mode up ]` command was changed to `link-delay [ **msec** ] delay-time [ mode { up | updown } ]`.
  o If you specify the **msec** keyword, the value range for the `delay-time` argument is 0 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.
  o If you specify the **updown** keyword, the link-down or link-up event is not reported unless the interface is still down or up when the suppression interval 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 ]
```

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 (?).

Modified feature: BGP support for IPv6 link-local address for peer relationship establishment

Feature change description

BGP can use an IPv6 link-local address to establish a peer relationship with a peer when the following conditions exist:

- The IPv6 link-local address belongs to the interface directly connected to the local router.
• The **peer connect-interface** command is configured on the peer to specify the interface as the source interface.

Command changes

Modified command: peer connect-interface

**Syntax**

```
peer { group-name | ip-address } connect-interface interface-type interface-number
undo peer { group-name | ip-address } connect-interface
```

**Views**

BGP view, BGP-VPN instance view, IPv6 BGP-VPN instance view

**Change description**

Before modification: This command is available in BGP view and BGP-VPN instance view.

After modification: This command is available in BGP view, BGP-VPN instance view, and IPv6 BGP-VPN instance view.
This release has the following changes:

- New feature: Route addition for assigned prefixes on the DHCPv6 relay agent
- New feature: Telnet/SSH user connection control
- New feature: Advertising the COMMUNITY attribute through BGP VPN-IPv6/VPNv6 routes
- Modified feature: BGP support for IPv6 link-local address for peer relationship establishment
- Modified feature: BPDU tunneling

New feature: Route addition for assigned prefixes on the DHCPv6 relay agent

Configuring route addition for assigned prefixes on the DHCPv6 relay agent

The route addition feature enables the DHCPv6 relay agent to automatically add a route to the client's network. The DHCPv6 relay agent learns the client's network from the IPv6 prefix information in the PD option of the received legal DHCPv6 reply message.

This feature can only be configured on the DHCPv6 relay agent that directly connects to the DHCPv6 client.

To configure route addition for assigned prefixes on the DHCPv6 relay agent:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ipv6 dhcp relay iapd-route-add</td>
<td>By default, route addition is disabled on the DHCPv6 relay agent.</td>
</tr>
<tr>
<td>3.</td>
<td>display ipv6 dhcp relay prefix { all</td>
<td>ipv6-prefix/prefix-length }</td>
</tr>
<tr>
<td>4.</td>
<td>reset ipv6 dhcp relay prefix ipv6-prefix/prefix-length</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Command reference

display ipv6 dhcp relay prefix

Use `display ipv6 dhcp relay prefix` to display information about the IPv6 prefixes recorded by the DHCPv6 relay agent.

Syntax

`display ipv6 dhcp relay prefix { all | ipv6-prefix/prefix-length }`  

Views

Any view
Default command level
1: Monitor level

Parameters
all: Displays information about all IPv6 prefixes recorded by the DHCPv6 relay agent.
ipv6-prefix/prefix-length: Specifies an IPv6 prefix and the prefix length. The value range for prefix-length is 1 to 128.

Examples
# Display information about all IPv6 prefixes recorded by the DHCPv6 relay agent.
<sysname> display ipv6 dhcp relay prefix all
Total number: 2
IPv6 Prefix               Interface               Expiration time
1:1::/64                  Vlan2                   Nov 23 16:12:43 2010
1:2::/64                  InLoop0                 Nov 24 16:12:43 2010
# Display information about IPv6 prefix 1:1::/64.
<sysname> display ipv6 dhcp relay prefix 1:1::/64
IPv6 Prefix               Interface               Expiration time
1:1::/64                  Vlan2                   Nov 23 16:12:43 2010

Table 1 Command output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number</td>
<td>Total number of the IPv6 prefixes.</td>
</tr>
<tr>
<td>IPv6 prefix</td>
<td>IPv6 prefix assigned to the DHCPv6 client.</td>
</tr>
<tr>
<td>Interface</td>
<td>Layer 3 interface connected to the DHCPv6 client.</td>
</tr>
<tr>
<td>Expiration time</td>
<td>Time when the IPv6 prefix expires.</td>
</tr>
</tbody>
</table>

ipv6 dhcp relay iapd-route-add

Use ipv6 dhcp relay iapd-route-add to enable route addition for assigned prefixes on the DHCPv6 relay agent.
Use undo ipv6 dhcp relay iapd-route-add to disable the route addition feature.

Syntax
ipv6 dhcp relay iapd-route-add
undo ipv6 dhcp relay iapd-route-add

Default
The route addition feature is disabled.

Views
System view

Default command level
2: System level

Examples
# Enable route addition for assigned prefixes on the DHCPv6 relay agent.
<sysname> sysname
**reset ipv6 dhcp relay prefix**

Use **reset ipv6 dhcp relay prefix** to clear information about the IPv6 prefixes recorded by the DHCPv6 relay agent.

**Syntax**

```
reset ipv6 dhcp relay prefix ipv6-prefix/prefix-length
```

**Views**

User view

**Default command level**

1: Monitor level

**Parameters**

`ipv6-prefix/prefix-length`: Specifies an IPv6 prefix and the prefix length. The value range for `prefix-length` is 1 to 128.

**Examples**

# Clear information about IPv6 prefix 1:1::/64.

<sysname> reset ipv6 dhcp relay prefix 1:1::/64

---

**New feature: Telnet/SSH user connection control**

**Configuring Telnet/SSH user connection control**

This feature allows you to control Telnet/SSH user connections to the device based on the referenced ACL. Only the Telnet/SSH users that the referenced ACL permits can initiate Telnet/SSH connections to the device.

All Telnet/SSH users can initiate Telnet/SSH connections to the device when any one of the following conditions exits:

- You do not specify any ACLs.
- The specified ACL does not exist.
- The specified ACL does not have any rules.

**Configuration prerequisites**

Before you configure Telnet/SSH user connection control, configure the ACL as required.

**Configuration procedure**

To configure Telnet user connection control:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure Telnet user connection control.</td>
<td>• Configure IPv4 Telnet user connection control: <code>telnet server acl acl-number</code> • Configure IPv6 Telnet user connection control:</td>
</tr>
</tbody>
</table>
To configure SSH user connection control:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure SSH user connection control.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Configure IPv4 SSH user connection control:</td>
<td><strong>ssh server acl acl-number</strong></td>
</tr>
<tr>
<td></td>
<td>• Configure IPv6 SSH user connection control:</td>
<td><strong>ssh server ipv6 acl ipv6 acl-number</strong></td>
</tr>
</tbody>
</table>

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
```

**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**

By default, no ACLs are specified and all IPv4 SSH users can initiate SSH connections to the device.

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 new SSH connections after the 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
```
ssh server ipv6 acl

Use **ssh server ipv6 acl** to specify an ACL to control IPv6 SSH user connections.
Use **undo ssh server ipv6 acl** to restore the default.

**Syntax**

```plaintext
ssh server ipv6 acl ipv6 acl-number
undo ssh server ipv6 acl
```

**Views**

System view

**Default command level**

3: Manage level

**Parameters**

- **ipv6**: Specifies an IPv6 ACL.
- **acl-number**: Specifies an IPv6 ACL by its number in the range of 2000 to 3999.

**Usage guidelines**

By default, no ACLs are specified and all IPv6 SSH users can initiate SSH connections to the device. 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 new SSH connections after the 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.

```plaintext
<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

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.
By default, no ACLs are specified and all IPv4 Telnet users can initiate Telnet connections to the device.
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 new Telnet connections after the 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

Use telnet server ipv6 acl 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

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.

By default, no ACLs are specified and all IPv6 Telnet users can initiate Telnet connections to the device.

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 new Telnet connections after the 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.

```bash
<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: Advertising the COMMUNITY attribute through BGP VPN-IPv6/VPNv6 routes

Advertising the COMMUNITY attribute through BGP VPN-IPv6/VPNv6 routes

BGP can advertise the COMMUNITY attribute to a peer through BGP VPN-IPv6/VPNv6 routes in an MPLS L3VPN network.

To advertise the COMMUNITY attribute through BGP VPN-IPv6 routes:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP view.</td>
<td><code>bgp as-number</code></td>
</tr>
<tr>
<td>3.</td>
<td>Enter IPv6 BGP-VPN instance view.</td>
<td><code>ipv6-family vpn-instance vpn-instance-name</code></td>
</tr>
<tr>
<td>4.</td>
<td>Advertise the COMMUNITY attribute to a peer.</td>
<td><code>peer ipv6-address advertise-community</code></td>
</tr>
</tbody>
</table>
To advertise the COMMUNITY attribute through BGP VPNv6 routes:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP view.</td>
<td>bgp as-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enter BGP-VPNv6 subaddress family view.</td>
<td>ipv6-family vpnv6</td>
</tr>
<tr>
<td>4.</td>
<td>Advertise the COMMUNITY attribute to a peer.</td>
<td>peer ip-address advertise-community</td>
</tr>
</tbody>
</table>

Command reference

**peer advertise-community (IPv6 BGP-VPN instance view)**

Use **peer advertise-community** to advertise the COMMUNITY attribute to a peer.

Use **undo peer advertise-community** to disable the COMMUNITY attribute advertisement to a peer.

**Syntax**

```
peer ipv6-address advertise-community
undo peer ipv6-address advertise-community
```

**Default**

No COMMUNITY attribute is advertised to any peer.

**Views**

IPv6 BGP-VPN instance view

**Default command level**

2: System level

**Parameters**

`ipv6-address`: Specifies a peer by its IPv6 address.

**Examples**

```
# Advertise the COMMUNITY attribute to peer 1:2::3:4 through BGP VPN-IPv6 routes. (The VPN has been created.)
<Sysname> system-view
<Sysname> bgp 100
[Sysname-bgp] ipv6-family vpn-instance vpn1
[Sysname-bgp-ipv6-vpn1] peer 1:2::3:4 advertise-community
```

**peer advertise-community (BGP-VPNv6 subaddress family view)**

Use **peer advertise-community** to advertise the COMMUNITY attribute to a peer.

Use **undo peer advertise-community** to disable the COMMUNITY attribute advertisement to a peer.

**Syntax**

```
peer ip-address advertise-community
```
undo peer ip-address advertise-community

Default
No COMMUNITY attribute is advertised to any peer.

Views
BGP-VPNv6 subaddress family view

Default command level
2: System level

Parameters

ip-address: Specifies a peer by its IP address.

Examples

# Advertise the COMMUNITY attribute to peer 1.1.1.1 through BGP VPNv6 routes.
/sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family vpnv6
[Sysname-bgp-af-vpnv6] peer 1.1.1.1 advertise-community

Modified feature: BGP support for IPv6 link-local address for peer relationship establishment

Feature change description

BGP can use an IPv6 link-local address to establish a peer relationship with a peer when the following conditions exist:

- The IPv6 link-local address belongs to the interface directly connected to the local router.
- The peer connect-interface command is configured on the peer to specify the interface as the source interface.

Command changes

Modified command: peer connect-interface

Syntax

peer { group-name | ip-address } connect-interface interface-type interface-number
undo peer { group-name | ip-address } connect-interface

Views

BGP view, BGP-VPN instance view, IPv6 BGP-VPN instance view

Change description

Before modification: This command is available in BGP view and BGP-VPN instance view.
After modification: This command is available in BGP view, BGP-VPN instance view, and IPv6 BGP-VPN instance view.
Modified feature: BPDU tunneling

Feature change description

In this release, Layer 2 aggregate interfaces support configuring BPDU tunneling for Layer 2 protocols LLDP, UDLD, PAGP, LACP, and DLDP.

BPDU tunneling configured on a member port of a Layer 2 aggregation group for Layer 2 protocol LLDP, UDLD, PAGP, LACP, or DLDP does not take effect. The configuration takes effect when the member port leaves the aggregation group.

Command changes

Modified command: bpdu-tunnel dot1q

The bpdu-tunnel dot1q command can be configured in Layer 2 Ethernet port view, port group view, and Layer 2 aggregate interface view. The configuration of this command in Layer 2 Ethernet port view and port group view is not changed. This section describes the change of the command in Layer 2 aggregate interface view.

Old syntax

bpdu-tunnel dot1q { cdp | gvrp | hgmp | pvst | stp | vtp }
undo bpdu-tunnel dot1q { cdp | gvrp | hgmp | pvst | stp | vtp }

New syntax

bpdu-tunnel dot1q { cdp | dldp | gvrp | hgmp | lacp | lldp | pagp | pvst | stp | udld | vtp }
undo bpdu-tunnel dot1q { cdp | dldp | gvrp | hgmp | lacp | lldp | pagp | pvst | stp | udld | vtp }

Views
Layer 2 aggregate interface view

Change description

Before modification: Layer 2 aggregate interfaces do not support configuring BPDU tunneling for Layer 2 protocols LLDP, UDLD, PAGP, LACP, and DLDP.

After modification: Layer 2 aggregate interfaces support configuring BPDU tunneling for Layer 2 protocols LLDP, UDLD, PAGP, LACP, and DLDP.
This release has the following changes:

- New feature: 802.1X voice VLAN
- New feature: Sending EAPOL frames untagged on a port
- New feature: TCP fragment attack protection
- New feature: Tracert packet source IPv6 address configuration

New feature: 802.1X voice VLAN

Configuring an 802.1X voice VLAN

You can configure an 802.1X voice VLAN on an 802.1X-enabled port that connects to a voice terminal. The 802.1X voice VLAN feature is effective only on voice terminals that support VLAN-tagged packets.

The 802.1X voice VLAN feature works with a remote authentication server. The device uses the following process to implement this feature:

1. Identifies a voice terminal from the packet sent by the authentication server when the terminal passes 802.1X authentication. The authentication server identifies the terminal type by information such as its OUI and user account, and then sends the terminal type information to the device.
2. Assigns the port to the configured voice VLAN as a tagged member and sends the voice VLAN information through an LLDP or CDP packet to the terminal.

A voice terminal is not associated with a specific voice VLAN. The voice VLAN assigned to the voice terminal depends on the voice VLAN configuration on the access port.

Configuration guidelines

When you configure an 802.1X voice VLAN, follow these guidelines:

- You can configure only one 802.1X voice VLAN on a port. The 802.1X voice VLANs on different ports can be different.
- To ensure a correct exchange of 802.1X EAPOL packets, you must configure the `dot1x eapol untag` command. For information about this command, see "New feature: Sending EAPOL frames untagged on a port."
- 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 802.1X VLAN manipulations, see HP 5820X & 5800 Switch Series Security Configuration Guide-R18xx.
- 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 5820X & 5800 Switch Series Layer 2 - LAN Switching Configuration Guide-R18xx.
Configure LLDP or CDP compatibility on the device. For information about the LLDP and CDP compatibility features, see HP 5820X & 5800 Switch Series Layer 2 - LAN Switching Configuration Guide-R18xx.

Configuration procedure

To configure an 802.1X voice VLAN on a port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3. Configure an 802.1X voice VLAN on the port.</td>
<td>dot1x voice vlan vlan-id</td>
<td>By default, no 802.1X voice VLAN is configured on a port.</td>
</tr>
</tbody>
</table>

Command reference

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

**Default**

No 802.1X voice VLAN is configured on a port.

**Views**

Layer 2 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 this command, see "New feature: Sending EAPOL frames untagged on a port."

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 802.1X VLAN manipulations, see HP 5820X & 5800 Switch Series Security Configuration Guide-R18xx.

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 5820X & 5800 Switch Series Layer 2 - LAN Switching Configuration Guide-R18xx.
- Configure LLDP or CDP compatibility on the device. For information about the LLDP and CDP compatibility features, see HP 5820X & 5800 Switch Series Layer 2 - LAN Switching Configuration Guide-R18xx.

Examples

```
# Configure VLAN 20 as the 802.1X voice VLAN on GigabitEthernet 1/0/1.
<Sysname> system-view
  [Sysname] interface gigabitethernet 1/0/1
  [Sysname-GigabitEthernet1/0/1] dot1x voice vlan 20
```

New feature: Sending EAPOL frames untagged on a port

Configuring a port to send EAPOL frames untagged

EAPOL frames exchanged between the 802.1X client and the network access device must not contain VLAN tags. If any 802.1X user attached to a port is assigned a tagged VLAN, you must enable the port to send EAPOL frames untagged to the 802.1X client.

To configure a port to send EAPOL packets untagged to the 802.1X client:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the port to send 802.1X EAPOL frames untagged.</td>
<td>dot1x eapol untag</td>
</tr>
</tbody>
</table>

Command reference

dot1x eapol untag

Use dot1x eapol untag to configure a port to send EAPOL packets untagged.
Use undo dot1x eapol untag to restore the default.

Syntax

```
dot1x eapol untag
undo dot1x eapol untag
```

Default

Whether the port sends EAPOL packets with VLAN tags depends on the VLAN settings on the port.

Views

Layer 2 Ethernet interface view

Default command level

3: Manage level
Usage guidelines

EAPOL frames exchanged between the 802.1X client and the network access device must not contain VLAN tags. If any 802.1X user attached to a port is assigned a tagged VLAN, you must enable the port to send EAPOL frames untagged.

Examples

# Configure GigabitEthernet 1/0/1 to send EAPOL packets untagged.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x eapol untag

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>attack-defense tcp fragment enable</td>
<td>By default, TCP fragment attack protection is enabled.</td>
</tr>
</tbody>
</table>

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: Tracert packet source IPv6 address configuration

Specifying the source IPv6 address for tracert packets

You can specify the source IPv6 address for tracert packets in the tracert ipv6 command.

Command changes

Modified command: tracert ipv6

Old syntax
tracert ipv6 [-f first-ttl | -m max-ttl | -p port | -q packet-number | -tos tos | -vpn-instance vpn-instance-name | -w timeout] * host

New syntax
tracert ipv6 [-a source-ipv6 | -f first-ttl | -m max-ttl | -p port | -q packet-number | -tos tos | -vpn-instance vpn-instance-name | -w timeout] * host

Parameters
-a source-ipv6: Specifies the source IPv6 address for tracert packets. The IPv6 address must already exist on the device. If you do not specify this option, the source IPv6 address of tracert packets is an IP address of the outgoing interface of the packets (address selection conforms to RFC 3484.).

Views
Any view

Change description
Before modification: The tracert ipv6 command does not support the -a source-ipv6 option.
After modification: The tracert ipv6 command supports the -a source-ipv6 option.
This release has the following changes:
- Modified feature: Auto status transition of dynamic secure MAC addresses
- Modified feature: IPv6 address with a 127-bit prefix length

Modified feature: Auto status transition of dynamic secure MAC addresses

Feature change description

Before R1808P23: A dynamic secure MAC address entry will not be deleted if the port for the entry goes down.

R1808P23 and later versions: 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: IPv6 address with a 127-bit prefix length

Feature change description

Before R1808P23: 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.

R1808P23 and later versions:
- 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.
This release has no feature changes.
This release has the following changes:

- New feature: Discarding IPv6 packets that contain extension headers

**New feature: Discarding IPv6 packets that contain extension headers**

Enabling a device to discard IPv6 packets that contain extension headers

This feature enables a device to discard a received IPv6 packet 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable the device to discard IPv6 packets that contain extension headers.</td>
<td>ipv6 option drop enable</td>
</tr>
</tbody>
</table>

**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.

```bash
<Sysname> system-view
[Sysname] ipv6 option drop enable
```
This release has the following changes:

- New feature: Multicast across VPNs
- New feature: Configuring the expected bandwidth of an interface
- New feature: Configuring DHCPv6 relay on an MCE
- Modified feature: Customizing DHCP options

**New feature: Multicast across VPNs**

Configuring multicast across VPNs

**Overview**

MD VPN implements multicasting between the multicast source and the receivers when they are in the same VPN. However, multicast data in different VPNs are isolated. If the multicast source and the receivers are in different VPNs, you must configure multicast across VPNs so that the receivers can receive multicast data from the multicast source.

**Figure 1 Multicast across VPNs**

As shown in Figure 1, Source 1 is in Site 1 of VPN A, Receiver 1 is in Site 2 of VPN A, Receiver 2 is in Site 1 of VPN B. MD VPN enables Receiver 1 to receive multicast data from only Source 1, and multicast across VPNs enables Receiver 2 to receive multicast data from Source 1.

The PE that directly connects to the multicast source is called the "source-side PE." The PEs that directly connect to the sites of the receivers are called the "receiver-side PEs". In this figure, PE 1 is the source-side PE, and PE 2 and PE 3 are the receiver-side PEs. To implement multicast across VPNs, source-side PE configuration and receiver-side PE configuration schemes are available.
Source-side PE configuration

To implement multicast across VPNs, this configuration covers creating VPN instance that the receivers belongs to on the source-side PE, and configuring a share-group for the VPN instance.

**Figure 2 Source-side PE configuration**

As shown in **Figure 2**, configure VPN instance A, create VPN instance B, and specify the share-group on PE 1.

After the configuration, a share-MDT is established for VPN instance A and VPN instance B respectively on the public network. After receiving multicast packets from Source 1, PE 1 duplicates and encapsulates them, and forwards them to PE 2 and PE 3 along the share-MDTs. PE 2 and PE 3 de-encapsulate and forward them to Receiver 1 and Receiver 2, respectively.

Receiver-side PE configuration

To implement multicast across VPNs, this configuration covers creating VPN instance that the multicast source belongs to on the receiver-side PE, and configuring a share-group for the VPN instance.
As shown in Figure 3, configure VPN instance B, create VPN instance A, and specify the share-group on PE 3. Because PE 2 serves VPN A, create VPN instance A and specify the share-group on PE 2. After the configuration, a share-MDT is established for VPN instance A. After receiving multicast packets from Source 1, PE 1 encapsulates and forwards them to PE 2 and PE 3 along the share-MDT. PE 2 and PE 3 de-encapsulate and forward them to Receiver 1 and Receiver 2, respectively.

The following limitations apply to the source-side PE configuration and receiver-side PE configuration schemes.

- In the VPN to which the multicast sources belong and the VPNs to which the receivers belong, PIM-SM, BIDIR-PIM, or PIM-SSM is supported, but PIM-DM is not supported.
- The PIM modes, SSM group policies, and multicast source policies of the VPN to which the multicast sources belong must be consistent with those of the VPNs to which the receivers belong.
- The RP must be in the same site of the same VPN as the multicast source.
- Multicasting cannot be implemented along multiple VPNs. For example, the multicast data from VPN A cannot be forwarded to VPN C by VPN B.

Specifying the source IP address for multicast across VPNs

To implement multicast across VPNs, you must specify the source IP address for multicast across VPNs.

Configuration prerequisites

Before you perform this configuration, complete the following tasks:

- Create a VPN instance on each PE and specify the share-group.
- Create the receivers’ VPN instances on the source-side PE, and
  o For source-side PE configuration, specify the share-group.
  o For receiver-side PE configuration, create the multicast source’s VPN instance on the receiver-side PE and specify the share-group.
• Configure the RD in all VPN instances on the PEs and enable IP multicasting.
• Configure the same PIM mode (PIM-SM, BIDIR-PIM, or PIM-SSM) in the multicast source's VPN and the receivers' VPNs.
• Determine the IP addresses of the multicast source and RP, and their home VPN instances.

Configuration procedure

If the receivers and the multicast source are in different VPNs, configure the IP addresses of both the multicast source and RP as the source IP address. This allows multicast across VPNs in the VPN instance views of the receivers on the receiver-side PE.

Perform the following configuration on the PE.

To specify the source IP address for multicast across VPNs:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter VPN instance view.</td>
<td>ip vpn-instance vpn-instance-name</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the source IP address for multicast across VPNs.</td>
<td>multicast extra-vpn vpn-instance-name source-address { mask-length</td>
</tr>
</tbody>
</table>

Configuration example (Source-side PE configuration)

Network requirements

As shown in Figure 1, the multicast VPN feature has been configured on the MPLS L3VPN network. Multicast data can be correctly forwarded within VPN a.

Configure multicast across VPNs on PE 1 so that the receiver host R2 in VPN b can receive the multicast data from VPN a.

Figure 1 Network diagram

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>CE a1</td>
<td>Loopback 1</td>
<td>1.1.1.1/32</td>
</tr>
<tr>
<td>Device</td>
<td>Interface</td>
<td>IP address</td>
</tr>
<tr>
<td>--------</td>
<td>-----------</td>
<td>--------------</td>
</tr>
<tr>
<td>S</td>
<td>—</td>
<td>100.1.1.1/24</td>
</tr>
</tbody>
</table>

Configuration procedure

This example assumes that the network interoperability, routing information distribution, and multicast VPNs have been correctly configured.

1. Configure VPN instances:

   # Create a VPN instance b on PE 1.
   ```
   <PE1> system-view
   [PE1] ip vpn-instance b
   ```

   # Configure 200:1 as the RD and route target for VPN b.
   ```
   [PE1-vpn-instance-b] route-distinguisher 200:1
   [PE1-vpn-instance-b] vpn-target 200:1 both
   ```

   # Enable IP multicast routing for VPN b.
   ```
   [PE1-vpn-instance-b] multicast routing-enable
   ```

   # Configure 239.2.2.2 as the share-group for VPN b.
   ```
   [PE1-vpn-instance-b] multicast-domain share-group 239.2.2.2 binding mtunnel 1
   ```

   # Create a VPN instance b on PE 2.
   ```
   <PE2> system-view
   [PE2] ip vpn-instance b
   ```

   # Configure 200:1 as the RD and route target for VPN b.
   ```
   [PE2-vpn-instance-b] route-distinguisher 200:1
   [PE2-vpn-instance-b] vpn-target 200:1 both
   ```

   # Enable IP multicast routing for VPN b.
   ```
   [PE2-vpn-instance-b] multicast routing-enable
   ```

   # Configure 239.2.2.2 as the share-group for VPN b.
   ```
   [PE2-vpn-instance-b] multicast-domain share-group 239.2.2.2 binding mtunnel 1
   ```

   # Bind VLAN-interface 15 with VPN b on PE 2. (PE 2 connects to CE b1 through VLAN-interface 15.)
   ```
   [PE2] interface Vlan-interface 15
   [PE2-Vlan-interface15] ip binding vpn-instance b
   [PE2-Vlan-interface15] quit
   ```

   # Configure MBGP on PE 1 and PE 2 so they can exchange route information of VPN b.
   (Details not shown.)

2. Configure multicast across VPNs:

   # On the devices that forward the multicast data to VPN b, complete all multicast VPN configurations except the RP configurations. For more information, see **IP multicast Configuration Guide**.

   # Display the RP information of VPN a on PE 1.
   ```
   [PE1] display pim vpn-instance a rp-info
   ```

   VPN-Instance: a
   PIM-SM BSR RP information:
   Group/MaskLen: 224.0.0.0/4
   RP: 1.1.1.1
   Priority: 192
# Configure the multicast source address and the RP address of VPN a as the source IP address for multicast across VPNs in VPN b.

```
[PE1] ip vpn-instance b  
[PE1-vpn-instance-b] multicast extra-vpn a 100.1.1.1 255.255.255.255  
[PE1-vpn-instance-b] multicast extra-vpn a 1.1.1.1 255.255.255.255  
[PE1-vpn-instance-b] quit
```

# Configure the RP of VPN a as the static RP of VPN b.

```
[PE1] pim vpn-instance b  
[PE1-pim-b] static-rp 1.1.1.1
```

# On PE 2, configure the RP of VPN a as the static RP of VPN b.

```
[PE2] pim vpn-instance b  
[PE2-pim-b] static-rp 1.1.1.1  
[PE2-pim-b] quit
```

# Configure 100:1 as the import route target for VPN b. (100:1 is the export route target for VPN a.)

```
[PE2] ip vpn-instance b  
[PE2-vpn-instance-b] vpn-target 100:1 import  
[PE2-vpn-instance-b] quit
```

# On CE b1, configure the RP of VPN a as the static RP in the PIM-SM domain.

```
<CE_b1> system-view  
[CE_b1] pim  
[CE_b1-pim] static-rp 1.1.1.1
```

Configuration example (Receiver-side PE configuration)

Network requirements

As shown in Figure 2, the multicast VPN feature has been configured on the MPLS L3VPN network. Multicast data can be correctly forwarded within VPN a.

Configure multicast across VPNs on PE 2 so that the receiver host R2 in VPN b can receive the multicast data from VPN a.
Configuration procedure

This example assumes that the network interoperability, routing information distribution, and multicast VPNs have been correctly configured.

1. Configure VPN instances:
   
   
   ```
   # Create VPN instance b on PE 2.
   <PE2> system-view
   [PE2] ip vpn-instance b
   
   # Configure 200:1 as the RD and route target for VPN b.
   [PE2-vpn-instance-b] route-distinguisher 200:1
   [PE2-vpn-instance-b] vpn-target 200:1 both
   
   # Enable IP multicast routing for VPN b.
   [PE2-vpn-instance-b] multicast routing-enable
   
   # Bind VLAN-interface 15 with VPN b on PE 2. (PE 2 connects to CE b1 through VLAN-interface 15.)
   [PE2] interface Vlan-interface 15
   [PE2-Vlan-interface15] ip binding vpn-instance b
   [PE2-Vlan-interface15] quit
   
   # On all interfaces that forward multicast data to VPN b, enable IP multicast routing. (Details not shown.)
   
   # On PE 2 and CE b1, configure a routing protocol so that they can exchange routing information of VPN b. (Details not shown.)
   ```

2. Configure multicast across VPNs:
# Display the RP information of VPN a on CE a1.
<CE_a1> display pim vpn-instance a rp-info
VPN-Instance: a
PIM-SM BSR RP information:
Group/MaskLen: 224.0.0.0/4
    RP: 1.1.1.1 (local)
    Priority: 0
    HoldTime: 150
    Uptime: 02:20:50
    Expires: 00:01:51

# On PE 2, configure the RP address and the multicast source address of VPN a as the source IP address for multicast across VPNS in VPN b.
[PE2] ip vpn-instance b
[PE2-vpn-instance-b] multicast extra-vpn a 1.1.1.1 255.255.255.255
[PE2-vpn-instance-b] multicast extra-vpn a 100.1.1.1 255.255.255.255
[PE2-vpn-instance-b] quit

# Configure the RP of VPN a as the static RP of VPN b.
[PE2] pim vpn-instance b
[PE2-pim-b] static-rp 1.1.1.1

# On CE b1, configure the RP of VPN a as the static RP of the PIM-SM domain.
<CE_b1> system-view
[CE_b1] pim
[CE_b1-pim] static-rp 1.1.1.1
[CE_b1-pim] quit

# On CE b1, configure the routes to the static RP and the multicast source. This example uses static routes.
[CE_b1] ip route-static 1.1.1.1 255.255.255.255 200.1.1.1
[CE_b1] ip route-static 100.1.1.1 255.255.255.255 200.1.1.1

Command reference

This section introduces only the new and modified commands for multicast VPN.
For more information about other commands for multicast across VPNS, see IP multicast Command Reference and MPLS Command Reference.

multicast extra-vpn

Use multicast extra-vpn to specify the source IP address for multicast across VPNS.
Use undo multicast extra-vpn to restore the default.

Syntax

multicast extra-vpn vpn-instance-name source-address { mask-length | mask }
undo multicast extra-vpn vpn-instance-name source-address { mask-length | mask }

Default

No source IP address for multicast across VPNS is specified.

Views

VPN instance view
Default command level
2: System level

Parameters

`vpn-instance-name`: Name of an MPLS L3VPN instance, a case-sensitive string of 1 to 31 characters.

`source-address`: Source IP address for multicast across VPNs.

`mask-length`: Mask length of the specified source IP address, in the range of 0 to 32.

`mask`: Subnet mask of the specified source IP address.

Examples

```
# In VPN mvpn, specify 10.1.1.1/32 in VPN red as the source IP address for multicast across VPNs.
<Sysname> system-view
<Sysname> ip vpn-instance mvpn
<Sysname-vpn-instance-mvpn] multicast extra-vpn red 10.1.1.1 32
```

New feature: Configuring the expected bandwidth of an interface

Configuring the expected bandwidth of an interface

Configuring the expected bandwidth of an interface enables network management systems to monitor whether the actual bandwidth of the interface is consistent with the expected bandwidth.

To configure the expected bandwidth of an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the expected bandwidth of the interface.</td>
<td>bandwidth bandwidth-value</td>
</tr>
</tbody>
</table>

Command reference

`bandwidth`

Use `bandwidth` to configure the expected bandwidth of an interface.

Use `undo bandwidth` to restore the default.

Syntax

`bandwidth bandwidth-value`

`undo bandwidth`

Views

Ethernet interface view, Layer 2 aggregate interface view, Layer 3 aggregate interface view, VLAN interface view, tunnel interface view
Default command level
2: System level

Parameters

bandwidth-value: Specifies the expected bandwidth in the range of 1 to 4294967295 kbps.

Usage guidelines
You can obtain the expected bandwidth of an interface by querying the ifspeed value of the MIB node with third-party software.
The expected bandwidth is used by network management systems for bandwidth monitoring. It does not affect the actual bandwidth of the interface.

Examples

# Set the expected bandwidth of Ethernet interface GigabitEthernet 1/0/1 to 10000 kbps.
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] bandwidth 10000

New feature: Configuring DHCPv6 relay on an MCE

Configuring DHCPv6 relay on an MCE

An MCE device serving as the DHCPv6 relay agent can forward DHCPv6 packets between a DHCPv6 server and clients on either a public network or a private network. For more information about MCE, see MPLS Configuration Guide.

Command reference
None.

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 vaule range for the *code* argument is 2 to 254, excluding 50 through 54, 58, 59, 61, and 82.
This release has the following changes:

- Modified feature: ACL-based packet filtering on a VLAN interface

**Modified feature: ACL-based packet filtering on a VLAN interface**

**Feature change description**

In versions prior to Release 1808P16, the ACL applied to a VLAN interface filters packets forwarded at Layer 3. In Release 1808P16 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 1808P16, 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 1808P16 and later versions, the configuration on Switch A is as follows:

<SwitchA>system-view

System View: return to User View with Ctrl+Z.

[SwitchA]acl number 3000

[SwitchA-acl-adv-3000]rule permit ip source 192.168.0.1 0 destination 10.1.1.1 0.0.0.255

[SwitchA-acl-adv-3000]rule permit ip source 192.168.0.1 0.0.0.255 destination 192.168.0.10 0.0.0.255

[SwitchA-acl-adv-3000]rule deny ip

[SwitchA-acl-adv-3000]quit

[SwitchA]interface Vlan-interface 20

[SwitchA-Vlan-interface20]packet-filter 3000 inbound

Because the ACL takes effect on packets forwarded at Layer 3 and packets forwarded at Layer 2, you need to configure one more permit rule to permit packets from PC A to PC B. Configure the rules in the following order:

a. A permit rule that permits packets from PC A to Switch B.

b. A permit rule that permits packets from PC A to PC B.

c. A deny rule that denies all packets.
This release has the following changes:

- Modified feature: Setting the device name
- Modified feature: BGP load balancing
- Modified feature: Multicast BGP load balancing

**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: BGP load balancing**

**Feature change description**

This release enables you to implement load balancing over either IBGP or EBGP ECMP routes.

**Command changes**

Modified command: **balance**

**Old syntax**

```
balance number
undo balance
```

**New syntax**

```
balance [ebgp | ibgp] number
undo balance [ebgp | ibgp]
```
Views

BGP view, BGP-VPN instance view, IPv6 address family view, IPv6 BGP-VPN instance view

Parameters

**ebgp**: Enables load balancing over EBGP ECMP routes.

**ibgp**: Enables load balancing over IBGP ECMP routes.

**number**: Specifies the maximum number of BGP ECMP routes for load balancing. When it is set to 1, load balancing is disabled.

Change description

Before modification: BGP does not differentiate between EBGP and IBGP ECMP routes and it uses all available ECMP routes to implement load balancing.

After modification: You can use the **ebgp** or **ibgp** keyword to implement load balancing over either EBGP or IBGP ECMP routes. If you do not specify the **ibgp** or **ebgp** keyword, this command enables load balancing over both EBGP and IBGP ECMP routes. After you execute the **balance ibgp number** command or the **balance ebgp number** command, the **balance number** command cannot be executed. To execute the **balance number** command, you must remove the setting by using the **undo** form of the command; and vice versa.

**Modified feature: Multicast BGP load balancing**

Feature change description

This release enables you to implement load balancing over MBGP routes learned from either IBGP peers or EBGP peers.

Command changes

Modified command: balance

Old syntax

```plaintext
balance number
undo balance
```

New syntax

```plaintext
balance [ ebgp | ibgp ] number
undo balance [ ebgp | ibgp ]
```

Views

MBGP address family view, IPv6 MBGP address family view

Parameters

**ebgp**: Configures load balancing over MBGP routes learned from EBGP peers.

**ibgp**: Configures load balancing over MBGP routes learned from IBGP peers.

**number**: Specifies the maximum number of multicast MBGP routes for load balancing. When it is set to 1, load balancing is disabled.

Change description

Before modification: Multicast BGP does not differentiate between MBGP routes learned from IBGP peers and those learned from EBGP peers, and it uses all available MBGP routes to implement load balancing.
After modification: You can use the `ebgp` or `ibgp` keyword to implement load balancing over MBGP routes learned from either IBGP peers or EBGP peers. If you do not specify the `ibgp` or `ebgp` keyword, this command enables load balancing over all MBGP routes. After you execute the `balance ibgp number` command or the `balance ebgp number` command, the `balance number` command cannot be executed. To execute the `balance number` command, you must first use the undo form of the `balance ibgp number` or `balance ebgp number` command to remove the former configuration; and vice versa.
This release has the following changes:

- New feature: Configuring switch-MDT
- New feature: Configuring multicast VPN inter-AS option B

### New feature: Configuring switch-MDT

#### Configuring switch-MDT

##### Overview

Multicast VPN is a technique that implements multicast delivery in VPNs.

If the multicast VPN feature is enabled for a VPN instance, the multicast packet of a VPN is transmitted through the share-MDT on the public network. All PE devices that support that VPN instance receive the multicast packet, no matter whether any active receivers exist in the attached sites. This might occupy large network resources and add extra burden on the PE devices.

To optimize multicast transmission, the MD solution establishes a dedicated switch-MDT between the PE devices connected to the VPN multicast receivers or multicast sources. Then, the multicast stream is switched from the share-MDT to the switch-MDT, to deliver the multicast data to only those receivers that need it.

#### Table 8 Basic concepts in switch-MDT

<table>
<thead>
<tr>
<th>Concept</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch-multicast distribution tree (Switch-MDT)</td>
<td>A switch-MDT is an MDT that uses a switch-group as it group address. At MDT switchover, PE devices with downstream receivers join a switch-group, forming a switch-MDT, along which the ingress PE forwards the encapsulated VPN multicast traffic over the public network.</td>
</tr>
<tr>
<td>Switch-group</td>
<td>When the multicast traffic of a VPN keeps arriving, the PE device assigns it an independent multicast address called switch-group, and notifies the other PE devices that they should use that address to forward the multicast traffic for that VPN. This initiates a switchover to the switch-MDT.</td>
</tr>
<tr>
<td>Switch-group-pool</td>
<td>The switch-group-pool is a range of multicast addresses. At MDT switchover, an address (namely, switch-group address) is chosen from the switch-group-pool. The multicast packets for the VPN that enter the public network at the PE device will be encapsulated using that address. The switch-group-pool of a VPN must not overlap that of another VPN, and must not contain the share-group of another VPN.</td>
</tr>
</tbody>
</table>

##### Introduction to switch-MDT

The following describes how the switch-MDT is implemented in a MD VPN:

- The public network of the service provider supports multicast:
  - The PE devices must support the public network and multiple VPN instances.
  - Each instance runs PIM independently.
VPN multicast traffic between the PE devices and the CE devices is transmitted on a per-VPN-instance basis, and the public network multicast traffic between the PE devices and the P devices is transmitted through the public network.

- Each VPN instance is assigned a unique share-group address. The VPN data is transparent to the public network.

A PE device encapsulates any VPN multicast packet within a normal public network multicast packet, no matter what multicast group the VPN packet is destined for or whether it is a protocol packet or a data packet. The PE device uses the share-group as the public network multicast group for the packet. Then, the PE sends the public network multicast packet onto the public network.

- A share-group corresponds to a unique MD. For each share-group, a unique share-MDT is constructed through the public network resources for multicast data forwarding. All the VPN multicast packets transmitted in this VPN are forwarded along this share-MDT, no matter at which PE device they entered the public network.

- A share-group is assigned a unique switch-group-pool for MDT switchover. When a VPN multicast stream that entered the public network at a PE device keeps arriving for a certain period of time, the PE chooses an idle address (namely, switch-group) from the switch-group-pool, and encapsulates the multicast packets for that VPN using that address.

- All the ingress PE devices in the network monitor the forwarding rate on the share-MDT:
  a. When a VPN multicast stream that entered the public network at a specific PE device keeps arriving for a certain period of time, the PE device initiates an MDT switchover message to the downstream along the share-MDT. This makes a switch-MDT to be built by using the switch-group between that PE device and the remote PE devices with receivers downstream.
  b. After a switch-delay period has passed, a switchover from the share-MDT to the switch-MDT starts.

All VPN multicast packets that have entered the public network at that PE device are encapsulated into public network multicast packets using the switch-group, instead of using the share-group, so that they are switched from the share-MDT to the switch-MDT.

A VPN uniquely corresponds to an MD and an MD serves only one VPN, which is called a "one-to-one relationship." Such a relationship exists between VPN, MD, MTI, share-group, and switch-group-pool.

For information about MD, MDT, MT, MTI, share-group, and share-MDT, see IP multicast Configuration Guide in HP 5820X&5800 Switch Series Configuration Guides.

Switching from share-MDT to switch-MDT

The process of share-MDT to switch-MDT switchover is as follows:

3. The source-side PE (PE 1 in this example) device periodically examines the forwarding traffic of the VPN multicast data. The switchover from the share-MDT to switch-MDT takes place only when the following criteria are both met:
   o The VPN multicast data has passed the filtering by an ACL rule for share-MDT to switch-MDT switchover.
   o The VPN multicast data has been forwarded for a certain period of time.

4. PE 1 chooses an idle switch-group address from the switch-group-pool and sends an MDT switchover message to all the other PE devices down the share-MDT. This message contains the VPN multicast source address, the VPN multicast group address and the switch-group address.

5. Each PE device that receives this message examines whether it interfaces with a VPN that has receivers of that VPN multicast stream. If so, it joins the switch-MDT rooted at PE 1. Otherwise, it caches the message and will join the switch-MDT when it has attached receivers.
6. After sending the MDT switchover message, PE 1 waits a certain period of time and then starts using the switch-group address to encapsulate the VPN multicast data, so that the multicast data is forwarded down the switch-MDT.

7. After the multicast traffic is switched from the share-MDT to the switch-MDT, PE 1 continues sending MDT switchover messages periodically, so that subsequent PE devices with attached receivers can join the switch-MDT. When a downstream PE device has no longer active receivers attached to it, it leaves the switch-MDT.

For a given VPN instance, the share-MDT and the switch-MDT are both forwarding tunnels in the same MD. A share-MDT is uniquely identified by a share-group address, and a switch-MDT is uniquely identified by a switch-group address. Each share-group is uniquely associated with a set of switch-group addresses, namely, a switch-group-pool.

NOTE:
When BIDIR-PIM is running on the public network or private network, switch-MDT switchover is not supported.

Backward switching from switch-MDT to share-MDT

After the VPN multicast traffic is switched to the switch-MDT, the multicast traffic conditions might change and no longer meet the aforesaid switchover criterion. In this case, PE 1, as in the preceding example, initiates a backward MDT switchover process. When any of the following criteria is met, the multicast traffic is switched from the switch-MDT back to the share-MDT:

- No VPN multicast data has been forwarded for a certain period of time (namely, the switch-hold down period).
- The associated switch-group-pool is changed and the switch-group address for encapsulating the VPN multicast data is out of the new address pool.
- The ACL rule for controlling the switching of VPN multicast traffic from the share-MDT to the switch-MDT is changed and the VPN multicast data fails to pass the new ACL rule.

Configuring switch-MDT

⚠️ CAUTION:
When BIDIR-PIM is running on the public network, do not configure switch-group. Otherwise, multicast packets cannot be correctly transmitted on the public network.

Configuring MDT switchover parameters

To avoid frequent switchover between the share-MDT and the switch-MDT:

- MDT switchover does not take place immediately after the source-side PE receives the first VPN multicast packet that matches the permit statement in the ACL. Instead, the PE starts a switch-delay timer. If the source-side PE keeps receiving VPN multicast packets that match the permit statement in the ACL when the switch-delay timer expires, a switchover from the share-MDT to the switch-MDT occurs. Otherwise, the share-MDT is still used.

- Likewise, a backward switching does not take place immediately after the source-side PE stops receiving VPN multicast packets that match the permit statement in the ACL. Instead, the PE starts a switch-hold down timer. If the source-side PE does not receive any VPN multicast packet that matches the permit statement in the ACL when the switch-hold down timer expires, a switchover from the switch-MDT to the share-MDT occurs. Otherwise, the switch-MDT is still used.

Perform the following configuration on the PE.

To configure MDT switchover parameters:
### Enabling switch-group reuse logging

For a given VPN, if the number of VPN multicast streams to be switched to switch-MDTs exceeds the number of addresses in the switch-group-pool, the VPN instance on the source-side PE device can reuse the addresses in the address pool. With switch-group reuse logging enabled, the address reuse information will be logged.

Perform the following configuration on the PE.

To enable the switch-group reuse logging:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter VPN instance view.</td>
<td>ip vpn-instance vpn-instance-name</td>
<td>N/A</td>
</tr>
<tr>
<td>3. Enable the switch-group reuse logging.</td>
<td>multicast-domain switch-group-reuse</td>
<td>Disabled by default.</td>
</tr>
</tbody>
</table>

**NOTE:**

- Attributed to the MD module, the group address reuse logging information has a severity level of informational. For more information about the logging information, see *Network Management and Monitoring Configuration Guide in HP 5820X&5800 Switch Series Configuration Guides*.

- When switch-group reuse logging is enabled, the generated group address reuse logging information will be sent to the information center, where you can configure the rules for outputting the logging information. For more information about the configuration of the information center, see *Network Management and Monitoring Configuration Guide in HP 5820X&5800 Switch Series Configuration Guides*.

### Displaying and maintaining switch-MDT

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display switch-group information received by the specified VPN instance in the MD.</td>
<td>display multicast-domain vpn-instance vpn-instance-name switch-group receive [ brief ] [ active</td>
<td>group group-address</td>
</tr>
<tr>
<td>Display switch-group information</td>
<td>display multicast-domain vpn-instance</td>
<td>Available in any view.</td>
</tr>
<tr>
<td>Task</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>sent by the specified VPN instance in the MD.</td>
<td>`vpn-instance-name switch-group send [group group-address</td>
<td>reuse interval</td>
</tr>
</tbody>
</table>

**Command reference**

display multicast-domain vpn-instance switch-group receive

Use `display multicast-domain vpn-instance switch-group receive` to display the switch-group information received by the specified VPN instance in the MD.

**Syntax**

```
display multicast-domain vpn-instance vpn-instance-name switch-group receive [ brief | [active | group group-address | sender source-address | vpn-source-address [mask {mask-length | mask}] | vpn-group-address [mask {mask-length | mask}] | * ] [ [begin | exclude | include] regular-expression] ]
```

**Views**

Any view

**Default command level**

1: Monitor level

**Parameters**

- `vpn-instance-name`: Name of an MPLS L3VPN instance, a case-sensitive string of 1 to 31 characters.
- `brief`: Displays the brief switch-group information received by the specified VPN instance.
- `active`: Displays the received switch-group information about active multicast domains.
- `group-address`: Public network multicast group address, in the range of 224.0.1.0 to 239.255.255.
- `source-address`: Public network multicast source address.
- `vpn-source-address`: VPN multicast source address.
- `mask`: Subnet mask of the specified VPN multicast source/group address, 255.255.255.255 by default.
- `mask-length`: Mask length of the specified multicast source/group address, in the range of 0 to 32. The system default is 32.
- `vpn-group-address`: VPN multicast group address, in the range of 224.0.0.0 to 239.255.255.

`: 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 switch-group information received by VPN instance mvpn in the MD.
```
<Sysname> display multicast-domain vpn-instance mvpn switch-group receive
MD switch-group information received by VPN-Instance: mvpn
Total 2 switch-groups for 8 entries
Total 2 switch-groups for 8 entries matched
switch group: 226.1.1.0 ref count: 4, active count: 2
  sender: 172.100.1.1 active count: 1
    (192.6.1.5, 239.1.1.1) expire time: 00:03:10 active
    (192.6.1.5, 239.1.1.158) expire time: 00:03:10
  sender: 181.100.1.1 active count: 1
    (195.6.1.2, 239.1.2.12) expire time: 00:03:10 active
    (195.6.1.2, 239.1.2.197) expire time: 00:03:10
switch group: 229.1.1.0 ref count: 4, active count: 2
  sender: 185.100.1.1 active count: 1
    (198.6.1.5, 239.1.3.62) expire time: 00:03:10 active
    (198.6.1.5, 225.1.1.109) expire time: 00:03:10
  sender: 190.100.1.1 active count: 1
    (200.6.1.2, 225.1.4.80) expire time: 00:03:10 active
    (200.6.1.2, 225.1.4.173) expire time: 00:03:10
# Display the brief switch-group information received by VPN instance mvpn in the MD.
<Sysname> display multicast-domain vpn-instance mvpn switch-group receive brief
MD switch-group information received by VPN-Instance: mvpn
Total 2 switch-groups for 8 entries
Total 2 switch-groups for 8 entries matched
switch group: 226.1.1.0 ref count: 4, active count: 2
switch group: 229.1.1.0 ref count: 4, active count: 2

Table 9 Command output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MD switch-group information received by VPN-Instance: mvpn</td>
<td>Switch-group information received by VPN instance mvpn.</td>
</tr>
<tr>
<td>Total 2 switch-groups for 8 entries</td>
<td>Totally two switch-groups, corresponding to eight (S, G) entries.</td>
</tr>
<tr>
<td>Total 2 switch-groups for 8 entries matched</td>
<td>Totally two switch-groups are matched, corresponding to eight (S, G) entries.</td>
</tr>
<tr>
<td>switch group</td>
<td>Switch-group address received.</td>
</tr>
<tr>
<td>sender</td>
<td>BGP peer address of the PE device that sent the switch-group information.</td>
</tr>
<tr>
<td>ref count</td>
<td>Number of VPN multicast groups referenced by the switch-group.</td>
</tr>
<tr>
<td>active count</td>
<td>Number of active VPN multicast groups (multicast groups with active receivers) referenced by the switch-group.</td>
</tr>
<tr>
<td>expire time</td>
<td>Remaining time of the VPN (S, G) entry referenced by the switch-group.</td>
</tr>
</tbody>
</table>
Related commands

display multicast-domain vpn-instance switch-group send

display multicast-domain vpn-instance switch-group send

Use display multicast-domain vpn-instance switch-group send to display the switch-group information sent by the specified VPN instance in the MD.

Syntax

display multicast-domain vpn-instance vpn-instance-name switch-group send [ group group-address | reuse interval | vpn-source-address [ mask { mask-length | mask } ] | vpn-group-address [ mask { mask-length | mask } ] ] * [ | { begin | exclude | include } regular-expression ]

Views

Any view

Default command level

1: Monitor level

Parameters

vpn-instance-name: Name of an MPLS L3VPN instance, a case-sensitive string of 1 to 31 characters.
group-address: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.
reuse interval: Displays the information about switch-group reuses that took place during the specified length of time in seconds. The value range of interval is 1 to 2147483647.
vpn-source-address: VPN multicast source address.
mask: Subnet mask of the specified VPN multicast source/group address, 255.255.255.255 by default.
mask-length: Mask length of the specified multicast source/group address, in the range of 0 to 32. The system default is 32.
vpn-group-address: VPN multicast group address, in the range of 224.0.0.0 to 239.255.255.255.
regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Examples

# Display the switch-group information sent by VPN instance mvpn in the MD.
<Sysname> display multicast-domain vpn-instance mvpn switch-group send
MD switch-group information sent by VPN-Instance: mvpn
Total 2 switch-groups for 6 entries

Total 2 switch-groups for 6 entries matched

226.1.1.0 reference_count: 3
(192.6.1.5, 239.1.1.1) switch time: 00:00:21
(192.6.1.5, 239.1.1.158) switch time: 00:00:21
# Display the switch-group reuse information sent by VPN instance mvpn during 30 seconds in the MD.

display multicast-domain vpn-instance mvpn switch-group send reuse 30
MD switch-group information sent by VPN-Instance: mvpn

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MD switch-group information sent by VPN-Instance: mvpn</td>
<td>Switch-group information sent by VPN instance mvpn.</td>
</tr>
<tr>
<td>Total 2 switch-groups for 6 entries</td>
<td>Totally two switch-groups, corresponding to six (S, G) entries.</td>
</tr>
<tr>
<td>Total 2 switch-groups for 6 entries matched</td>
<td>Totally two switch-groups are matched, corresponding to six (S, G) entries.</td>
</tr>
<tr>
<td>reference_count</td>
<td>Number of VPN multicast groups referenced by the sent switch-group.</td>
</tr>
<tr>
<td>switch time</td>
<td>Switching time of the VPN (S, G) entry referenced by the switch-group.</td>
</tr>
<tr>
<td>reuse_count</td>
<td>Number of switch-group reuses during the specified length of time.</td>
</tr>
</tbody>
</table>

Related commands

- display multicast-domain vpn-instance switch-group receive
- multicast-domain holddown-time

Use `multicast-domain holddown-time` to configure the switch-holddown period.
Use `undo multicast-domain holddown-time` to restore the default.

Syntax

```
multicast-domain holddown-time interval
```

Default

- The switch-holddown period is 60 seconds.

Views

- VPN instance view
Default command level
2: System level

Parameters
interval: Switch-holddown period in seconds, namely, the delay time before multicast traffic to be switched from the share-MDT back to the share-MDT, in the range of 0 to 180.

Usage guidelines
This command cannot be configured without previous share-MDT configuration in the VPN instance.

Examples
# Set the switch-holddown period to 80 seconds in VPN instance mvpn.
<Sysname> system-view
<Sysname-vpn-instance-mvpn> multicast-domain holddown-time 80

multicast-domain log switch-group-reuse

Use multicast-domain log switch-group-reuse to enable switch-group reuse logging.
Use undo multicast-domain log to disable switch-group reuse logging.

Syntax
multicast-domain log switch-group-reuse
undo multicast-domain log

Default
The switch-group reuse logging function is disabled.

Views
VPN instance view

Default command level
2: System level

Usage guidelines
This command cannot be configured without the previous share-MDT configuration in the VPN instance.

Examples
# Enable switch-group reuse logging in VPN instance mvpn.
<Sysname> system-view
<Sysname-vpn-instance-mvpn> multicast-domain log switch-group-reuse

multicast-domain switch-delay

Use multicast-domain switch-delay to configure the switch-delay period.
Use undo multicast-domain switch-delay to restore the default.

Syntax
multicast-domain switch-delay switch-delay
undo multicast-domain switch-delay
Views
VPN instance view

Default command level
2: System level

Parameters

switch-delay: Switch-delay period in seconds, namely, the delay time for multicast traffic to be switched from the share-MDT to the switch-MDT, in the range of 3 to 60.

Default
The switch-delay period is 5 seconds.

Examples
# Set the switch-delay period to 20 seconds in VPN instance mvpn.
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] multicast-domain switch-delay 20

multicast-domain switch-group-pool

Use multicast-domain switch-group-pool to configure the address range of the switch-group-pool and the switching condition.

Use undo multicast-domain switch-group-pool to restore the default.

Syntax

multicast-domain switch-group-pool switch-group-pool { mask | mask-length } [ acl acl-number ] *
undo multicast-domain switch-group-pool

Default
No switch-group-pool is configured and multicast traffic is never switched to a switch-MDT.

Views
VPN instance view

Default command level
2: System level

Parameters

switch-group-pool: The start address of the switch-group-pool, in the range of 224.0.1.0 to 239.255.255.255.

mask: Mask for addresses in the switch-group-pool.

mask-length: Mask length for addresses in the switch-group-pool, in the range of 25 to 32.

acl-number: Advanced ACL number, in the range of 3000 to 3999. An advanced ACL defines the (S, G) entry or entries to which the configured MDT switching condition applies. If you do not specify an ACL, the configured MDT switching condition applies to all (S, G) entries. When configuring this ACL, specify the protocol type as IP and use the source and destination parameters to specify a multicast source address range and a multicast group address range, respectively.

Usage guidelines
This command cannot be configured without the previous share-MDT configuration in the VPN instance.
On a given PE device, the switch-group address range for a VPN must not contain the share-group of any VPN.

On a given PE device, the switch-group address range for a VPN instance must not overlap with that for any other VPN instance. A new configuration with this command in the same VPN instance supersedes the existing configuration.

If you use the `multicast-domain switch-group-pool` command on a switch, share-MDT to switch-MDT switching will take place after the switch receives multicast traffic for this VPN instance and has maintained it for the switch-delay period.

**Examples**

```
# Configure the address range of the switch-group-pool in VPN instance mvpn as 225.2.2.0 to 225.2.2.15.
<Sysname> system-view
<Sysname> ip vpn-instance mvpn
<Sysname-vpn-instance-mvpn] multicast-domain switch-group-pool 225.2.2.0 28
```

**Related commands**

`multicast-domain switch-delay`

**New feature: Configuring multicast VPN inter-AS option B**

Configuring multicast VPN inter-AS option B

The multicast VPN inter-AS option B feature implements inter-AS multicast VPN in an inter-AS option B network. This new feature enables protocols packets to carry RPF proxy vector and BGP connector information.

The RPF proxy vector is used on the public network to create a correct share-MDT, and the BGP connector is used on the private network to create a correct forwarding entry.

For more information about multicast VPN, see *IP Multicast Configuration Guide* in *HP 5820X&5800 Switch Series Configuration Guides*.

For more information about inter-AS option B, see *MPLS Configuration Guide* in *HP 5820X&5800 Switch Series Configuration Guides*.

**Share-MDT establishment by using RPF proxy vector on public networks**

In a multicast VPN inter-AS option B network, the unicast routes between different ASs are isolated, so the unicast routing table cannot be used to create a share-MDT. However, different PEs can exchange BGP-MDT routing information, so the BGP MDT routing table can be used to create a share-MDT. BGP MDT can be configured only on the public network running PIM-SSM.

For more information about BGP MDT, see *IP Multicast Configuration Guide* in *HP 5820X&5800 Switch Series Configuration Guides*. 
Share-MDT establishment process

As shown in Figure 1, the process of establishing a share-MDT is as follows:

1. Different PEs exchange their BGP MDT routing information with each other on the public network.
2. PE 1 prepares to send a PIM join message to PE 2, but does not find a unicast route to PE 2. It checks the received BGP MDT information, and determines that the next hop to PE 2 is ASBR 1 and the next hop address is the address of interface Loop 0 on ASBR 1. This next hop address is referred to as the "RPF vector." The RPF vector is a proxying address for the remote PE. It is used by other devices in the same AS for upstream neighbor address check. Therefore, the RPF vector is also called the "RPF proxy vector."

PE 1 encapsulates the RPF vector information in a PIM join message.
3. According to the RPF vector, PE 1 finds out that its upstream interface is connected to P 1. PE 1 sends the PIM join message to P 1.
4. After receiving the PIM join message from PE 1, P 1 implements the RPF vector check. P 1 finds out that the RPF vector is not on the local network and that the upstream interface is connected to ASBR 1. Therefore, it forwards the PIM join message to ASBR 1.
5. After receiving the PIM join message from P 1, ASBR 1 implements the RPF vector check and finds out that the RPF vector is on the local network. Then, by looking up the BGP MDT information, ASBR 1 determines that the next hop to PE 2 is ASBR 2 and there is a unicast route to ASBR 2. ASBR 1 forwards the PIM join message to ASBR 2.
6. After receiving the PIM join message from ASBR 1, ASBR 2 removes the RPF vector information in the PIM join message because a unicast route to PE 2 exists. Then, ASBR 2 unicasts the PIM join message to PE 2 hop by hop.
7. When the PIM join message arrives at PE 2, the share-MDT from PE 1 to PE 2 is created. After that, PE 2 initiates a similar process to establish the share-MDT from PE 2 to PE 1.

The share-MDT establishment for the multicast VPN inter-AS option B network is completed.

Configuring the multicast RPF proxy vector feature

Configure the multicast RPF proxy vector feature on each PE device (excluding ASBR) in different ASs.

To make HP switches compatible with other manufacturers' products, you also need to configure the multicast RPF proxy vector compatibility feature on each HP switch.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a VPN instance, and enter VPN instance view.</td>
<td>ip vpn-instance, vpn-instance-name</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>3.</td>
<td>Enable the multicast RPF</td>
<td>By default, the multicast RPF proxy vector feature is disabled for the</td>
</tr>
<tr>
<td></td>
<td>proxy vector feature for the</td>
<td>VPN instance.</td>
</tr>
<tr>
<td></td>
<td>VPN instance.</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Enable the multicast RPF</td>
<td>By default, the multicast RPF proxy vector compatibility feature</td>
</tr>
<tr>
<td></td>
<td>proxy vector compatibility</td>
<td></td>
</tr>
<tr>
<td></td>
<td>feature.</td>
<td></td>
</tr>
</tbody>
</table>

Upstream neighbor address check by using BGP connector on a private network

When a PE device sends a PIM join message for private network to a peer PE through the MTI, it looks up its unicast routing table and use the next hop address as the upstream neighbor address. After receiving the PIM join message, one of the following occurs:

- In an intra-AS network, the upstream neighbor address corresponds to the incoming interface address of the remote PE, the upstream neighbor address check succeeds.
- In an inter-AS network without BGP connector enabled, the upstream neighbor address is the incoming interface address of the ASBR in the local AS, the upstream neighbor address check fails.

To make sure the PIM join message passes the upstream neighbor address check in a multicast VPN inter-AS option B network, the following conditions must be met:

- BGP peers need to carry in their VPNv4 routing exchange messages the BGP connectors (IP addresses of the BGP peers).
- The PE devices need to fill the BGP connector in the upstream neighbor address field when they send a PIM join message to their peer PEs.

Configuration example

Network requirements

As shown in Figure 2:

- Site 1 and Site 2 belong to the same VPN. CE 1 of Site 1 accesses the network through PE 1 in AS 100 and CE 2 of Site 2 accesses the network through PE 2 in AS 600. PEs in the same AS run IS-IS.
- PE 1 and ASBR-PE 1 exchange labeled IPv4 routes by MP-IBGP. PE 2 and ASBR-PE 2 exchange labeled IPv4 routes by MP-IBGP. ASBR-PE 1 and ASBR-PE 2 exchange labeled IPv4 routes by MP-EBGP.
- ASBRs do not perform route target filtering of received VPN-IPv4 routes.

Perform the following configuration to implement multicast VPN:

- Enable PIM-SSM on the public network, and configure the SSM multicast group range as 232.0.0.0/8.
- Configure an MD VPN on the public network, and bind the share-group address 232.1.1.1 with a VPN instance on the PEs (non-ASBR).
- Configure a BGP MDT on the PEs and ASBRs.
Figure 2 Network diagram

Table 1 Interface and IP address assignment

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>PE 1</td>
<td>Loop0</td>
<td>2.2.2.9/32</td>
<td>PE 2</td>
<td>Loop0</td>
<td>5.5.5.9/32</td>
</tr>
<tr>
<td>PE 1</td>
<td>Vlan-int12</td>
<td>30.0.0.1/8</td>
<td>PE 2</td>
<td>Vlan-int12</td>
<td>20.0.0.1/8</td>
</tr>
<tr>
<td>PE 1</td>
<td>Vlan-int11</td>
<td>1.1.1.2/8</td>
<td>PE 2</td>
<td>Vlan-int11</td>
<td>9.1.1.2/8</td>
</tr>
<tr>
<td>ASBR-PE 1</td>
<td>Loop0</td>
<td>3.3.3.9/32</td>
<td>ASBR-PE 2</td>
<td>Loop0</td>
<td>4.4.4.9/32</td>
</tr>
<tr>
<td>ASBR-PE 1</td>
<td>Vlan-int11</td>
<td>1.1.1.1/8</td>
<td>ASBR-PE 2</td>
<td>Vlan-int11</td>
<td>9.1.1.1/8</td>
</tr>
<tr>
<td>ASBR-PE 1</td>
<td>Vlan-int12</td>
<td>11.0.0.2/8</td>
<td>ASBR-PE 2</td>
<td>Vlan-int12</td>
<td>11.0.0.1/8</td>
</tr>
</tbody>
</table>

Configuration procedure

1. Configure PE 1:
   # Enable IP multicast routing for the public network, configure LSR ID, and enable MPLS and LDP.
   <PE1> system-view
   [PE1] multicast routing-enable
   [PE1] mpls lsr-id 2.2.2.9
   [PE1] mpls
   [PE1-mpls] label advertise non-null
   [PE1-mpls] quit
   [PE1] mpls ldp
   [PE1-mpls-ldp] quit
   # Configure interface VLAN-interface 11, enable MPLS, LDP and PIM-SM on the interface.
   [PE1] interface vlan-interface 11
   [PE1-Vlan-interface11] ip address 1.1.1.2 255.0.0.0
   [PE1-Vlan-interface11] mpls
   [PE1-Vlan-interface11] mpls ldp
   [PE1-Vlan-interface11] pim sm
# Configure interface Loopback 0 and enable PIM-SM on the interface.
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 2.2.2.9 32
[PE1-LoopBack0] pim sm
[PE1-LoopBack0] quit

# Create VPN instance vpn1 and configure the RD and route target attributes.
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] route-distinguisher 11:11
[PE1-vpn-instance-vpn1] vpn-target 3:3 import-extcommunity
[PE1-vpn-instance-vpn1] vpn-target 3:3 export-extcommunity

# Enable IP multicast routing for VPN instance vpn1, configure a share-group address, and enable multicast RPF proxy vector.
[PE1-vpn-instance-vpn1] multicast routing-enable
[PE1-vpn-instance-vpn1] multicast-domain share-group 232.1.1.1 binding mtunnel 0
[PE1-vpn-instance-vpn1] multicast rpf proxy vector
[PE1-vpn-instance-vpn1] quit

# Create service loopback group 1 and specify its service type as multicast tunnel.
[PE1] service-loopback group 1 type multicast-tunnel

# Select an unused available interface, disable spanning tree protocols, LLDP, and NDP on the interface, and add the interface to service loopback group 1.
[PE1] interface gigabitethernet1/0/3
[PE1-GigabitEthernet1/0/3] undo stp enable
[PE1-GigabitEthernet1/0/3] undo ndp enable
[PE1-GigabitEthernet1/0/3] undo lldp enable
[PE1-GigabitEthernet1/0/3] port service-loopback group 1
[PE1-GigabitEthernet1/0/3] quit

# Bind the interface connected with CE 1 to the created VPN instance and enable PIM-SM on the interface.
[PE1] interface vlan-interface 12
[PE1-Vlan-interface12] ip binding vpn-instance vpn1
[PE1-Vlan-interface12] ip address 30.0.0.1 8
[PE1-Vlan-interface12] pim sm
[PE1-Vlan-interface12] quit

# Enable OSPF on PE 1 for the public network and VPN instance vpn1, and redistribute BGP routes to the VPN routing table of vpn1.
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.2 0.255.255.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
[PE1]ospf 2 vpn-instance vpn1
[PE1-ospf-2] import-route bgp
[PE1-ospf-2] area 0
[PE1-ospf-2-area-0.0.0.0] network 30.0.0.1 0.255.255.255
[PE1-ospf-2-area-0.0.0.0] quit
[PE1-ospf-2] quit
# Enable BGP on PE 1.

[PE1] bgp 100

# Configure IBGP peer 3.3.3.9 as a VPNv4 peer.

[PE1-bgp] peer 3.3.3.9 as-number 100
[PE1-bgp] peer 3.3.3.9 connect-interface loopback 0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpnv4] peer 3.3.3.9 enable
[PE1-bgp-af-vpnv4] quit

# Configure a BGP MDT peer.

[PE1-bgp] ipv4-family mdt
[PE1-bgp-af-mdt] peer 3.3.3.9 enable
[PE1-bgp-af-mdt] quit

# Redistribute direct routes and OSPF routes to the VPN routing table of vpn1.

[PE1-bgp] ipv4-family vpn-instance vpn1
[PE1-bgp-vpn1] import-route direct
[PE1-bgp-vpn1] import-route ospf 2
[PE1-bgp-vpn1] quit
[PE1-bgp] quit

2. Configure ASBR-PE 1:

# Enable IP multicast routing for the public network, configure LSR ID, and enable MPLS and LDP.

<ASBR-PE1> system-view
[ASBR-PE1] multicast routing-enable
[ASBR-PE1] mpls lsr-id 3.3.3.9
[ASBR-PE1] mpls
[ASBR-PE1-mpls] label advertise non-null
[ASBR-PE1-mpls] quit
[ASBR-PE1] mpls ldp
[ASBR-PE1-mpls-ldp] quit

# Configure interface VLAN-interface 11, and enable MPLS, LDP and PIM-SM on the interface.

[ASBR-PE1] interface vlan-interface 11
[ASBR-PE1-Vlan-interface11] ip address 1.1.1.1 255.0.0.0
[ASBR-PE1-Vlan-interface11] mpls
[ASBR-PE1-Vlan-interface11] mpls ldp
[ASBR-PE1-Vlan-interface11] pim sm
[ASBR-PE1-Vlan-interface11] quit

# Configure interface VLAN-interface 12, and enable MPLS and PIM-SM on the interface.

[ASBR-PE1] interface vlan-interface 12
[ASBR-PE1-Vlan-interface12] ip address 11.0.0.2 255.0.0.0
[ASBR-PE1-Vlan-interface12] mpls
[ASBR-PE1-Vlan-interface12] mpls ldp
[ASBR-PE1-Vlan-interface12] pim sm
[ASBR-PE1-Vlan-interface12] quit

# Configure interface Loopback 0 and enable PIM-SM on the interface.

[ASBR-PE1] interface loopback 0
[ASBR-PE1-LoopBack0] ip address 3.3.3.9 32
[ASBR-PE1-LoopBack0] pim sm
[ASBR-PE1-LoopBack0] quit

# Enable OSPF on ASBR-PE 1.
**Configure ASBR-PE 1:**

- Enable BGP on ASBR-PE 1.
  
  ```
  [ASBR-PE1-bgp] peer 2.2.2.9 as-number 100
  [ASBR-PE1-bgp] peer 2.2.2.9 connect-interface loopback 0
  [ASBR-PE1-bgp] peer 11.0.0.1 as-number 600
  # Disable route target based filtering of received VPNv4 routes.
  # Configure both IBGP peer 2.2.2.0 and EBGP peer 11.0.0.1 as VPNv4 peers.
  [ASBR-PE1-bgp-af-vpnv4] peer 11.0.0.1 enable
  [ASBR-PE1-bgp-af-vpnv4] peer 2.2.2.9 enable
  # Configure BGP MDT peers.
  [ASBR-PE1-bgp-af-mdt] peer 11.0.0.1 enable
  [ASBR-PE1-bgp-af-mdt] peer 2.2.2.9 enable
  ```

**Configure ASBR-PE 2:**

- Enable IP multicast routing for the public network, configure LSR ID, and enable MPLS and LDP.
  
  ```
  <ASBR-PE2> system-view
  [ASBR-PE2] multicast routing-enable
  [ASBR-PE2] mpls lsr-id 4.4.4.9
  [ASBR-PE2-mpls] label advertise non-null
  [ASBR-PE2-mpls] quit
  [ASBR-PE2] mpls ldp
  [ASBR-PE2-mpls-ldp] quit
  # Configure interface VLAN-interface 11, and enable MPLS, LDP, and PIM-SM on the interface.
  [ASBR-PE2-Vlan-interface11] ip address 9.1.1.1 255.0.0.0
  [ASBR-PE2-Vlan-interface11] mpls
  [ASBR-PE2-Vlan-interface11] mpls ldp
  [ASBR-PE2-Vlan-interface11] pim sm
  [ASBR-PE2-Vlan-interface11] quit
  # Configure interface VLAN-interface 12, and enable MPLS and PIM-SM on the interface.
  [ASBR-PE2-Vlan-interface12] ip address 11.0.0.1 255.0.0.0
  [ASBR-PE2-Vlan-interface12] mpls
  [ASBR-PE2-Vlan-interface12] pim sm
  [ASBR-PE2-Vlan-interface12] quit
  # Configure interface Loopback 0 and enable PIM-SM on the interface.
  ```
4. Configure PE 2:

# Enable OSPF on ASBR-PE 2.
[ASBR-PE2] ospf
[ASBR-PE2-ospf-1] area 0
[ASBR-PE2-ospf-1-area-0.0.0.0] network 4.4.4.9 0.0.0.0
[ASBR-PE2-ospf-1-area-0.0.0.0] network 9.1.1.1 0.255.255.255
[ASBR-PE2-ospf-1-area-0.0.0.0] quit
[ASBR-PE2-ospf-1] quit

# Enable BGP on ASBR-PE 2.
[ASBR-PE2] bgp 600
[ASBR-PE2-bgp] peer 11.0.0.2 as-number 100
[ASBR-PE2-bgp] peer 5.5.5.9 as-number 600
[ASBR-PE2-bgp] peer 5.5.5.9 connect-interface loopback 0

# Disable route target based filtering of received VPNv4 routes.
[ASBR-PE2-bgp] ipv4-family vpnv4

# Configure both IBGP peer 5.5.5.9 and EBGP peer 11.0.0.2 as VPNv4 peers.
[ASBR-PE2-bgp-af-vpnv4] peer 11.0.0.2 enable
[ASBR-PE2-bgp-af-vpnv4] peer 5.5.5.9 enable
[ASBR-PE2-bgp-af-vpnv4] quit

# Configure BGP MDT peers.
[ASBR-PE2-bgp] ipv4-family mdt
[ASBR-PE2-bgp-af-mdt] peer 11.0.0.2 enable
[ASBR-PE2-bgp-af-mdt] peer 5.5.5.9 enable
[ASBR-PE2-bgp-af-mdt] quit

# Enable BGP on ASBR-PE 2.
[ASBR-PE2] bgp 600
[ASBR-PE2-bgp] peer 11.0.0.2 as-number 100
[ASBR-PE2-bgp] peer 5.5.5.9 as-number 600
[ASBR-PE2-bgp] peer 5.5.5.9 connect-interface loopback 0

# Disable route target based filtering of received VPNv4 routes.
[ASBR-PE2-bgp] ipv4-family vpnv4

# Configure both IBGP peer 5.5.5.9 and EBGP peer 11.0.0.2 as VPNv4 peers.
[ASBR-PE2-bgp-af-vpnv4] peer 11.0.0.2 enable
[ASBR-PE2-bgp-af-vpnv4] peer 5.5.5.9 enable
[ASBR-PE2-bgp-af-vpnv4] quit

# Configure BGP MDT peers.
[ASBR-PE2-bgp] ipv4-family mdt
[ASBR-PE2-bgp-af-mdt] peer 11.0.0.2 enable
[ASBR-PE2-bgp-af-mdt] peer 5.5.5.9 enable
[ASBR-PE2-bgp-af-mdt] quit

Configure PE 2:

# Enable IP multicast routing for the public network, configure LSR ID, and enable MPLS and LDP.
<PE2> system-view
[PE2] multicast routing-enable
[PE2] mpls lsr-id 5.5.5.9
[PE2] mpls
[PE2-mpls] label advertise non-null
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit

# Configure interface VLAN-interface 11, and enable MPLS, LDP, and PIM-SM on the interface.
[PE2] interface vlan-interface 11
[PE2-Vlan-interface11] ip address 9.1.1.2 255.0.0.0
[PE2-Vlan-interface11] mpls
[PE2-Vlan-interface11] mpls ldp
[PE2-Vlan-interface11] pim sm
[PE2-Vlan-interface11] quit

# Configure interface Loopback 0 and enable PIM-SM on the interface.
[PE2] interface loopback 0
# Create VPN instance vpn1 and configure the RD and route target attributes.

```
[PE2] ip vpn-instance vpn1
[PE2-vpn-instance-vpn1] route-distinguisher 11:11
[PE2-vpn-instance-vpn1] vpn-target 3:3 import-extcommunity
[PE2-vpn-instance-vpn1] vpn-target 3:3 export-extcommunity
```

# Enable IP multicast routing for VPN instance vpn1, configure a share-group address, and enable multicast RPF proxy vector.

```
[PE2-vpn-instance-vpn1] multicast routing-enable
[PE2-vpn-instance-vpn1] multicast-domain share-group 232.1.1.1 binding mtunnel 0
[PE2-vpn-instance-vpn1] multicast rpf proxy vector
[PE2-vpn-instance-vpn1] quit
```

# Create service loopback group 1 and specify its service type as multicast tunnel.

```
[PE2] service-loopback group 1 type multicast-tunnel
```

# Select an unused available interface, disable spanning tree protocols, LLDP, and NDP on the interface, and add the interface to service loopback group 1.

```
[PE2] interface gigabitethernet1/0/3
[PE2-GigabitEthernet1/0/3] undo stp enable
[PE2-GigabitEthernet1/0/3] undo ndp enable
[PE2-GigabitEthernet1/0/3] undo lldp enable
[PE2-GigabitEthernet1/0/3] port service-loopback group 1
[PE2-GigabitEthernet1/0/3] quit
```

# Bind the interface connected with CE 2 to the created VPN instance and enable PIM-SM on the interface.

```
[PE2] interface vlan-interface 12
[PE2-Vlan-interface12] ip binding vpn-instance vpn1
[PE2-Vlan-interface12] ip address 20.0.0.1 8
[PE2-Vlan-interface12] pim sm
[PE2-Vlan-interface12] quit
```

# Enable OSPF on PE2 for the public network and VPN instance vpn1, and redistribute the BGP routes to the VPN routing table of vpn1.

```
<PE2> system-view
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 5.5.5.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 9.1.1.2 0.255.255.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
[PE2] ospf 2 vpn-instance vpn1
[PE2-ospf-2] import-route bgp
[PE2-ospf-2] area 0
[PE2-ospf-2-area-0.0.0.0] network 20.0.0.1 0.255.255.255
[PE2-ospf-2-area-0.0.0.0] quit
[PE2-ospf-2] quit
```

# Enable BGP on PE 2.

```
[PE2] bgp 600
```
# Configure IBGP peer 4.4.4.9 as a VPNv4 peer.
[PE2-bgp] peer 4.4.4.9 as-number 600
[PE2-bgp] peer 4.4.4.9 connect-interface loopback 0
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp-af-vpnv4] peer 4.4.4.9 enable
[PE2-bgp-af-vpnv4] quit

# Configure a BGP MDT peer.
[PE2-bgp] ipv4-family mdt
[PE2-bgp-af-mdt] peer 4.4.4.9 enable
[PE2-bgp-af-mdt] quit

# Redistribute direct routes and OSPF routes to the VPN routing table of vpn1.
[PE2-bgp] ipv4-family vpn-instance vpn1
[PE2-bgp-vpn1] import-route direct
[PE2-bgp-vpn1] import-route ospf 2
[PE2-bgp-vpn1] quit
[PE2-bgp] quit

Command reference

This section introduces only the new and modified commands for multicast VPN.

For more information about other commands for multicast VPN inter-AS option B, see IP multicast Command Reference in HP 5820X&5800 Switch Series Command Reference.

For more information about other commands for inter-AS option B, see MPLS Command Reference in HP 5820X&5800 Switch Series Command Reference.

New command: multicast rpf proxy vector

Use multicast rpf proxy vector to enable the multicast RPF proxy vector feature for a VPN instance.

Use undo multicast rpf proxy to restore the default.

Syntax

multicast rpf proxy vector
undo multicast rpf proxy vector

Default

The multicast RPF proxy vector feature is not enabled in a VPN instance.

Views

VPN instance view

Default command level

2: System level

Usage guidelines

You can enable the multicast RPF proxy vector feature on a PE device for inter-AS VPN implementation. After you enable this feature, the PE device carries the RPF vector information in PIM join messages. The RPF vector information is used to create a correct share-MDT on the public network.

Examples

# Enable the multicast RPF proxy vector feature for VPN instance mvpn.
New command: multicast rpf-proxy-vector compatible

Use **multicast rpf-proxy-vector compatible** to enable multicast RPF proxy vector compatibility. Use **undo multicast rpf-proxy-vector compatible** to restore the default.

**Syntax**

```
multicast rpf-proxy-vector compatible
undo multicast rpf-proxy-vector compatible
```

**Default**

Multicast RPF proxy vector compatibility is disabled.

**Views**

System view

**Default command level**

2: System level

**Usage guidelines**

You must enable multicast RPF proxy vector compatibility on each device on the public network to make the devices compatible with other manufacturers' products for interoperability purposes.

**Examples**

```
# Enable multicast RPF proxy vector compatibility.
<Sysname> system-view
<Sysname> multicast rpf-proxy-vector compatible
```

Modified command: display pim routing-table

**Syntax**

```
display pim [ all-instance | vpn-instance vpn-instance-name ] routing-table [ group-address [ mask { mask-length | mask } ] | source-address [ mask { mask-length | mask } ] | incoming-interface [ interface-type interface-number | register ] | outgoing-interface { include | exclude | match } { interface-type interface-number | register } | mode mode-type | flags flag-value | fsm ] * [ | { begin | exclude | include } regular-expression ]
```

**Views**

Any view

**Examples**

```
# Display PIM routing table information on the public network.
<Sysname> display pim routing-table
VPN-Instance: public net
Total 0 (*, G) entry; 1 (S, G) entry

(6.6.6.9, 232.0.0.1)
   Protocol: pim-ssm, Flag:
   UpTime: 02:54:43
   Upstream interface: Vlan-interface1
```
Upstream neighbor: 20.0.3.4
RPF prime neighbor: 20.0.3.4

RPF Vector: 20.0.3.4

Downstream interface(s) information:
Total number of downstreams: 2
1: Vlan-interface2
   Protocol: pim-ssm, UpTime: 23:24:33, Expires: 00:02:57
1: VPN-Instance: vpn1
   Protocol: MD, UpTime: 02:54:43, Expires: -

# Display the state machine information in the PIM routing table on the public network.
<Sysname> display pim routing-table fsm

VPN-Instance: public net
Total 0 (*, G) entry; 1 (S, G) entry

Abbreviations for FSM states:
   NI - no info, J - joined, NJ - not joined, P - pruned,
   NP - not pruned, PP - prune pending, W - winner, L - loser,
   F - forwarding, AP - ack pending, DR - designated router,
   NDR - non-designated router, RCV - downstream receivers

(6.6.6.9, 232.0.0.1)
   Protocol: pim-ssm, Flag: SPT LOC ACT
   UpTime: 02:54:43
   Upstream interface: Vlan-interface1
     Upstream neighbor: 20.0.3.4
     RPF prime neighbor: 20.0.3.4
RPF Vector: 20.0.3.4
   Join/Prune FSM: [J]

Downstream interface(s) information:
Total number of downstreams: 2
1: Vlan-interface2
   Protocol: pim-ssm, UpTime: 23:26:31, Expires: 00:02:59
   DR state: [NDR]
   Join/Prune FSM: [J]
   Assert FSM: [NI]
1: VPN-Instance: vpn1
   Protocol: MD, UpTime: 02:54:43, Expires: -
   DR state: [DR]
   Join/Prune FSM: [NI]
   Assert FSM: [NI]

FSM information for non-downstream interfaces: None

Change description

After modification, the display pim routing-table command and the display pim routing-table fsm command display RPF vector information.
Modified command: display pim neighbor

Syntax

display pim [ all-instance | vpn-instance vpn-instance-name ] neighbor [ interface interface-type interface-number | neighbor-address | verbose ] * [ | { begin | exclude | include } regular-expression ]

Views

Any view

Examples

# Display information about all PIM neighbors on the public network.
<Sysname> display pim neighbor
VPN-Instance: public net
Total Number of Neighbors = 2

    Neighbor     Interface          Uptime     Expires  Dr-Priority  Mode
    10.1.1.2     Vlan1             02:50:49   00:01:31  1            V
    20.1.1.2     Vlan2             02:49:39   00:01:42  1            V

# On the public network, display detailed information about the PIM neighbor whose IP address is 11.110.0.20.
<Sysname> display pim neighbor 11.110.0.20 verbose
VPN-Instance: public net
Neighbor: 11.110.0.20
    Interface: Vlan-interface3
    Uptime: 00:00:10
    Expiry time: 00:00:30
    DR Priority: 1
    Generation ID: 0x2ACEFE15
    Holdtime: 105 s
    LAN delay: 500 ms
    Override interval: 2500 ms
    State refresh interval: 60 s
    Neighbor tracking: Disabled
    Bidirectional PIM: Disabled
    RPF Vector: Enabled

Change description

After modification:

- The display pim neighbor command displays a new mode ("v") in the Mode field in the output. The field value of "v" means that the RPF proxy vector feature is enabled on the PIM neighbor.
- The display pim neighbor verbose command displays whether the RPF proxy vector feature is enabled on all PIM neighbors.
This release has no feature changes.
This release has the following changes:
- New feature: Enabling MAC authentication multi-VLAN mode

**New feature: Enabling MAC authentication multi-VLAN mode**

**Overview**

By default, a MAC authentication-enabled port forwards packets for an authenticated user only in the VLAN where the user is authenticated. If the user forwards packets in a different VLAN, the port must re-authenticate the user. After the user passes re-authentication, the port will update the MAC and VLAN mapping of the user. For a user that sends various types of traffic (for example, data, video, and audio) in multiple VLANs, frequent MAC re-authentication can downgrade the system performance and affect data transmission quality.

The MAC authentication multi-VLAN mode enables a MAC authentication-enabled port to forward packets for an authenticated user in up to five VLANs without re-authentication.

For example, an IP phone can send tagged and untagged frames, the IP phone is connected to a MAC authentication-enabled port, and the port receives tagged frames in VLAN 2 and untagged frames in VLAN 1. Before you enable the multi-VLAN mode on the port, the port must re-authenticate the IP phone repeatedly, because it sends tagged frames and untagged frames alternately in different VLANs. After you enable the multi-VLAN mode, the port can receive tagged and untagged frames alternately from the IP phone without triggering a MAC re-authentication. The multi-VLAN mode improves the transmission quality of data that is vulnerable to delay and interference.

**Configuration procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>mac-authentication host-mode multi-vlan</td>
<td>By default, A MAC-authenticated user only can forward packets in the VLAN where it was authenticated.</td>
</tr>
</tbody>
</table>

**Command reference**

mac-authentication host-mode multi-vlan

**Syntax**

mac-authentication host-mode multi-vlan
undo mac-authentication host-mode multi-vlan
View
   Layer 2 Ethernet interface view

Default level
   2: System level

Description
   Use mac-authentication host-mode multi-vlan to enable MAC authentication multi-VLAN mode
   on a port.
   Use undo mac-authentication host-mode multi-vlan to restore the default.
   By default, the MAC authentication multi-VLAN mode is disabled on a port.
   The multi-VLAN mode enables a MAC-authenticated user to forward packets in multiple VLANs on
   the port without re-authentication. The device supports a maximum of four such VLANs on a port.

Examples
   # Enable MAC authentication multi-VLAN mode on port GigabitEthernet 1/0/2.
   <Sysname> system-view
   [Sysname] interface gigabitethernet 1/0/2
   [Sysname-GigabitEthernet1/0/2] mac-authentication host-mode multi-vlan
This release has the following changes:
- New feature: Supporting multicast routing and forwarding based on secondary IP addresses

**New feature: Supporting multicast routing and forwarding based on secondary IP addresses**

Multicast routing and forwarding based on secondary IP addresses

Previous software versions support multicast routing and forwarding based on only primary IP addresses even if secondary IP addresses are configured on the interface. In this version, the switch sends PIM hello packets that contain a list of secondary IP addresses, which is obtained and maintained by its PIM neighbors. In this way, multicast packets can be forwarded to the segments indicated by primary and secondary IP addresses.

The switch sends PIM hello packets only to PIM routers that are on the segments indicated by their primary IP addresses and PIM neighbor relationship is established based only on the primary IP addresses.

For more information about primary and secondary IP addresses, see *Layer 3—IP Services Configuration Guide*.

**Command reference**

**Modified command: display pim neighbor**

**Syntax**

```
display pim [ all-instance | vpn-instance vpn-instance-name ] neighbor [ interface interface-type interface-number | neighbor-address | verbose ] * [ | { begin | exclude | include } regular-expression ]
```

**Views**

Any view

**Default command level**

1: Monitor level

**Parameters**

- `all-instance`: Specifies all VPN instances.
- `vpn-instance vpn-instance-name`: Specifies a VPN, where `vpn-instance-name` is a case-sensitive string of 1 to 31 characters.
- `interface interface-type interface-number`: Displays the PIM neighbor information on a particular interface.
- `neighbor-address`: Displays the information of a particular PIM neighbor.
- `verbose`: Displays the detailed PIM neighbor 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.

Usage guidelines

If neither all-instance nor vpn-instance is specified, this command displays information about all PIM neighbors in the public network.

Examples

# In the public network, display detailed information about the PIM neighbor (11.110.0.20).
<Sysname> display pim neighbor 11.110.0.20 verbose

VPN-Instance: public net
Neighbor: 11.110.0.20
    Interface: Vlan-interface3
    Uptime: 00:00:10
    Expiry time: 00:00:30
    DR Priority: 1
    Generation ID: 0x2ACEFE15
    Holdtime: 105 s
    LAN delay: 500 ms
    Override interval: 2500 ms
    State refresh interval: 60 s
    Neighbor tracking: Disabled
    Bidirectional PIM: Disabled
    Neighbor Secondary Address(es):
      11.110.1.20
      11.110.2.20
      11.110.3.20

Table 11 Command output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN-Instance: public net</td>
<td>Public network.</td>
</tr>
<tr>
<td>Total Number of Neighbors</td>
<td>Total number of PIM neighbors.</td>
</tr>
<tr>
<td>Neighbor</td>
<td>IP address of the PIM neighbor.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface that connects to the PIM neighbor.</td>
</tr>
<tr>
<td>Uptime</td>
<td>Length of time for which the PIM neighbor has been up, in hh:mm:ss.</td>
</tr>
<tr>
<td>Expires/Expiry time</td>
<td>Remaining time of the PIM neighbor, in hh:mm:ss. &quot;Never&quot; means that the PIM neighbor is always up and reachable.</td>
</tr>
<tr>
<td>Dr-Priority/DR Priority</td>
<td>Priority of the PIM neighbor.</td>
</tr>
<tr>
<td>Mode</td>
<td>Mode of the PIM neighbor. The value &quot;B&quot; means the BIDIR-PIM mode. If nothing is displayed, it means the non-BIDIR-PIM mode.</td>
</tr>
<tr>
<td>Generation ID</td>
<td>Generation ID of the PIM neighbor. (A random value that indicates a status change of the PIM neighbor.)</td>
</tr>
<tr>
<td>Holdtime</td>
<td>Holdtime of the PIM neighbor; &quot;forever&quot; means that the PIM neighbor is always up and reachable.</td>
</tr>
<tr>
<td>LAN delay</td>
<td>Prune message delay.</td>
</tr>
<tr>
<td>Override interval</td>
<td>Prune override interval.</td>
</tr>
<tr>
<td>State refresh interval</td>
<td>Interval for sending state refresh messages.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Displayed only when the PIM neighbor operates in PIM-DM mode and the state refresh capability is enabled.</td>
</tr>
<tr>
<td>Neighbor tracking</td>
<td>Neighbor tracking status (enabled/disabled).</td>
</tr>
<tr>
<td>Bidirectional PIM</td>
<td>BIDIR-PIM status (enabled/disabled).</td>
</tr>
<tr>
<td>Neighbor Secondary Address(es)</td>
<td>Secondary IP addresses of the PIM neighbor.</td>
</tr>
</tbody>
</table>

**Change description**

Before modification: No secondary IP addresses are displayed in the detailed PIM neighbor information.

After modification: Secondary IP addresses are displayed in the detailed PIM neighbor information.
This release has the following changes:

- New feature: Configuring a criterion to match the packet length
- New feature: Configuring a multiport ARP entry
- New feature: Configuring a multiport unicast MAC address entry
- New feature: Configuring LLDP to advertise a specific voice VLAN
- Modified feature: Looped-port status processing mechanism
- Modified feature: Portal redirection
- Modified feature: Implementing ACL-based IPsec
- Modified feature: Executing a batch file
- Modified feature: Configuring system information for the SNMP agent

**New feature: Configuring a criterion to match the packet length**

Configuring a criterion to match the packet length

A criterion to match the packet length is effective on only IP packets.

The packet length includes the IP header length and IP datagram length. It does not include the Ethernet frame header length.

To configure a criterion to match the packet length:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Create a class and enter class view.</td>
<td>traffic classifier classifier-name [ operator { and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
3. Configure a criterion to match the packet length.

**if-match packet-length**

Use `if-match packet-length` to configure a criterion to match the packet length.

**Syntax**

```plaintext
if-match packet-length { min min-value | max max-value } *
```

**Views**

Traffic class view

**Default command level**

2: System level

**Parameters**

- **min min-value**: Specifies the minimum packet length in the range of 1 to 2000 bytes.
- **max max-value**: Specifies the maximum packet length in the range of 1 to 2000 bytes. If you configure both the `min min-value` and `max max-value` options, `max-value` must be greater than `min-value`.

**Examples**

```plaintext
# Define a match criterion for class class to match packets longer than 1000 bytes and shorter than 1500 bytes.
<Sysname> system-view
[Sysname] traffic classifier class
[Sysname-classifier-class]if-match packet-length min 1000 max 1500
```
New feature: Configuring a multiport ARP entry

Configuring a multiport ARP entry

For a multiport ARP entry, the multicast or multiport unicast MAC address entry specifies the VLAN ID and output ports, and the static ARP entry specifies the VPN and the IP address. A multiport ARP entry is never overwritten by a dynamic, or static ARP entry.

The multiport ARP entry does not take effect if the corresponding VLAN interface is not created, is down, or does not match the specified VPN. Thus, packets matching it are discarded. It takes effect when the VLAN interface is up, and matches the specified VPN.

The static ARP entry uses its MAC address to find a matching multicast or multiport unicast MAC address entry. If the MAC address exists in multiple VLANs, the static ARP entry uses the MAC address that has the smallest VLAN ID to generate the multiport ARP entry.

When multiport ARP entries reach the maximum number, the static ARP entry and the matching multicast or multiport unicast MAC address entry cannot generate a multiport ARP entry. In addition, they cannot automatically generate the multiport ARP entry when any existing multiport ARP entries are removed. You need to manually configure them again.

To configure a multiport ARP entry:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure a multicast or multiport unicast MAC address entry.</td>
<td>- Configure a multiport unicast MAC address entry: <code>mac-address multiport mac-address interface interface-list vlan vlan-id</code>&lt;br&gt;- Configure a multicast MAC address entry: <code>mac-address multicast mac-address interface interface-list vlan vlan-id</code></td>
</tr>
<tr>
<td>3.</td>
<td>Configure a static ARP entry</td>
<td><code>arp static ip-address mac-address vlan-id [vpn-instance vpn-instance-name]</code></td>
</tr>
</tbody>
</table>

Command reference

For more information about multiport unicast MAC address entries, see "New feature: Configuring a multiport unicast MAC address entry." For more information about multicast MAC address entries, see IP Multicast Command Reference. For more information about static ARP entries, see Layer 3—IP Services Command Reference.
New feature: Configuring a multiport unicast MAC address entry

Configuring a multiport unicast MAC address entry

You can configure a multiport unicast MAC address entry to associate a unicast MAC address with multiple ports, so that a frame that matches the entry is forwarded out of multiple ports. For example, in NLB unicast mode, all servers within the cluster use the cluster's MAC address as their own address, and frames destined for the cluster are forwarded to every server. In this case, you can configure a multiport unicast MAC address entry on the device connected to the group of servers. In this manner, the device forwards the frame destined for the server group through all ports connected to the servers within the cluster.

Figure 1 NLB cluster

Configuring a multiport unicast MAC address entry globally

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure a multiport unicast MAC address entry for the specified interfaces.</td>
<td>mac-address multiport mac-address interface interface-list vlan vlan-id</td>
</tr>
</tbody>
</table>

Configuring a multiport unicast MAC address entry on the specified interfaces
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view or port group view.</td>
<td>Use either command. Settings in Layer 2 Ethernet interface view or Layer 2 aggregate interface view take effect on the interface only. Settings in port group view take effect on all member ports in the port group.</td>
</tr>
<tr>
<td>3.</td>
<td>Configure a multiport unicast MAC address entry for the interface or interfaces.</td>
<td>By default, no multiport unicast MAC address entry is configured. Make sure that you have created the VLAN and assigned the interface or interfaces to the VLAN. Do not configure an interface as the output interface of a multiport unicast MAC address entry if the interface receives frames destined for the multiport unicast MAC address. Otherwise, the frames are flooded in the VLAN to which they belong.</td>
</tr>
</tbody>
</table>

### Displaying multiport unicast MAC address entries

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the multiport unicast MAC address entries.</td>
<td>`display mac-address multiport [ vlan vlan-id ] [ count ] [</td>
<td>{ begin</td>
</tr>
</tbody>
</table>

### Command reference

**display mac-address multiport**

Use `display mac-address multiport` to display multiport unicast MAC address entries.

**Syntax**

```
display mac-address multiport [ vlan vlan-id ] [ count ] [ | { begin | exclude | include } regular-expression ]
```

**Views**

Any view

**Default command level**

1: Monitor level

**Parameters**

- `vlan vlan-id`: Displays multiport unicast MAC address entries of the specified VLAN, where `vlan-id` ranges from 1 to 4094.
- `count`: Displays the number of multiport unicast MAC address entries.
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

```bash
# Display multiport unicast MAC address entries.
<Sysname> display mac-address multiport

<table>
<thead>
<tr>
<th>MAC ADDR</th>
<th>VLAN ID</th>
<th>STATE</th>
<th>PORT INDEX</th>
<th>AGING TIME(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001-0101-0101</td>
<td>2</td>
<td>Multiport</td>
<td>GigabitEthernet1/0/1</td>
<td>NOAGED</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GigabitEthernet1/0/2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GigabitEthernet1/0/3</td>
<td></td>
</tr>
</tbody>
</table>

--- 1 mac address(es) found ---
```

### Table 12 Command output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC ADDR</td>
<td>MAC address.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>ID of the VLAN to which the MAC address belongs.</td>
</tr>
<tr>
<td>STATE</td>
<td>State of a MAC address entry. <strong>Multiport</strong> indicates a multiport unicast MAC address entry manually configured by the user.</td>
</tr>
<tr>
<td>PORT INDEX</td>
<td>Outgoing port for packets that are destined for the MAC address.</td>
</tr>
<tr>
<td>AGING TIME</td>
<td>Aging time. <strong>NOAGED</strong> indicates that the entry does not age.</td>
</tr>
<tr>
<td>mac address(es) found</td>
<td>Number of matching MAC address entries.</td>
</tr>
</tbody>
</table>

### mac-address multiport (interface view)

Use **mac-address multiport** to configure a multiport unicast MAC address entry for the specified interface.

Use **undo mac-address multiport** to remove a multiport unicast MAC address entry for the interface.

**Syntax**

```bash
mac-address multiport mac-address vlan vlan-id
undo mac-address multiport mac-address vlan vlan-id
```

**Default**

No multiport unicast MAC address entry is configured.

**Views**

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

**Default command level**

2: System level
Parameters

`mac-address`: Specifies a unicast MAC address, excluding the all-zero MAC address.

`vlan vlan-id`: Specifies an existing VLAN to which the Ethernet interface belongs, where `vlan-id` is the specified VLAN ID, ranging from 1 to 4094.

Examples

```
# Add a multiport unicast MAC address entry for MAC address 0001-0001-0101 on port Ethernet 1/1
# that belongs to VLAN 2.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address multiport 0001-0001-0101 vlan 2
```

`mac-address multiport` (system view)

Use `mac-address multiport` to configure a multiport unicast MAC address entry for the specified interfaces.

Use `undo mac-address multiport` to remove a multiport unicast MAC address entry for the specified interfaces.

Syntax

```
mac-address multiport mac-address interface interface-list vlan vlan-id
undo mac-address multiport mac-address interface interface-list vlan vlan-id
undo mac-address [ multiport ] [ [ mac-address ] vlan vlan-id ]
```

Default

No multiport unicast MAC address entry is configured.

Views

System view

Default command level

2: System level

Parameters

`mac-address`: Specifies a unicast MAC address, excluding the all-zero MAC address.

`interface-list`: Specifies interfaces in the format of `{ { interface-type interface-number } [ to
{ interface-type interface-number } ] } &<1-4>`. The interface type can be the Layer 2 Ethernet
interface or Layer 2 aggregate interface. &<1-4> specifies that you can configure up to four
interfaces or interface ranges.

`vlan-id`: Specifies an existing VLAN to which the Ethernet interface belongs, where `vlan-id` is the
specified VLAN ID, ranging from 1 to 4094.

Usage guidelines

If you execute the `undo mac-address multiport` command without specifying the `multiport`
keyword, this command deletes all MAC address entries (including multicast MAC address entries,
multiport unicast MAC address entries, and unicast MAC address entries).

Examples

```
# Add a multiport unicast MAC address entry for MAC address 000f-e201-0101 to send all frames
destined to this MAC address out of ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3
# that belong to VLAN 2.
<Sysname> system-view
```
**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 hone 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 2 shows the procedure of voice VLAN advertisement through LLDP.

**Figure 2 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view or port group view.</td>
<td>• Enter Layer 2 Ethernet interface view: <code>interface interface-type interface-number</code>&lt;br&gt;• Enter port group view: <code>port-group manual</code></td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>3.</td>
<td>Configure LLDP to advertise a specific voice VLAN.</td>
<td>By default, LLDP advertises the voice VLAN configured on the port.</td>
</tr>
</tbody>
</table>

### 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**

```plaintext
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**

```plaintext
# Configure port GigabitEthernet 1/0/1 to advertise voice VLAN 4094.
<Sysname> system-view
<Sysname> interface gigabitethernet 1/0/1
<Sysname-GigabitEthernet1/0/1] lldp voice-vlan 4094
```
Modified feature: Looped-port status processing mechanism

Feature change description

Before modification: If a port's loopback protection action is shutdown, the system automatically shuts down the port when it detects a loop on the port, leaving the port in Loop down state at the physical layer. After the loop is removed, you must execute the undo shutdown command on the port to restore the port's forwarding capability.

After modification: The system automatically starts a port status detection timer when a port is shut down because of a loopback. After the timer expires, the system automatically brings up the port to restore its forwarding capability. The timer is 30 seconds by default. You can use the shutdown-interval time command to change the timer. Setting the timer to 0 disables the automatic forwarding capability restoration function. For more information about the shutdown-interval time command, see Fundamentals Command Reference.

Command changes

None

Modified feature: Portal redirection

Feature change description

Before modification: After you enable Layer 3 portal authentication, the device redirects all HTTP requests from unauthenticated users to the portal server.

After modification: After you enable Layer 3 portal authentication, the device examines whether an HTTP request is from a browser after it receives the HTTP request from an unauthenticated users. If yes, the device redirects the request to the portal server. Otherwise, the device directly drop the request. This can protect the portal server from receiving a large number of HTTP packets sent from terminal users through software, and protect the portal server from being occupied in processing such packets.

Command changes

None

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.
IPsec configuration example

Network requirements
As shown in Figure 3, 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 3 Network diagram**

![Network diagram](image)

Configuration procedure
IKE configuration is supported only when the switches operate in FIPS mode.

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 transform set named tran1.
   [SwitchA] ipsec transform-set tran1
   # Specify the encapsulation mode as tunnel.
   [SwitchA-ipsec-transform-set-tran1] encapsulation-mode tunnel
   # Specify the security protocol as ESP.
   [SwitchA-ipsec-transform-set-tran1] transform esp
   # Specify the algorithms for the proposal.
   [SwitchA-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
   [SwitchA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
   [SwitchA-ipsec-transform-set-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 transform set.
   [SwitchA-ipsec-policy-isakmp-map1-10] transform-set 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 transform set named tran1.
[SwitchB] ipsec transform-set tran1

# Specify the encapsulation mode as tunnel.
[SwitchB-ipsec-transform-set-tran1] encapsulation-mode tunnel

# Specify the security protocol as ESP.
[SwitchB-ipsec-transform-set-tran1] transform esp

# Specify the algorithms for the proposal.
[SwitchB-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
[SwitchB-ipsec-transform-set-tran1] esp authentication-algorithm shal
[SwitchB-ipsec-transform-set-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 transform set.
[SwitchB-ipsec-policy-isakmp-use1-10] transform-set 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 4, 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 4 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 transform set tran1.
   [SwitchA] ipsec transform-set tran1

   # Set the packet encapsulation mode to tunnel.
   [SwitchA-ipsec-transform-set-tran1] encapsulation-mode tunnel

   # Use security protocol ESP.
   [Switch-ipsec-transform-set-tran1] transform esp

   # Specify encryption and authentication algorithms.
   [SwitchA-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
   [SwitchA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
   [SwitchA-ipsec-transform-set-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 transform set tran1.
[SwitchA-ipsec-policy-isakmp-map1-10] transform-set 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 an IPsec transform set named tran1.
[SwitchB] ipsec transform-set tran1

# Set the packet encapsulation mode to tunnel.
[SwitchB-ipsec-transform-set-tran1] encapsulation-mode tunnel

# Use security protocol ESP.
[SwitchB-ipsec-transform-set-tran1] transform esp

# Specify encryption and authentication algorithms.
[SwitchB-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
[SwitchB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[SwitchB-ipsec-transform-set-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 transform set tran1.
[SwitchB-ipsec-policy-isakmp-use1-10] transform-set 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: Executing a batch file

Feature change description

Removed the requirement for the extension of the batch file.

Command changes

Modified command: execute

Syntax

execute filename

Views

System view

Change description

Before modification: The batch file must use .bat as the extension.
After modification: The batch file can use any extension.

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.
This release has the following changes:

- New feature: FIPS
- New feature: Configuring ACL-based IPsec
- New feature: IKE
- New feature: Disabling password recovery capacity
- New feature: Verifying the correctness and integrity of the file
- New feature: Enabling MAC address migration log notifying
- New feature: Configuring packet capture
- New feature: Enabling log file overwrite-protection
- New feature: Setting the MTU of the VPLS instance
- New feature: Configuring an OSPFv3 NSSA area
- 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: Displaying RPS status 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 an 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.

If you enable or disable the FIPS mode on an IRF fabric, restart the IRF fabric to make your configuration take effect.

In FIPS mode, the switch does not support Telnet logins.

Enabling the FIPS mode

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable the FIPS mode.</td>
<td>fips mode enable</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2. Trigger a self-test.</td>
<td>fips self-test</td>
</tr>
</tbody>
</table>

Displaying and maintaining FIPS

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display FIPS mode state</td>
<td>display fips status</td>
<td>Available in any view.</td>
</tr>
</tbody>
</table>

FIPS configuration example

Network requirements

The PC connects to the switch through a console port. Configure the switch to operate in FIPS mode and create a local user for the PC so that the PC can log in to the switch.

Network diagram

**Figure 1 Network diagram**

![Network Diagram](image)

Configuration procedure

1. Configure the 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 to **terminal**, privilege level to **3**, and password to **AAbbcc1234%**. The password must contain at least 10 characters by default and must contain both uppercase and lowercase letters, digits, and special characters. Configure the password in interactive mode.

```bash
[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.

```bash
[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.

```bash
<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. To solve this problem, 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
# Display the current FIPS mode.
<Sysname> display fips status
FIPS mode is enabled

Related commands
fips mode enable

fips self-test

Use fips self-test to trigger a self-test on the password algorithms.

Syntax
fips self-test

Views
System view

Default command level
3: Manage level

Usage guidelines
To examine whether the cryptography modules operate normally, you can use a command to trigger a self-test on the cryptographic algorithms. The triggered self-test is the same as the power-up self-test.

If the self-test fails, the device automatically reboots.

Examples
# Trigger a self-test on the cryptographic algorithms.
<Sysname> system-view
[Sysname] fips self-test
Self-tests are running. Please wait...
Self-tests succeeded.

New feature: Configuring ACL-based IPsec

NOTE:
- The term router in this document refers to both routers and switches.
- IKE configuration is available for only the switches in FIPS mode. For information about the FIPS mode, see New feature: FIPS.
- A switch in IRF mode does not support IPsec automatic negotiation.

Configuring ACL-based IPsec

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.

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 transform sets to specify the security protocols, and authentication and encryption algorithms.
3. Configure IPsec policies to associate data flows with IPsec transform sets 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.

Complete the following tasks to configure ACL-based IPsec:

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring ACLs</td>
<td>Required</td>
</tr>
<tr>
<td>Configuring an IPsec transform set</td>
<td>Basic IPsec configuration</td>
</tr>
<tr>
<td>Configuring an IPsec policy</td>
<td></td>
</tr>
<tr>
<td>Applying an IPsec policy group to an interface</td>
<td></td>
</tr>
<tr>
<td>Configuring the IPsec session idle timeout</td>
<td>Optional</td>
</tr>
<tr>
<td>Enabling ACL checking of de-encapsulated IPsec packets</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the IPsec anti-replay function</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring packet information pre-extraction</td>
<td>Optional</td>
</tr>
<tr>
<td>Enabling invalid SPI recovery</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring IPsec RRI</td>
<td>Optional</td>
</tr>
</tbody>
</table>

⚠️ **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.

To use IPsec in combination with QoS, make sure that 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*.

For more information about ACL configuration, see *ACL and QoS Configuration Guide*.

### 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. For the outbound traffic, IPsec uses the source and destination IP addresses specified in the rule to match the source and destination IP addresses of the traffic. For the returned inbound traffic, IPsec uses the destination IP address and the source IP address specified in the rule to match the source IP address and the destination IP address of the traffic.
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:
- Non-IPsec 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 defining ACL rules 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.
- Do not use ACLs referenced by IPsec for other services.
- Make sure you create a mirror image ACL rule on the remote peer for each ACL rule created at the local peer. Otherwise, IPsec may protect traffic only in one direction.

**Mirror image ACLs**

To make sure that SAs can be set up and the traffic protected by IPsec can be processed correctly at the remote peer, on the remote peer, create a mirror image ACL rule for each ACL rule created at the local peer.

If the ACL rules on peers do not form mirror images of each other, SAs can be set up only when both of the following requirements are met:
- The range specified by an ACL rule on one peer is covered by its counterpart ACL rule on the other peer.
- The peer with the narrower rule initiates SA negotiation. If a wider ACL rule is used by the SA initiator, the negotiation request may be rejected because the matching traffic is beyond the scope of the responder.

**Protection mode**

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.

**Configuring an IPsec transform set**

This section is not newly added. In this version, related commands that are executed in FIPS mode were modified.

An IPsec transform set, part of an IPsec policy, defines the security parameters for IPsec SA negotiation, including the security protocol, and the encryption and authentication algorithms.

To configure an IPsec transform set:
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create an IPsec transform set and enter its view.</td>
<td>ipsec transform-set transform-set-name</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the security protocol for the IPsec transform set.</td>
<td>transform { ah</td>
</tr>
<tr>
<td>4.</td>
<td>Specify the security algorithms.</td>
<td>• Specify the encryption algorithm for ESP: (In non-FIPS mode) esp encryption-algorithm { 3des</td>
</tr>
<tr>
<td>5.</td>
<td>Specify the IP packet encapsulation mode for the IPsec transform set.</td>
<td>encapsulation-mode { transport</td>
</tr>
</tbody>
</table>

**NOTE:**
Changes to an IPsec transform set 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.
Configuring an IPsec policy

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."

IPsec policies define which IPsec transform sets 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.

NOTE:
The IKE negotiation mode is supported only in FIPS mode.

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 transform sets 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 transform sets used by the IPsec policies on all routers must have the same security protocols, security algorithms, and encapsulation mode. 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 neighbor 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 transform sets. ACLs are not required for IPsec policies for an IPv6 protocol.

To configure a manual IPsec policy:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ipsec policy <strong>policy-name</strong> seq-number manual</td>
<td>By default, no IPsec policy exists.</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>3.</td>
<td>security acl acl-number</td>
<td>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. An IPsec policy can reference only one ACL. If you apply multiple ACLs to an IPsec policy, only the last one takes effect.</td>
</tr>
<tr>
<td>4.</td>
<td>transform-set transform-set-name</td>
<td>By default, an IPsec policy references no IPsec transform set. A manual IPsec policy can reference only one IPsec transform set. To change an IPsec transform set for an IPsec policy, you must remove the reference first.</td>
</tr>
<tr>
<td>5.</td>
<td>tunnel local ip-address</td>
<td>Not needed for IPsec policies to be applied to IPv6 routing protocols and required for other applications. Not configured by default.</td>
</tr>
<tr>
<td>6.</td>
<td>tunnel remote ip-address</td>
<td>Not needed for IPsec policies to be applied to IPv6 routing protocols and required for other applications. Not configured by default.</td>
</tr>
<tr>
<td>7.</td>
<td>sa spi { inbound</td>
<td>outbound } { ah</td>
</tr>
</tbody>
</table>
8. Configure keys for the SA.

- Configure an authentication key in hexadecimal for AH:
  \[\text{sa authentication-hex \{ inbound | outbound \} ah \{ cipher | simple \} hex-key}\]
- Configure an authentication key in characters for AH:
  \[\text{sa string-key \{ inbound | outbound \} ah \{ cipher | simple \} string-key}\]
- Configure a key in characters for ESP:
  \[\text{sa string-key \{ inbound | outbound \} esp \{ cipher | simple \} string-key}\]
- Configure an authentication key in hexadecimal for ESP:
  \[\text{sa authentication-hex \{ inbound | outbound \} esp \{ cipher | simple \} hex-key}\]
- Configure an encryption key in hexadecimal for ESP:
  \[\text{sa encryption-hex \{ inbound | outbound \} esp \{ cipher | simple \} hex-key}\]

Configure keys properly for the security protocol (AH or ESP) you have specified.
If you configure a key in two modes: string and hexadecimal, only the last configured one will be used.
If you configure a key in characters for ESP, the system automatically generates an authentication key and an encryption key for ESP.
For ESP, if you configure an authentication key, the system automatically generates an authentication key and an encryption key.
The \text{sa string-key} command is not supported in FIPS mode.

NOTE:
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.

Configuring an IPsec policy that uses IKE

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, complete the following tasks:
- Configure the ACLs and the IPsec transform sets for the IPsec policy.
- To use IKE version 1 (IKEv1) negotiation, configure the IKE peer. For more information about IKE peer configuration, see "Configuring IKE."

The parameters for the local and remote ends must match.
To configure an IPsec policy that uses IKE:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ipsec policy policy-name seq-number isakmp</td>
<td>By default, no IPsec policy exists.</td>
</tr>
<tr>
<td>3.</td>
<td>connection-name name</td>
<td>Optional. By default, no IPsec connection name is configured.</td>
</tr>
<tr>
<td>4.</td>
<td>security acl acl-number</td>
<td>By default, an IPsec policy references no ACL.</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remark</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>--------</td>
</tr>
<tr>
<td>5.</td>
<td>transform-set transform-set-name&amp;&lt;1-6&gt;</td>
<td>By default, an IPsec policy references no IPsec transform set. With SAs to be established through IKE negotiation, an IPsec policy can reference up to six IPsec transform sets. During negotiation, IKE searches for a fully matched IPsec transform set 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.</td>
</tr>
<tr>
<td>6.</td>
<td>ike-peer peer-name</td>
<td>Required for IKEv1 negotiation.</td>
</tr>
<tr>
<td>7.</td>
<td>pfs { dh-group2</td>
<td>dh-group5</td>
</tr>
<tr>
<td>8.</td>
<td>sa duration { time-based seconds</td>
<td>traffic-based kilobytes }</td>
</tr>
<tr>
<td>9.</td>
<td>policy enable</td>
<td>Optional. Enabled by default.</td>
</tr>
<tr>
<td>10.</td>
<td>quit</td>
<td>N/A</td>
</tr>
<tr>
<td>11.</td>
<td>ipsec sa global-duration { time-based seconds</td>
<td>traffic-based kilobytes }</td>
</tr>
</tbody>
</table>
NOTE:
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.

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.

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. A manual IPsec policy can be applied to only one interface. HP recommends that you apply an IPsec policy that uses IKE to only one interface.

To apply an IPsec policy group to an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Apply an IPsec policy group to the interface.</td>
<td>ipsec policy policy-name</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the IPsec session idle timeout.</td>
<td>ipsec session idle-time seconds Optional. 300 seconds by default.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ipsec decrypt check</td>
<td>Optional. Enabled by default.</td>
</tr>
</tbody>
</table>

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.

**IMPORTANT:**
- 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.

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.

To configure IPsec anti-replay checking:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ipsec anti-replay check</td>
<td>Optional. Enabled by default.</td>
</tr>
<tr>
<td>3.</td>
<td>ipsec anti-replay window width</td>
<td>Optional. 32 by default.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ipsec policy policy-name seq-number [ isakmp</td>
<td>manual ]</td>
</tr>
<tr>
<td>3.</td>
<td>qos pre-classify</td>
<td>Disabled by default.</td>
</tr>
</tbody>
</table>

Enabling invalid SPI recovery

This feature is supported only in FIPS mode.

When the security gateway at one end of an IPsec tunnel loses its SAs due to rebooting or any other reason, its peer security gateway may not know the problem and send IPsec packets to it. These packets will be discarded by the receiver because the receiver cannot find appropriate SAs for them, resulting in a traffic blackhole. This situation changes only after the concerned SAs on the sender get aged out and new SAs are established between the two peers. To prevent such service interruption, configure the invalid SPI recovery feature.

The invalid SPI recovery feature allows the receiver to send an INVALID SPI NOTIFY message to tell the sender the invalid SPIs. Upon receiving the message, the sender immediately deletes the corresponding SAs. The subsequent traffic triggers the two peers to set up new SAs for data transmission.

Because attackers may exploit INVALID SPI NOTIFY messages to attack the IPsec packet sender (DoS attack), the invalid SPI recovery feature is disabled by default, making the receiver discard packets with invalid SPIs.

To enable invalid SPI recovery:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ipsec invalid-spi-recovery enable</td>
<td>Optional. Disabled by default</td>
</tr>
</tbody>
</table>

Configuring IPsec RRI

IPsec RRI is supported only in FIPS mode.

IPsec RRI works in static mode or dynamic mode.
Static IPsec RRI

Static IPsec RRI creates static routes based on the destination address information in the ACL that
the IPsec policy references. The next hop address of the route is a user specified remote peer
address, or the IP address of the remote tunnel endpoint.

Static IPsec RRI creates static routes immediately after you enable IPsec RRI in an IPsec policy and
apply the IPsec policy. When you disable RRI, or remove the ACL or the peer gateway IP address
from the policy, IPsec RRI deletes all static routes it has created.

The static mode applies to scenarios where the topologies of branch networks seldom change.

Dynamic IPsec RRI

Dynamic IPsec RRI dynamically creates static routes based on IPsec SAs. In each static route, the
destination address is the address of a protected branch network, and the next hop is the
user-specified remote peer address or the remote tunnel endpoint's address learned during IPsec
SA negotiation.

Dynamic IPsec RRI creates static routes when the IPsec SAs are established, and deletes the static
routes when the IPsec SAs are deleted.

The dynamic mode applies to scenarios where the topologies of branch networks change frequently.
For example, when branches have dial-in users, you can configure dynamic IPsec RRI to avoid
frequent configuration changes that are otherwise required on the headquarters gateway.

A good practice is to configure IPsec RRI on a headquarters gateway to create static routes for the
IPsec tunnels to branches. For the static routes, you can perform the following operations:
• Change their route preference for equal-cost multipath (ECMP) routing or route backup. If
  multiple routes to the same destination have the same preference, traffic is balanced among
  them. If multiple routes to the same destination have different preference values, the route with
  the highest preference forwards traffic and all other routes are backup routes.
• Change their tag value so the gateway can control the use of the static routes based on routing
  policies.

To configure IPsec RRI:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ipsec policy policy-name seq-number [ isakmp</td>
<td>manual ]</td>
</tr>
<tr>
<td>3.</td>
<td>reverse-route [ remote-peer ip-address [ gateway</td>
<td>static ]</td>
</tr>
<tr>
<td>4.</td>
<td>reverse-route preference preference-value</td>
<td>Optional. 60 by default.</td>
</tr>
<tr>
<td>5.</td>
<td>reverse-route tag tag-value</td>
<td>Optional. 0 by default.</td>
</tr>
</tbody>
</table>
NOTE:
- IPsec RRI can work in both tunnel mode and transport mode.
- When you change the route attributes, static IPsec RRI deletes all static routes it has created and creates new static routes. In contrast, dynamic IPsec RRI applies the new attributes only to subsequent static routes. It does not delete or modify static routes it has created.

Displaying and maintaining IPsec

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display IPsec policy information.</td>
<td>`display ipsec policy [ brief</td>
<td>name policy-name [ seq-number ]] [ [ begin</td>
</tr>
<tr>
<td>Display IPsec transform set information.</td>
<td>`display ipsec transform-set [ transform-set-name ] [ [ begin</td>
<td>exclude</td>
</tr>
<tr>
<td>Display IPsec SA information.</td>
<td>`display ipsec sa [ brief</td>
<td>policy policy-name [ seq-number ]</td>
</tr>
<tr>
<td>Display IPsec session information.</td>
<td>`display ipsec session [ tunnel-id integer ] [ [ begin</td>
<td>exclude</td>
</tr>
<tr>
<td>Display IPsec packet statistics.</td>
<td>`display ipsec statistics [ tunnel-id integer ] [ [ begin</td>
<td>exclude</td>
</tr>
<tr>
<td>Display IPsec tunnel information.</td>
<td>`display ipsec tunnel [ [ begin</td>
<td>exclude</td>
</tr>
<tr>
<td>Clear SAs.</td>
<td>`reset ipsec sa [ parameters dest-address protocol spi</td>
<td>policy policy-name [ seq-number ]</td>
</tr>
<tr>
<td>Clear IPsec sessions.</td>
<td><code>reset ipsec session [ tunnel-id integer ]</code></td>
<td>Available in user view.</td>
</tr>
<tr>
<td>Clear IPsec statistics.</td>
<td><code>reset ipsec statistics</code></td>
<td>Available in user view.</td>
</tr>
</tbody>
</table>

IPsec configuration examples

IKE-based IPsec tunnel for IPv4 packets configuration example

Network requirements

As shown in Figure 4, 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 4 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 transform set named tran1.
   [SwitchA] ipsec transform-set tran1

   # Specify the encapsulation mode as tunnel.
   [SwitchA-ipsec-transform-set-tran1] encapsulation-mode tunnel

   # Specify the security protocol as ESP.
   [SwitchA-ipsec-transform-set-tran1] transform esp

   # Specify the algorithms for the IPsec transform set.
   [SwitchA-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
   [SwitchA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
   [SwitchA-ipsec-transform-set-tran1] quit

   # Configure the IKE peer.
   [SwitchA] ike peer peer
   [SwitchA-ike-peer-peer] pre-shared-key Ab12<><> 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 transform set.
   [SwitchA-ipsec-policy-isakmp-map1-10] transform-set 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 transform set named tran1.
[SwitchB] ipsec transform-set tran1
# Specify the encapsulation mode as tunnel.
[SwitchB-ipsec-transform-set-tran1] encapsulation-mode tunnel
# Specify the security protocol as ESP.
[SwitchB-ipsec-transform-set-tran1] transform esp
# Specify the algorithms for the IPsec transform set.
[SwitchB-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
[SwitchB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[SwitchB-ipsec-transform-set-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 transform set.
[SwitchB-ipsec-policy-isakmp-use1-10] transform-set 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. Verify the configuration:
After the previous configuration, send traffic from Switch B to Switch A. Switch A starts IKE negotiation with Switch B when receiving the first packet. If IKE negotiation is successful and SAs are set up, the traffic between the two switches will be IPsec protected.

Command reference

Modified command: ah authentication-algorithm

Old syntax

```
ah authentication-algorithm { md5 | sha1 }
undo ah authentication-algorithm
```

New syntax

In non-FIPS mode:

```
ah authentication-algorithm { md5 | sha1 }
```
undo ah authentication-algorithm

In FIPS mode:

ah authentication-algorithm sha1
undo ah authentication-algorithm

Views

IPsec transform set view

Default command level

2: System level

Parameters

md5: Uses MD5. 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 CenterToA.
<Sysname> system-view
<Sysname> ipsec policy policy1 1 isakmp
<Sysname-ipsec-policy-isakmp-policy1-1> connection-name CenterToA
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 of 1 to 65535.
    remote ip-address: Displays detailed information about the IPsec SA with a specified remote address. This option is available only for 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 of 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 available only for FIPS mode.
If you do not specify any parameters, the command displays information about all IPsec sessions.
IPsec can find matched tunnels directly by session, reducing the intermediate matching procedures and improving the forwarding efficiency. A session is identified by the quintuplet of protocol, source IP address, source port, destination IP address, and destination port.

Examples
# Display information about all IPsec sessions.
<Sysname> display ipsec session
------------------------------------------------------------
total sessions : 2
------------------------------------------------------------
tunnel-id : 3
session idle time/total duration (sec) : 36/300

session flow :  (8 times matched)
    Sour Addr : 15.15.15.1    Sour Port:  0  Protocol : 1
    Dest Addr : 15.15.15.2    Dest Port:  0  Protocol : 1

------------------------------------------------------------
tunnel-id : 4
session idle duration/total duration (sec) : 7/300

session flow :  (3 times matched)
    Sour Addr : 12.12.12.1    Sour Port:  0  Protocol : 1
    Dest Addr : 13.13.13.1    Dest Port:  0  Protocol : 1

# Display information about the session with an IPsec tunnel ID of 5.
<Sysname> display ipsec session tunnel-id 5
------------------------------------------------------------
total sessions : 1
------------------------------------------------------------
tunnel-id : 5
session idle time/total duration (sec) : 30/300

session flow :  (4 times matched)
    Sour Addr : 12.12.12.2    Sour Port:  0  Protocol : 1
    Dest Addr : 13.13.13.2    Dest Port:  0  Protocol : 1

Table 1 Command output
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>total sessions</td>
<td>Total number of IPsec sessions</td>
</tr>
<tr>
<td>tunnel-id</td>
<td>IPsec tunnel ID, same as the connection-id of the IPsec SA</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>session idle time</td>
<td>Idle duration of the IPsec session in seconds</td>
</tr>
<tr>
<td>total duration</td>
<td>Lifetime of the IPsec session in seconds, defaulted to 300 seconds</td>
</tr>
<tr>
<td>session flow</td>
<td>Flow information of the IPsec session</td>
</tr>
<tr>
<td>times matched</td>
<td>Total number of packets matching the IPsec session</td>
</tr>
<tr>
<td>Sour Addr</td>
<td>Source IP address of the IPsec session</td>
</tr>
<tr>
<td>Dest Addr</td>
<td>Destination IP address of the IPsec session</td>
</tr>
<tr>
<td>Sour Port</td>
<td>Source port number of the IPsec session</td>
</tr>
<tr>
<td>Dest Port</td>
<td>Destination port number of the IPsec session</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol number of the IPsec protected data flow, for example, 1 for ICMP</td>
</tr>
</tbody>
</table>

**Related commands**

reset ipsec session

**Modified command: esp authentication-algorithm**

**Old syntax**

```plaintext
esp authentication-algorithm { md5 | sha1 }
undo esp authentication-algorithm
```

**New syntax**

In non-FIPS mode:

```plaintext
esp authentication-algorithm { md5 | sha1 }
undo esp authentication-algorithm
```

In FIPS mode:

```plaintext
esp authentication-algorithm sha1
undo esp authentication-algorithm
```

**Views**

IPsec transform set view

**Default command level**

2: System level

**Parameters**

- **md5**: Uses the MD5 algorithm, which uses a 128-bit key. This keyword is not available for FIPS mode.
- **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-cbc-128 | aes-cbc-192 | aes-cbc-256 | des }
undo esp encryption-algorithm

New syntax

In non-FIPS mode:

esp encryption-algorithm { 3des | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | des }
undo esp encryption-algorithm

In FIPS mode:

esp encryption-algorithm { aes-cbc-128 | aes-cbc-192 | aes-cbc-256 }
undo esp encryption-algorithm

Views

IPsec transform set view

Default command level

2: System level

Parameters

3des: Uses the triple Data Encryption Standard (3DES) in CBC mode, which uses a 168-bit key. This keyword is not available for FIPS mode.
aes-cbc-128: Uses the Advanced Encryption Standard (AES) in CBC mode that uses a 128-bit key.
aes-cbc-192: Uses AES in CBC mode that uses a 192-bit key.
aes-cbc-256: Uses AES in CBC mode that uses a 256-bit key.
des: Uses the DES in cipher block chaining (CBC) mode, which uses a 56-bit key. 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.

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 invalid-spi-recovery enable

Use ipsec invalid-spi-recovery enable to enable invalid security parameter index (SPI) recovery.
Use undo ipsec invalid-spi-recovery enable to restore the default.

Syntax

ipsec invalid-spi-recovery enable
undo ipsec invalid-spi-recovery enable

Default

The invalid SPI recovery is disabled. The receiver discards IPsec packets with invalid SPIs.
Views
System view

Default command level
2: System level

Usage guidelines
This command is supported only in FIPS mode.
Invalid SPI recovery enables an IPsec security gateway to send an INVALID SPI NOTIFY message to its peer when it receives an IPsec packet but cannot find any SA with the specified SPI. When the peer receives the message, it deletes the SAs on its side. Then, subsequent traffic triggers the two peers to establish new SAs.

Examples
# Enable invalid SPI recovery.
<Sysname> system-view
[Sysname] ipsec invalid-spi-recovery enable

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.
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.
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 vian-interface 1
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 ]

Default
  No IPsec policy exists.

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. No hyphen (-) 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 available only for 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.

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 3600 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 of 180 to 604800.
- **kilobytes**: Traffic-based global SA lifetime in kilobytes, in the range of 2560 to 4294967295.

Usage guidelines

- This keyword is available only for 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 on manually configured SAs.

Related commands

- `sa duration`
- `display ipsec sa duration`

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
```

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 3600.

Usage guidelines

- This command is available only for FIPS mode.

Examples

# Set the IPsec session idle timeout to 600 seconds.
Modified command: ipsec transform-set

Syntax

```
ipsec transform-set transform-set-name
undo ipsec transform-set transform-set-name
```

Views

System view

Default command level

2: System level

Parameters

`transform-set-name`: Name of an IPsec transform set, 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: 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


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.

Related commands

ipsec policy (system view)

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-group14

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)

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

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 address, security protocol, and SPI. This keyword is available only for 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 of 256 to 4294967295.

policy: Specifies IPsec SAs that use an IPsec policy.

policy-name: Name of the IPsec policy, a case-sensitive string of 1 to 15 alphanumeric characters.

seq-number: Sequence number of the IPsec policy, in the range of 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 available only for FIPS mode.

ip-address: Remote address.
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 of 1 to 2000000000.

Usage guidelines
This keyword is available only for 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: reverse-route
Use reverse-route to enable and configure the IPsec Reverse Route Inject (RRI) feature.
Use undo reverse-route to disable IPsec RRI.

Syntax
reverse-route [ remote-peer ip-address [ gateway | static ] | static ]
undo reverse-route

Default
IPsec RRI is disabled.

Views
IPsec policy view

Default command level
2: System level
Parameters

**static**: Enables static IPsec RRI. Static IPsec RRI creates static routes based on the ACL that the IPsec policy references. This keyword is available only in IPsec policy view. If this keyword is not specified, you enable dynamic IPsec RRI, which creates static routes based on IPsec SAs.

**remote-peer ip-address**: Specifies a next hop for the static routes. To use the static routes for route backup and load balancing, specify this option.

**gateway**: Creates two recursive routes: one to the remote tunnel endpoint and the other to the protected remote private network. Use the gateway keyword in an IKE-enabled IPsec policy to define an explicit default forwarding path for IPsec traffic.

Usage guidelines

This command is supported only in FIPS mode.

IPsec RRI works in static mode or dynamic mode:

- Static IPsec RRI creates one static route for each destination address permitted by the ACL that the IPsec policy references. Static IPsec RRI creates static routes immediately after you configure IPsec RRI for an IPsec policy and apply the IPsec policy. When you disable RRI, or remove the ACL or the peer gateway IP address from the policy, IPsec RRI deletes all static routes it has created. The static mode applies to scenarios where the topologies of branch networks seldom change.

- Dynamic IPsec RRI dynamically creates static routes based on IPsec SAs. Dynamic IPsec RRI creates static routes when the IPsec SAs are established, and deletes the static routes when the IPsec SAs are deleted. The dynamic mode applies to scenarios where the topologies of branch networks change frequently.

The destination and next hop address in a static route created by IPsec RRI depend on your settings. See Table 2.

Table 2 Possible IPsec RRI configurations and the generated routing information

<table>
<thead>
<tr>
<th>Command</th>
<th>IPsec RRI mode</th>
<th>Route destination</th>
<th>Next hop address</th>
</tr>
</thead>
<tbody>
<tr>
<td>reverse-route static</td>
<td>Static</td>
<td>Destination IP address specified in a permit rule of the ACL that is referenced by the IPsec policy</td>
<td>• Manual IPsec policy: Peer tunnel address set with the tunnel remote command&lt;br&gt;• IPsec policy that uses IKE: The remote tunnel endpoint, which is the address configured in the remote-address command in IKE view.</td>
</tr>
<tr>
<td>reverse-route remote-peer ip-address static</td>
<td>Static</td>
<td>Address identified by the ip-address argument</td>
<td></td>
</tr>
<tr>
<td>reverse-route</td>
<td>Dynamic</td>
<td>Protected peer private network</td>
<td>Remote tunnel endpoint</td>
</tr>
<tr>
<td>reverse-route remote-peer ip-address</td>
<td>Dynamic</td>
<td>Protected peer private network</td>
<td>Address identified by the ip-address argument, typically, the next hop address of the interface where the IPsec policy is applied</td>
</tr>
<tr>
<td>reverse-route remote-peer ip-address gateway</td>
<td>Dynamic</td>
<td>Remote tunnel endpoint</td>
<td>The address specified by the ip-address argument (outgoing interface: the interface where the IPsec policy is applied)</td>
</tr>
</tbody>
</table>
Enabling, disabling, or changing RRI settings in an IPsec policy deletes all IPsec SAs created or negotiated by the policy.

To view static routes created by RRI, use the `display ip routing-table` command. For information about the routing table, see *Layer 3—IP Routing Configuration Guide*.

If you configure an address range in IKE peer view, static IPsec RRI does not take effect.

**Examples**

# Configure static IPsec RRI to create static routes based on ACL 3000. Take the peer private network 3.0.0.0/24 as the destination and the remote gateway 1.1.1.2 as the next hop.

```bash
<Sysname> system-view
[Sysname] ike peer 1
[Sysname-ike-peer-1] remote-address 1.1.1.2
[Sysname-ike-peer-1] quit
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule 0 permit ip source 2.0.0.0 0.0.0.255 destination 3.0.0.0 0.0.0.255
[Sysname-acl-adv-3000] quit
[Sysname] ipsec policy 1 1 isakmp
[Sysname-ipsec-policy-isakmp-1-1] security acl 3000
[Sysname-ipsec-policy-isakmp-1-1] transform-set tran1
[Sysname-ipsec-policy-isakmp-1-1] ike-peer 1
[Sysname-ipsec-policy-isakmp-1-1] reverse-route static
[Sysname-ipsec-policy-isakmp-1-1] quit
[Sysname] interface vlan-interface1
[Sysname-Vlan-interface1] ipsec policy 1
[Sysname-Vlan-interface1] quit
```

# Display the routing table. You can see that IPsec RRI has created the static route. (Other routes are not shown.)

```bash
[Sysname] display ip routing-table
... Destination/Mask    Proto  Pre  Cost         NextHop         Interface
3.0.0.0/24          Static 60   0            1.1.1.2         Vlan-interface1
```

# Configure static IPsec RRI to create static routes based on ACL 3000. Take the peer private network as the destination and 1.1.1.3 as the next hop.

```bash
[Sysname] ipsec policy 1 1 isakmp
[Sysname-ipsec-policy-isakmp-1-1] reverse-route remote-peer 1.1.1.3 static
[Sysname-ipsec-policy-isakmp-1-1] quit
```

# Display the routing table. You can see that IPsec RRI has created the static route. (Other routes are not shown.)

```bash
[Sysname] display ip routing-table
... Destination/Mask    Proto  Pre  Cost         NextHop         Interface
3.0.0.0/24          Static 60   0            1.1.1.3         Vlan-interface1
```

# Configure dynamic IPsec RRI to create static routes based on IPsec SAs. Take the peer private network as the destination and the remote tunnel endpoint 1.1.1.2 as the next hop.

```bash
[Sysname] ipsec policy 1 1 isakmp
[Sysname-ipsec-policy-isakmp-1-1] reverse-route
[Sysname-ipsec-policy-isakmp-1-1] quit
```
# Display the routing table. The expected route appears in the table after the IPsec SA negotiation succeeds. (Other routes are not shown.)
[Sysname] display ip routing-table
...
Destination/Mask    Proto  Pre  Cost         NextHop         Interface
3.0.0.0/24          Static 60   0            1.1.1.2         Vlan-interface1

# Configure dynamic IPsec RRI to create static routes based on IPsec SAs. Take 1.1.1.3 as the next hop.
[Sysname] ipsec policy 1 1 isakmp
[Sysname-ipsec-policy-isakmp-1-1] reverse-route remote-peer 1.1.1.3
[Sysname-ipsec-policy-isakmp-1-1] quit

# Display the routing table. The expected route appears in the routing table after the IPsec SA negotiation succeeds. (Other routes are not shown.)
[Sysname] display ip routing-table
...
Destination/Mask    Proto  Pre  Cost         NextHop         Interface
3.0.0.0/24          Static 60   0            1.1.1.3         Vlan-interface1

# Configure dynamic IPsec RRI to create two static routes based on an IPsec SA: one to the peer private network 3.0.0.0/24 via the remote tunnel endpoint 1.1.1.2, and the other to the remote tunnel endpoint via 1.1.1.3.
[Sysname]ipsec policy 1 1 isakmp
[Sysname-ipsec-policy-isakmp-1-1] reverse-route remote-peer 1.1.1.3 gateway

# Display the routing table. The expected routes appear in the routing table after the IPsec SA negotiation succeeds. (Other routes are not shown.)
[Sysname] display ip routing-table
...
Destination/Mask    Proto  Pre  Cost         NextHop         Interface
1.1.1.2/32          Static 60   0            1.1.1.3         Vlan-interface1
3.0.0.0/24          Static 60   0            1.1.1.2         Vlan-interface1

Related commands
- reverse-route preference
- reverse-route tag

New command: reverse-route preference

Use reverse-route preference to change the preference of the static routes created by IPsec RRI.
Use undo reverse-route preference to restore the default.

Syntax
reverse-route preference preference-value
undo reverse-route preference

Default
The preference for the static routes created by IPsec RRI is 60.

Views
IPsec policy view
Default command level

2: System level

Parameters

preference-value: Sets a preference value for the static routes created by IPsec RRI. The value range is 1 to 255. A smaller value represents a higher preference.

Usage guidelines

This command is supported only in FIPS mode.

When you change the route preference, static IPsec RRI deletes all static routes it has created and creates new static routes. In contrast, dynamic IPsec RRI applies the new preference only to subsequent static routes. It does not delete or modify static routes it has created.

Examples

# Set the preference to 100 for static routes populated by IPsec RRI.
<Sysname>system-view
[Sysname] ipsec policy 1 1 isakmp
[Sysname-ipsec-policy-isakmp-1-1] reverse-route preference 100

Related commands

reverse-route

New command: reverse-route tag

Use reverse-route tag to set a route tag for the static routes created by IPsec RRI. This tag helps in implementing flexible route control through routing policies.

Use undo reverse-route tag to restore the default.

Syntax

reverse-route tag tag-value
undo reverse-route tag

Default

The tag value is 0 for the static routes created by IPsec RRI.

Views

IPsec policy view

Default command level

2: System level

Parameters

tag-value: Sets a route tag for the static routes. The value range is 1 to 4294967295.

Usage guidelines

This command is supported only in FIPS mode.

When you change the route tag, static IPsec RRI deletes all static routes it has created and creates new static routes. In contrast, dynamic IPsec RRI applies the new route tag only to subsequent static routes. It does not delete or modify static routes it has created.

For information about routing policies, see Layer 3—IP Routing Configuration Guide.

Examples

# Set the tag value to 50 for the static routes created by IPsec RRI.
Related commands
reverse-route

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 of 180 to 604800.
kilobytes: Traffic-based SA lifetime in kilobytes, in the range of 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 transform set 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.

Related commands

• 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

\[
\begin{align*}
\text{sa string-key} & \{ \text{inbound} \mid \text{outbound} \} \{ \text{ah} \mid \text{esp} \} \{ \text{cipher} \mid \text{simple} \} \text{string-key} \\
\text{undo sa string-key} & \{ \text{inbound} \mid \text{outbound} \} \{ \text{ah} \mid \text{esp} \}
\end{align*}
\]

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 the authentication algorithm and encryption algorithm, respectively.

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

\[
\begin{align*}
\text{security acl} & \text{ acl-number} \\
\text{undo security acl}
\end{align*}
\]

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 of 3000 to 3999.

Usage guidelines

This command is available only for 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.

An IPsec policy references only one ACL. If you specify more than one ACL for an IPsec policy, the IPsec policy references the one last specified.

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 transform set 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.

Modified command: transform-set

Old syntax

```
transform-set
undo transform-set
```
New syntax

- transform-set transform-set-name<&1-6>
- undo transform-set

Views

IPsec policy view

Default command level

2: System level

Parameters

transform-set-name<&1-6>: Specifies up to six space-separated transform sets by names. A transform set name is a string of 1 to 32 characters.

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: 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
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

The IKE configuration is available only for switches in FIPS mode.
Unless otherwise specified, IKE in this chapter refers to IKEv1.

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.
As shown in Figure 5, 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 6 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

- 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 "Configuring PKI."

Complete the following tasks to configure IKE:

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring a name for the local security gateway</td>
<td>Optional.</td>
</tr>
<tr>
<td>Configuring an IKE proposal</td>
<td>Optional. Required if you want to specify an IKE proposal for an IKE peer to reference.</td>
</tr>
<tr>
<td>Configuring an IKE peer</td>
<td>Required.</td>
</tr>
<tr>
<td>Setting keepalive timers</td>
<td>Optional.</td>
</tr>
</tbody>
</table>
# 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 by in IKE peer view is used.

To configure a name for the local security gateway:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure a name for</td>
<td>ike local-name name</td>
</tr>
<tr>
<td></td>
<td>the local security</td>
<td>Optional.</td>
</tr>
<tr>
<td></td>
<td>gateway.</td>
<td>By default, the device name is used as</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the name of the local security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>gateway.</td>
</tr>
</tbody>
</table>

# 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create an IKE proposal and enter its view.</td>
<td>ike proposal proposal-number</td>
</tr>
<tr>
<td>3.</td>
<td>Specify an encryption algorithm for the</td>
<td>encryption-algorithm aes-cbc</td>
</tr>
<tr>
<td></td>
<td>IKE proposal.</td>
<td>[ key-length ]</td>
</tr>
<tr>
<td>4.</td>
<td>Specify an authentication method for the</td>
<td>authentication-method</td>
</tr>
<tr>
<td></td>
<td>IKE proposal.</td>
<td>{ pre-share</td>
</tr>
<tr>
<td></td>
<td>Optional.</td>
<td>Optional.</td>
</tr>
<tr>
<td></td>
<td>128-bit AES-CBC by default.</td>
<td>Pre-shared key by default.</td>
</tr>
</tbody>
</table>

181
5. Specify an authentication algorithm for the IKE proposal.

   Command: `authentication-algorithm sha`
   Remarks: Optional. SHA1 by default.

6. Specify a DH group for key negotiation in phase 1.

   Command: `dh { group2 | group5 | group14 }`
   Remarks: Optional. `group2` (the 1024-bit DH group) by default.

7. Set the ISAKMP SA lifetime for the IKE proposal.

   Command: `sa duration seconds`
   Remarks: 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, a loopback interface address, for example, 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td><code>ike peer peer-name</code></td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td><code>exchange-mode main</code></td>
<td>Optional. main by default.</td>
</tr>
<tr>
<td>4.</td>
<td><code>proposal proposal-number&amp;&lt;1-6&gt;</code></td>
<td>Optional. By default, an IKE peer references</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>5.</td>
<td>Configure the pre-shared key for pre-shared key authentication</td>
<td>no IKE proposals, and, when initiating IKE negotiation, it uses the IKE proposals configured in system view.</td>
</tr>
<tr>
<td></td>
<td>pre-shared-key [ cipher</td>
<td>simple ] key</td>
</tr>
<tr>
<td>6.</td>
<td>Configure the PKI domain for digital signature authentication.</td>
<td>certificate domain domain-name</td>
</tr>
<tr>
<td>7.</td>
<td>Specify the ID type as IP address for IKE negotiation phase 1.</td>
<td>id-type { ip</td>
</tr>
<tr>
<td></td>
<td>• Specify a name for the local security gateway: local-name name</td>
<td>Optional.</td>
</tr>
<tr>
<td></td>
<td>• Configure the name of the remote security gateway: remote-name name.</td>
<td>Optional. By default, no name is configured for the local security gateway in IKE peer view, and the security gateway name configured by using the ike local-name command is used. The remote gateway name configured with remote-name command on the local gateway must be identical to the local name configured with the local-name command on the peer.</td>
</tr>
<tr>
<td>8.</td>
<td>Configure the names of the two ends.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Specify an IP address for the local gateway: local-address ip-address</td>
<td>Optional. By default, it is the primary IP address of the interface referencing the security policy.</td>
</tr>
<tr>
<td></td>
<td>• Configure the IP addresses of the remote gateway: remote-address { hostname [ dynamic ]</td>
<td>low-ip-address [ high-ip-address ] }</td>
</tr>
<tr>
<td>9.</td>
<td>Configure the IP addresses of the two ends.</td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td>Enable the NAT traversal function for IPsec/IKE.</td>
<td>nat traversal</td>
</tr>
<tr>
<td></td>
<td>Optional. Required when a NAT gateway is present in the VPN tunnel constructed by IPsec/IKE Disabled by default.</td>
<td></td>
</tr>
<tr>
<td>11.</td>
<td>Apply a DPD detector to the IKE peer.</td>
<td>dpd dpd-name</td>
</tr>
<tr>
<td></td>
<td>Optional. No DPD detector is applied to an IKE peer by default. For more information about DPD configuration, see “Configuring a DPD detector.”</td>
<td></td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the ISAKMP SA keepalive interval.</td>
<td>ike sa keepalive-timer interval seconds</td>
</tr>
<tr>
<td>3.</td>
<td>Set the ISAKMP SA keepalive timeout.</td>
<td>ike sa keepalive-timer timeout seconds</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the NAT keepalive interval.</td>
<td>ike sa nat-keepalive-timer interval seconds</td>
</tr>
</tbody>
</table>

Configuring a DPD detector

Dead peer detection (DPD) irregularly detects dead IKE peers. It works as follows:

1. When the local end sends an IPsec packet, it checks the time the last IPsec packet was received from the peer.
2. If the time interval exceeds the DPD interval, it sends a DPD hello to the peer.
3. If the local end receives no DPD acknowledgement within the DPD packet retransmission interval, it retransmits the DPD hello.
4. If the local end still receives no DPD acknowledgement after having made the maximum number of retransmission attempts (two by default), it considers the peer already dead, and clears the IKE SA and the IPsec SAs based on the IKE SA.

DPD enables an IKE entity to check the liveliness of its peer only when necessary. It generates less traffic than the keepalive mechanism, which exchanges messages periodically.

To configure a DPD detector:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a DPD detector and enter its view.</td>
<td>ike dpd dpd-name</td>
</tr>
<tr>
<td>3.</td>
<td>Set the DPD interval.</td>
<td>interval-time interval-time</td>
</tr>
<tr>
<td>4.</td>
<td>Set the DPD packet retransmission interval.</td>
<td>time-out time-out</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Disable Next payload field checking.</td>
<td>ike next-payload check disabled</td>
</tr>
</tbody>
</table>

Displaying and maintaining IKE

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display IKE DPD information.</td>
<td>display ike dpd { dpd-name } [ [ begin</td>
<td>exclude</td>
</tr>
<tr>
<td>Display IKE peer information.</td>
<td>display ike peer { peer-name } [ [ begin</td>
<td>exclude</td>
</tr>
<tr>
<td>Display IKE SA information.</td>
<td>display ike sa [ verbose [ connection-id connection-id</td>
<td>remote-address remote-address ] ]</td>
</tr>
<tr>
<td>Display IKE proposal information.</td>
<td>display ike proposal [ [ begin</td>
<td>exclude</td>
</tr>
</tbody>
</table>
IKE configuration examples

Main mode IKE with pre-shared key authentication configuration example

Network requirements

As shown in Figure 7, 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. Leave Switch B with only the default IKE proposal. Configure the two switches to use the pre-shared key authentication method.

Figure 7 Network diagram

Configuration procedure

Make sure Switch A and Switch B can reach each other.

1. Configure Switch A:
   # Assign an IP address to VLAN-interface 1.
   [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 transform set tran1.
   [SwitchA] ipsec transform-set tran1
   # Set the packet encapsulation mode to tunnel.
   [SwitchA-ipsec-transform-set-tran1] encapsulation-mode tunnel
   # Use security protocol ESP.
   [SwitchA-ipsec-transform-set-tran1] transform esp
   # Specify encryption and authentication algorithms.
   [SwitchA-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
   [SwitchA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
   [SwitchA-ipsec-transform-set-tran1] quit
   # Create an IKE proposal numbered 10.
   [SwitchA] ike proposal 10
   # Set the authentication algorithm to SHA1.
# Set the authentication method to **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
```

# 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
```

# Create an IPsec policy that uses IKE negotiation.

```
[SwitchA] ipsec policy map1 10 isakmp
```

# Reference IPsec transform set **tran1**.

```
[SwitchA-ipsec-policy-isakmp-map1-10] transform-set 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
```

# Apply the IPsec policy group to VLAN-interface 1.

```
[SwitchB] interface vlan-interface 1
```

```
[SwitchB-Vlan-interface1] ipsec policy use1
```

2. **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
```

# Configure ACL 3101 to identify traffic from Switch B to Switch A.

```
<SwitchB> system-view
```

```
[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 transform set **tran1**.

```
[SwitchB] ipsec transform-set tran1
```

# Set the packet encapsulation mode to tunnel.

```
[SwitchB-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

# Use security protocol ESP.

```
[SwitchB-ipsec-transform-set-tran1] transform esp
```

# Specify encryption and authentication algorithms.

```
[SwitchB-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
```

```
[SwitchB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
```

187
# Create IKE peer `peer`.

```bash
[SwitchB] ike peer peer
```

# Set the pre-shared key.

```bash
[SwitchB-ike-peer-peer] pre-shared-key Ab12<<>
```

# Specify the IP address of the peer security gateway.

```bash
[SwitchB-ike-peer-peer] remote-address 1.1.1.1
```

# Create an IPsec policy that uses IKE negotiation.

```bash
[SwitchB] ipsec policy use1 10 isakmp
```

# Reference ACL 3101 to identify the protected traffic.

```bash
[SwitchB-ipsec-policy-isakmp-use1-10] security acl 3101
```

# Reference IPsec transform set `tran1`.

```bash
[SwitchB-ipsec-policy-isakmp-use1-10] transform-set tran1
```

# Reference IKE peer `peer`.

```bash
[SwitchB-ipsec-policy-isakmp-use1-10] ike-peer peer
```

# Apply the IPsec policy group to VLAN-interface 1.

```bash
[SwitchB] interface vlan-interface 1
```

```bash
[SwitchB-Vlan-interface1] ipsec policy use1
```

3. Verify the configuration:

After the above configuration, send traffic from Switch B to Switch A. Switch A starts IKE negotiation with Switch B when receiving the first packet. IKE proposal matching starts with the one having the highest priority. During the matching process, lifetime is not involved but it is determined by the IKE negotiation parties.

## Troubleshooting IKE

When you configure parameters to establish an IPsec tunnel, enable IKE error debugging to locate configuration problems:

```
<Switch> debugging ike error
```

### Invalid user ID

**Symptom**

Invalid user ID.

**Analysis**

In IPsec, user IDs are used to identify data flows and to set up different IPsec tunnels for different data flows. Now, the IP address and username are used as the user ID.

The following is the debugging information:

```
got NOTIFY of type INVALID_ID_INFORMATION
```

Or

```
drop message from A.B.C.D due to notification type INVALID_ID_INFORMATION
```

**Solution**

Check that the ACLs in the IPsec policies configured on the interfaces at both ends are compatible. Configure the ACLs to mirror each other. For more information about ACL mirroring, see "Configuring IPsec."
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 transform sets 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

The commands in this chapter are available only for switches in FIPS mode.

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**


**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**

- `ike proposal`
- `display 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
• ike proposal
• display 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**

- ike proposal
- display 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: dpdl
  references: 1
  interval-time: 10
  time_out: 5
---------------------------

Table 3 Command output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>references</td>
<td>Number of IKE peers that use the DPD detector</td>
</tr>
<tr>
<td>Interval-time</td>
<td>DPD query trigging interval in seconds</td>
</tr>
<tr>
<td>time_out</td>
<td>DPD packet retransmission interval in seconds</td>
</tr>
</tbody>
</table>

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.
display ike peer

IKE Peer: rtb4tunn
exchange mode: main on phase 1
pre-shared-key simple 123
peer id type: ip
peer ip address: 44.44.44.55
local ip address:
peer name:
nat traversal: disable
dpd: dpd1

Table 4 Command output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>exchange mode</td>
<td>IKE negotiation mode in phase 1</td>
</tr>
<tr>
<td>pre-shared-key</td>
<td>Pre-shared key used in phase 1</td>
</tr>
<tr>
<td>peer id type</td>
<td>ID type used in phase 1</td>
</tr>
<tr>
<td>peer ip address</td>
<td>IP address of the remote security gateway</td>
</tr>
<tr>
<td>local ip address</td>
<td>IP address of the local security gateway</td>
</tr>
<tr>
<td>peer name</td>
<td>Name of the remote security gateway</td>
</tr>
<tr>
<td>nat traversal</td>
<td>Whether NAT traversal is enabled</td>
</tr>
<tr>
<td>dpd</td>
<td>Name of the peer DPD detector</td>
</tr>
</tbody>
</table>

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.
eclude: 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

<table>
<thead>
<tr>
<th>priority</th>
<th>authentication method</th>
<th>authentication algorithm</th>
<th>encryption algorithm</th>
<th>Diffie-Hellman group</th>
<th>duration (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>PRE_SHARED</td>
<td>SHA</td>
<td>AES_CBC_128</td>
<td>MODP_1024</td>
<td>86400</td>
</tr>
<tr>
<td>default</td>
<td>PRE_SHARED</td>
<td>SHA</td>
<td>AES_CBC_128</td>
<td>MODP_1024</td>
<td>86400</td>
</tr>
</tbody>
</table>

Table 5 Command output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority</td>
<td>Priority of the IKE proposal</td>
</tr>
<tr>
<td>authentication method</td>
<td>Authentication method used by the IKE proposal</td>
</tr>
<tr>
<td>authentication algorithm</td>
<td>Authentication algorithm used by the IKE proposal</td>
</tr>
<tr>
<td>encryption algorithm</td>
<td>Encryption algorithm used by the IKE proposal</td>
</tr>
<tr>
<td>Diffie-Hellman group</td>
<td>DH group used in IKE negotiation phase 1</td>
</tr>
<tr>
<td>duration (seconds)</td>
<td>ISAKMP SA lifetime of the IKE proposal in seconds</td>
</tr>
</tbody>
</table>

Related commands
- authentication-method
- ike proposal
- encryption-algorithm
- authentication-algorithm
- dh
- 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 of 1 to 2000000000.
remote: Displays detailed information about IKE SAs with a specified remote address.

ip-address: 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 6 Command output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>total phase-1 SAs</td>
<td>Total number of SAs for phase 1.</td>
</tr>
<tr>
<td>connection-id</td>
<td>Identifier of the ISAKMP SA.</td>
</tr>
<tr>
<td>peer</td>
<td>Remote IP address of the SA.</td>
</tr>
<tr>
<td>flag</td>
<td>Status of the SA:</td>
</tr>
<tr>
<td>phase</td>
<td>The phase the SA belongs to:</td>
</tr>
<tr>
<td>doi</td>
<td>Interpretation domain the SA belongs to.</td>
</tr>
</tbody>
</table>

# Display detailed information about the current IKE SAs.
<Sysname> display ike sa verbose
  connection id: 2
vpn-instance: 1
transmitting entity:
initiator status: active
---------------------------------------------
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-128

life duration(sec): 86400
remaining key duration(sec): 86379
exchange-mode: MAIN
diffie-hellman group: GROUP2
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 status: active
---------------------------------------------
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-128

life duration(sec): 86400
remaining key duration(sec): 82480
exchange-mode: MAIN
diffie-hellman group: GROUP2
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
status: active

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 7 Command output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>connection id</td>
<td>Identifier of the ISAKMP SA</td>
</tr>
<tr>
<td>vpn-instance</td>
<td>VPN instance name</td>
</tr>
<tr>
<td>transmitting entity</td>
<td>Entity in the IKE negotiation</td>
</tr>
<tr>
<td>local ip</td>
<td>IP address of the local gateway</td>
</tr>
<tr>
<td>local id type</td>
<td>Identifier type of the local gateway</td>
</tr>
<tr>
<td>local id</td>
<td>Identifier of the local gateway</td>
</tr>
<tr>
<td>remote ip</td>
<td>IP address of the remote gateway</td>
</tr>
<tr>
<td>remote id type</td>
<td>Identifier type of the remote gateway</td>
</tr>
<tr>
<td>remote id</td>
<td>Identifier of the remote security gateway</td>
</tr>
<tr>
<td>authentication-method</td>
<td>Authentication method used by the IKE proposal</td>
</tr>
<tr>
<td>authentication-algorithm</td>
<td>Authentication algorithm used by the IKE proposal</td>
</tr>
<tr>
<td>encryption-algorithm</td>
<td>Encryption algorithm used by the IKE proposal</td>
</tr>
<tr>
<td>life duration(sec)</td>
<td>Lifetime of the ISAKMP SA in seconds</td>
</tr>
<tr>
<td>remaining key duration(sec)</td>
<td>Remaining lifetime of the ISAKMP SA in seconds</td>
</tr>
<tr>
<td>exchange-mode</td>
<td>IKE negotiation mode in phase 1</td>
</tr>
<tr>
<td>diffie-hellman group</td>
<td>DH group used for key negotiation in IKE phase 1</td>
</tr>
<tr>
<td>nat traversal</td>
<td>Whether NAT traversal is enabled</td>
</tr>
</tbody>
</table>
Related commands

- ike proposal
- ike peer

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.

```bash
<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**

An IKE proposal uses the AES 128 encryption algorithm in CBC mode.

**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**

```plaintext
# Use 192-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-cbc 192
```

**Related commands**

- ike proposal
- display ike proposal

**exchange-mode**

Use `exchange-mode` to select an IKE negotiation mode.
Use `undo exchange-mode` to restore the default.

**Syntax**

```plaintext
exchange-mode main
undo exchange-mode
```

**Default**

Main mode is used.

**Views**

IKE peer view

**Default command level**

2: System level

**Examples**

```plaintext
# 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**

```plaintext
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 name of the Fully Qualified Domain Name (FQDN) type as the ID during IKE negotiation.
- **user-fqdn**: Uses a name of the user FQDN type 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.
If the ID type of FQDN is used, configure a name without any at sign (@) for the local security gateway, for example, `foo.bar.com`. If the ID type of user FQDN is used, configure a name with an at sign (@) for the local security gateway, for example, `test@foo.bar.com`.

Examples
# Use the ID type of name during IKE negotiation.
```bash
<Sysname> system-view
<Sysname> ike peer peer1
<Sysname-ike-peer-peer1> id-type name
```

Related commands
- `local-name`
- `ike local-name`
- `remote-name`
- `remote-address`
- `local-address`
- `exchange-mode`

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

- remote-name
- id-type

ike next-payload check disabled

Use ike next-payload check disabled to disable the checking of the Next payload field in the last payload of an IKE message during IKE negotiation, gaining interoperation with products assigning the field a value other than zero.

Use undo ike next-payload check disabled to restore the default.

Syntax

ike next-payload check disabled
undo ike next-payload check disabled

Default

The Next payload field is checked.

Views

System view

Default command level

2: System level

Examples

# Disable Next payload field checking for the last payload of an IKE message.
<Sysname> system-view
[Sysname] ike next-payload check disabled

ike peer (system view)

Use ike peer to create an IKE peer and enter IKE peer view.
Use undo ike peer to delete an IKE peer.

Syntax

ike peer peer-name
undo ike peer peer-name

Views

System view

Default command level

2: System level

Parameters

peer-name: IKE peer name, a string of 1 to 32 characters.
Examples

# Create an IKE peer named peer1 and enter IKE peer view.
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1]

ike proposal

Use ike proposal to create an IKE proposal and enter IKE proposal view. Use undo ike proposal to delete an IKE proposal.

Syntax

ike proposal proposal-number
undo ike proposal proposal-number

Views

System view

Default command level

2: System level

Parameters

proposal-number: IKE proposal number, in the range of 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 of 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 of 20 to 28,800.

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
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 of 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 default 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. Use this command if you want to specify a different address for the local security gateway.

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.

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

Related commands

- remote-name
- id-type

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

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. The key string must contain uppercase and lowercase letters, digits, and special 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 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>: Specifies up to six IKE proposals by sequence numbers. The sequence number of an IKE proposal is in the range of 1 to 65535. An IKE proposal with a smaller sequence number has a higher priority.

Usage guidelines
In the IKE negotiation phase 1, the local end 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: Uses dynamic address resolution for the IPsec remote peer name. If you do not provide this keyword, the local end 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 end 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 end 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 end can use the up-to-date remote IP address to initiate IKE negotiation.
Related commands

- id-type ip
- local-address

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 end to dynamically update the remote IP address.
<Sysname> system-view
[Sysname] ike peer peer2
[Sysname-ike-peer-peer2] remote-address test.com dynamic

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.

Related commands

- id-type
- local-name
- ike local-name

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
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 of 1 to 2000000000.

Usage guidelines

If you do not specify any parameter, 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 the IKE SA that uses connection ID 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 of 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
• ike proposal
• display 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

Views
IKE DPD view

Default command level
2: System level

Parameters
time-out: DPD packet retransmission interval in seconds, in the range of 1 to 60.

Usage guidelines
The default DPD packet retransmission interval is 5 seconds.

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: 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Disable password recovery capacity.</td>
<td>undo password-recovery enable</td>
</tr>
</tbody>
</table>

For more information about BootRom menus and password recovery capacity, see appendix B in HP A5800_5820X-CMW520-R1807P02 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: Verifying the correctness and integrity of the file

Verifying the correctness and integrity of the file

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify the correctness</td>
<td>crypto-digest sha256 file file-url</td>
<td>Available in user view.</td>
</tr>
<tr>
<td>and integrity of the file.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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)=7bcb92458222f91f9a09a807c4c4567ef4d5dc4e4abc06c2a741df7045433eb

New feature: 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enable MAC address migration log notifying.</td>
<td>mac-flapping notification enable</td>
<td>By default, MAC address migration log notifying is disabled.</td>
</tr>
</tbody>
</table>

The MAC address migration logs of the last one minute are displayed once every one minute.

**Command reference**

mac-flapping notification enable

Use `mac-flapping notification enable` to enable MAC address migration log notifying.

Use `undo mac-flapping notification enable` to disable the MAC address migration notifying.

**Syntax**

- `mac-flapping notification enable`
- `undo mac-flapping notification enable`

**Default**

MAC address migration log notifying is disabled.

**Views**

- System view

**Default command level:**

2: System level

**Usage guidelines**

A MAC address migration log contains a MAC address, ID of the VLAN to which the MAC address belongs, source interface from which the MAC address migrates, and the current interface with which the MAC address associates.

After enabling MAC address migration log notifying, the MAC address migration log of the last 1 minute are displayed once every 1 minute.

Up to 10 logs can be saved on each card in 1 minute.
Examples

# Enable MAC address migration log notifying.
<Sysname> system-view
[Sysname] mac-flapping notification enable
[Sysname]
%Sep 21 14:09:22:420 2012 HP MAC/5/MAC_FLAPPING: MAC address 0000-0012-0034 in vlan 500
has flapped from port GigabitEthernet1/0/16 to port GigabitEthernet1/0/1 1 time(s).

The output shows that the MAC address 0000-0012-0034 belongs to VLAN 500, the source interface
from which the MAC address migrates from is GE1/0/16, the current interface with which the MAC
address associates is GE1/0/1, and the MAC address migrates one time in the last one minute.

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>packet capture { acl</td>
<td></td>
</tr>
<tr>
<td></td>
<td>{ acl-number</td>
<td>ipv6 acl6-number }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>buffer-size size</td>
</tr>
<tr>
<td></td>
<td>capture-length</td>
<td>mode { circular</td>
</tr>
<tr>
<td>2.</td>
<td>Enable packet capture.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• (Approach 1) Start packet capture</td>
<td>Use either approach.</td>
</tr>
<tr>
<td></td>
<td>immediately:</td>
<td>You can set packet</td>
</tr>
<tr>
<td></td>
<td>packet capture start [ acl</td>
<td>capture parameters</td>
</tr>
<tr>
<td></td>
<td>{ acl-number</td>
<td>ipv6</td>
</tr>
<tr>
<td></td>
<td>acl6-number }</td>
<td>when you use approach</td>
</tr>
<tr>
<td></td>
<td></td>
<td>buffer-size size</td>
</tr>
<tr>
<td></td>
<td>capture-length</td>
<td>mode { circular</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• (Approach 2) Configure a packet</td>
<td>If you use approach 1, the existing</td>
</tr>
<tr>
<td></td>
<td>capture schedule:</td>
<td>packet capture</td>
</tr>
<tr>
<td></td>
<td>packet capture schedule</td>
<td>schedule is invalid.</td>
</tr>
<tr>
<td></td>
<td>datetime time date</td>
<td></td>
</tr>
<tr>
<td></td>
<td>packet capture stop</td>
<td>Stop packet capture</td>
</tr>
<tr>
<td></td>
<td></td>
<td>before you display,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>save, or clear the</td>
</tr>
</tbody>
</table>
buffered contents. The device automatically stops packet capture when:
  - The packet capture function operates in linear mode, and the packet capture buffer is full.
  - The number of packets captured exceeds the upper limit.
  - The duration of the packet capture process exceeds the upper limit.

4. Save the contents in the packet capture buffer.
   packet capture buffer save [ filename ]
   Optional. Save the file with a filename in .pcap format.

### Displaying and maintaining packet capture

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the current packet capture status.</td>
<td>display packet capture status</td>
<td>Available in any view.</td>
</tr>
<tr>
<td>Display the buffered contents.</td>
<td>display packet capture buffer [ start-index [ end-index ] ] [ length display-length ]</td>
<td>Available in any view.</td>
</tr>
<tr>
<td>Clear the buffered contents.</td>
<td>reset packet capture buffer</td>
<td>Available in user view.</td>
</tr>
</tbody>
</table>

### Packet capture configuration example

**Network requirements**

As shown in Figure 8, 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 8 Network diagram**

![Network diagram](image)

**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

<table>
<thead>
<tr>
<th>Current status</th>
<th>In process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Linear</td>
</tr>
<tr>
<td>Buffer size</td>
<td>2097152 (bytes)</td>
</tr>
<tr>
<td>Buffer used</td>
<td>1880 (bytes)</td>
</tr>
<tr>
<td>Max capture length</td>
<td>68 (bytes)</td>
</tr>
<tr>
<td>ACL information</td>
<td>Basic or advanced IPv4 ACL 2000</td>
</tr>
<tr>
<td>Schedule datetime</td>
<td>Unspecified</td>
</tr>
<tr>
<td>Upper limit of duration</td>
<td>Unspecified (seconds)</td>
</tr>
<tr>
<td>Duration</td>
<td>13 (seconds)</td>
</tr>
<tr>
<td>Upper limit of packets</td>
<td>Unspecified</td>
</tr>
<tr>
<td>Packets count</td>
<td>10</td>
</tr>
</tbody>
</table>

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  -rw-  -  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 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 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.

```bash
<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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Current status</strong></td>
<td>Packet capture status:</td>
</tr>
<tr>
<td></td>
<td>• <strong>In process</strong>—The packet capturing process is ongoing.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Scheduled</strong>—The packet capture schedule is configured, but does not start.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Paused</strong>—Packet capture is stopped temporarily, and you can display, save, and clear the contents in the packet capture buffer.</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Packet capture mode:</td>
</tr>
<tr>
<td></td>
<td>• Linear</td>
</tr>
<tr>
<td></td>
<td>• Circular</td>
</tr>
<tr>
<td><strong>Buffer size</strong></td>
<td>Packet capture buffer size.</td>
</tr>
<tr>
<td><strong>Buffer used</strong></td>
<td>Packet capture buffer size in use.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Max capture length</strong></td>
<td>Maximum length of the packet that can be stored in the packet buffer.</td>
</tr>
<tr>
<td><strong>ACL information</strong></td>
<td>ACL type and number for packet capture.</td>
</tr>
<tr>
<td><strong>Schedule datetime</strong></td>
<td>Start time of the packet capture schedule.</td>
</tr>
<tr>
<td><strong>Upper limit of duration</strong></td>
<td>Upper limit of the packet capture duration.</td>
</tr>
<tr>
<td><strong>Duration</strong></td>
<td>Packet capture duration.</td>
</tr>
<tr>
<td><strong>Upper limit of packets</strong></td>
<td>Maximum number of packets that can be captured.</td>
</tr>
<tr>
<td><strong>Packets count</strong></td>
<td>Number of packets that has been captured.</td>
</tr>
</tbody>
</table>
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> packet capture buffer-size 4096
<Sysname> packet capture acl 2000
<Sysname> packet capture start

# Restore the default settings for packet capture parameters, and disable packet capture.
<Sysname> undo packet capture

packet capture buffer save

Syntax
packet capture buffer save [ filename ]

View
User view

Default level
1: Monitor level

Parameters
filename: Specifies the name of the file to be saved. The filename cannot contain special characters
such as backslash (\), slash (/), colon (:), asterisk (*), quotation marks (" "), single quotes (’ ’),
less-than sign (<), greater-than sign (>), and vertical bar (|). If you do not specify this argument, the
command saves the file in the default filename pcapbuffer.pcap.

Description
Use packet capture buffer save to save the contents in the packet capture buffer.
• Save the file with a filename in the .pcap format.
• Do not use this command during the packet capturing process.

Related commands: packet capture.

Examples
# Save the contents in the packet capture buffer to file example.pcap.
<Sysname> packet capture buffer save example.pcap

packet capture schedule

Syntax
packet capture schedule datetime time date
undo packet capture schedule

View
User view
Default level
1: Monitor level

Parameters

time: Sets the time in the format of HH:MM:SS. HH takes a value range of 0 to 23, and MM and SS take a value range of 0 to 59.
date: Sets the date in the format of MM/DD/YYYY or YYYY/MM/DD. MM takes a value range of 1 to 12, YYYY takes a value range of 2000 to 2035, and the value range of DD depends on which month the day is in.

Description

Use packet capture schedule to configure a packet capture schedule.
Use undo packet capture schedule to invalidate the configured packet capture schedule.

By default, no packet capture schedule is configured.

- You can use the packet capture start command to enable packet capture as in this command.
- You can use the packet capture command to change packet capture parameters before the packet capture schedule starts, or use the packet capture start command to start packet capture immediately, and the existing packet capture schedule is invalidated.
- To disable packet capture and invalidate the configured packet capture schedule, execute the undo packet capture start command or the undo packet capture command without any keyword.

Related commands: packet capture.

Examples

# Configure a packet capture schedule.
<Sysname> packet capture schedule datetime 12:00:00 2012/12/25

packet capture start

Syntax

packet capture start [ acl { acl-number | ipv6 acl6-number } | buffer-size size | length capture-length | mode { circular | linear } | [ packets packet-number | seconds second-number ]]*

undo packet capture start

View

User view

Default level
1: Monitor level

Parameters

acl: Specifies an ACL for packet capture. If you do not specify this keyword, this command captures all packets that the device receives.
acl-number: Specifies the number of an IPv4 ACL:
- 2000 to 2999 for IPv4 basic ACLs
- 3000 to 3999 for IPv4 advanced ACLs
- 4000 to 4999 for Ethernet frame header ACLs
acl6-number: Specifies the number of an IPv6 ACL:
- 2000 to 2999 for IPv6 basic ACLs
- 3000 to 3999 for IPv6 advanced ACLs
buffer-size size: Specifies the packet capture buffer size in the range of 32 to 65535 KB. The default value is 2048.

length capture-length: Specifies the maximum length of the 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 no need to reconfigure them when you start packet capture again.

Related commands: packet capture stop, display packet capture status, and display packet capture buffer.

Examples

# Set the maximum length of the packet captured as 256 bytes, and start packet capture.

<Sysname> packet capture length 256 start

packet capture stop

Syntax

packet capture stop

View

User view

Default level

1: Monitor level
Parameters
None

Description
Use **packet capture stop** to temporarily stop packet capture.

- After packet capture is stopped, if you use the **packet capture** command to change packet capture parameters, the contents in the capture buffer are cleared.
- This command does not take effect if packet capture is not started.
- After packet capture is stopped, you can use the **display packet capture buffer**, **reset packet capture buffer**, or **packet capture buffer save** command to display or perform operations on the contents in the packet capture buffer, and use the **packet capture start** command to start packet capture again.


Examples

```bash
# 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

```bash
# Clear the contents in the packet capture buffer.
<Sysname> reset packet capture buffer
```

New feature: Enabling log file overwrite-protection

Enabling log file overwrite-protection

This function is available only in FIPS mode.

With log file overwrite-protection enabled, the device will not write new logs into the log files when the number of log files reaches the upper limit or the storage media have no space available.

To enable log file overwrite protection:
### Step 1. Enter system view.

**Command:**

```bash
system-view
```

**Remarks:** N/A

### Step 2. Enable log file overwrite-protection.

**Command:**

```bash
info-center logfile overwrite-protection [ all-port-powerdown ]
```

**Remarks:** By default, this function is disabled.

### NOTE:

With the `all-port-powerdown` argument specified in the `info-center logfile overwrite-protection [ all-port-powerdown ]` command, the device will shut down all its physical Ethernet ports except the management Ethernet port, Ethernet ports configured with stateful failover, and physical ports that have been bound to an IRF port when the number of log files reaches the upper limit or the storage media have no space available.

### Command reference

**info-center logfile overwrite-protection**

#### Syntax

```bash
info-center logfile overwrite-protection [ all-port-powerdown ]
undo info-center logfile overwrite-protection
```

#### View

- **System view**

#### Default level

- **2: System level**

#### Parameters

- **all-port-powerdown:** Shuts down all the physical Ethernet ports on the device except the management Ethernet port, Ethernet ports configured with stateful failover, and physical 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.

#### Description

Use `info-center logfile overwrite-protection` to enable the log file overwrite-protection function. When the number of log files reaches the upper limit or the storage media have no space available, 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 writes new logs into the log files.

This function is disabled by default.

#### Examples

```
# Enable the log file overwrite-protection function.
<Sysname> system-view
<Sysname> info-center logfile overwrite-protection
```
New feature: Setting the MTU of the VPLS instance

Setting the MTU of the VPLS instance

The MTU configured for a VPLS instance applies only to link negotiation messages. It is not used for data packets.

To set the MTU of the VPLS instance:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter VSI view.</td>
<td>vsi vsi-name</td>
</tr>
<tr>
<td>3.</td>
<td>Set the MTU of the VPLS instance.</td>
<td>mtu mtu</td>
</tr>
</tbody>
</table>

Command reference

mtu

Syntax

mtu mtu
undo mtu

View

VSI view

Default level

2: System level

Parameters

mtu: Maximum transmission unit (MTU) for the VPLS instance. The value range is 64 to 9216.

Description

Use mtu to set the MTU of a VPLS instance.

Use undo mtu to restore the default.

By default, the MTU of a VPLS instance is 1,500 bytes.

The MTU of a VPLS instance is a global attribute and is also the MTU of the PW. In Martini VPLS, the MTUs of VPLS instances of peer PEs must be identical. In Kompella VPLS, the MTUs of VPLS instances of peer PEs can be different.

Examples

# Set the MTU of VPLS instance aaa to 1400.
<Sysname> system-view
[Sysname] vsi aaa
[Sysname-vsi-aaa] mtu 1400
New feature: Configuring an OSPFv3 NSSA area

Configuring an OSPFv3 NSSA area

A stub area cannot import external routes, but an NSSA area can import external routes into the OSPFv3 routing domain while retaining other stub area characteristics.

To configure a totally NSSA area, configure the `nssa` command on all the routers attached to the area and configure the `nssa no-summary` command on the ABR. The ABR of a totally NSSA area does not advertise inter-area routes into the area.

Virtual links cannot transit an NSSA area or totally NSSA area.

To configure an NSSA area:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPFv3 view.</td>
<td>ospfv3 [ process-id ]</td>
</tr>
<tr>
<td>3.</td>
<td>Enter area view.</td>
<td>area area-id</td>
</tr>
<tr>
<td>5.</td>
<td>(Optional.) Specify a cost for the default route advertised to the NSSA area.</td>
<td>default-cost cost</td>
</tr>
</tbody>
</table>

Command reference

**nssa (OSPFv3 area view)**

Use `nssa` to configure the current area as an NSSA area.

Use `undo nssa` to restore the default.

**Syntax**

```
nssa [ default-route-advertise [ cost cost | type type ] | no-import-route | no-summary | suppress-fa | { translate-always | translate-never } | translator-stability-interval value ]
undo nssa
```

**Default**

No area is configured as an NSSA area.

**Views**

OSPFv3 area view

**Default command level**

2: System level
Parameters

**default-route-advertise**: Usable on an NSSA ABR or an ASBR only. If it is configured on an NSSA ABR, the ABR generates a default route in a NSSA-external-LSA LSA into the NSSA area regardless of whether a default route is available in the routing table. If it is configured on an ASBR, the ASBR generates a default route in a NSSA-external-LSA LSA only when the default route is available in the routing table. By default, the ABR or ASBR of an NSSA area does not advertise default routes.

**cost** *cost*: Specifies the cost of the default route in the NSSA-external-LSA, in the range of 0 to 16777214.

**type** *type*: Specifies the type of the default route in the NSSA-external-LSA, 1 or 2. The default is 2.

**no-import-route**: Usable only on an NSSA ABR that is also the ASBR of the OSPFv3 routing domain to disable redistributing routes in NSSA-external-LSA LSAs into the NSSA area, making sure that correct external routes are redistributed.

**no-summary**: Usable only on an NSSA ABR to advertise a default route in a Inter-Area-Prefix-LSA into the NSSA area and to not advertise other Inter-Area-Prefix-LSAs into the area. Such an area is a totally NSSA area.

**suppress-fa**: Specifies not to advertise the forwarding address (FA) in AS-external-LSA LSAs translated from locally generated NSSA-external-LSA LSAs.

**translate-always**: Specifies the NSSA ABR as a translator to translate NSSA-external-LSA LSAs to AS-external-LSA LSAs.

**translate-never**: Specifies the NSSA ABR not as a translator to translate NSSA-external-LSA LSAs to AS-external-LSA LSAs.

**translator-stability-interval** *value*: Specifies the stability interval of the translator, during which the translator can maintain its translating capability after a device with a higher priority becomes the new translator. The *value* argument is the stability interval in the range of 0 to 900 seconds and defaults to 0 (which means the translator does not maintain its translating capability when a new translator arises).

Usage guidelines

All routers attached to an NSSA area must be configured with the `nssa` command in area view.

When the `default-route-advertise` argument is specified, the default route takes one of the following cost values in a descending priority order:

- Cost specified by `default-route-advertise cost`
- Cost configured by the `default-cost` command for the area
- Cost configured by the `default cost` command for the process

Examples

```bash
# Configure Area 1 as an NSSA area.
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] area 1
[Sysname-ospfv3-100-area-0.0.0.1] nssa
```

**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`: Specifies a user privilege level in the range of 1 to 3. The default is 3.
- `hash`: Enables hash-based encryption.
- `{ cipher | simple } password`: Specifies a case-sensitive password string. The password length and form requirements vary with the `hash`, `cipher`, and `simple` keyword combinations and FIPS/non-FIPS mode (see Table 9 and Table 10).

**Table 9 Password length and form requirements for the password argument in non-FIPS mode**

<table>
<thead>
<tr>
<th>Keyword combination</th>
<th>Password string form</th>
<th>Length (in characters)</th>
</tr>
</thead>
<tbody>
<tr>
<td>simple</td>
<td>Plain text</td>
<td>1 to 16</td>
</tr>
<tr>
<td>hash simple</td>
<td>Plain text</td>
<td>1 to 16</td>
</tr>
<tr>
<td>cipher</td>
<td>Ciphertext</td>
<td>1 to 53</td>
</tr>
<tr>
<td>hash cipher</td>
<td>Ciphertext (hashed form)</td>
<td>1 to 110</td>
</tr>
</tbody>
</table>

**Table 10 Password length and form requirements for the password argument in FIPS mode**

<table>
<thead>
<tr>
<th>Keyword combination</th>
<th>Password string form</th>
<th>Length (in characters)</th>
</tr>
</thead>
<tbody>
<tr>
<td>simple</td>
<td>Plain text</td>
<td>8 to 16</td>
</tr>
<tr>
<td>cipher</td>
<td>Ciphertext</td>
<td>8 to 53</td>
</tr>
</tbody>
</table>

In FIPS mode, the password must contain uppercase and lowercase letters, digits, and special characters.

Change description

- Added the support for FIPS mode.
- In non-FIPS mode:
  - The `hash` keyword was added to support hash-based encryption.
  - The length of the ciphertext password was changed. After modification, a ciphertext password can be a ciphertext string of 1 to 53 characters or a hashed string of 1 to 110 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:

testation-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

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, must contain at least 8 characters, and must contain uppercase and lowercase letters, digits, and special characters.

Modified command: key (RADIUS scheme view)

Syntax

key { accounting | authentication } [ cipher | simple ] key
undo key { accounting | authentication }

Views

RADIUS scheme view
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, must contain at least 8 characters, and must contain uppercase and lowercase letters, digits, and special 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

Views

Local user view

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 "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

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, must contain at least 8 characters, and must contain uppercase and lowercase letters, digits, and special characters.
Modified command: primary authentication (RADIUS scheme view)

**Syntax**

```text
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

**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, must contain at least 8 characters, and must contain uppercase and lowercase letters, digits, and special characters.

Modified command: secondary accounting (RADIUS scheme view)

**Syntax**

```text
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

**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, must contain at least 8 characters, and must contain uppercase and lowercase letters, digits, and special characters.

Modified command: secondary authentication (RADIUS scheme view)

**Syntax**

```text
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

**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, must contain at least 8 characters, and must contain uppercase and lowercase letters, digits, and special characters.
Modified command: password-control composition

Syntax

```
password-control composition type-number type-length
undo password-control composition
```

Views

System view, user group view, local user view

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

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-length
undo password-control super composition
```

Views

System view

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

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

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

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:

```plaintext
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

Change description

After modification: In FIPS mode, the any authentication method and public key authentication method are deleted.

Modified command: ssh2

Old syntax

```plaintext
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:

```plaintext
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:

```plaintext
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

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-stoc-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] [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] [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] [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**

### Change description

After modification:

- In FIPS mode, the following parameters are added:
  - `prefer-ctos-cipher aes256`: Specifies `aes256-cbc` as the preferred encryption algorithm from client to server.
  - `prefer-stoc-cipher aes256`: Specifies `aes256-cbc` as the preferred encryption algorithm from server to client.

- In FIPS mode, the following parameters are deleted:
  - `identity-key dsa`: Specifies `dsa` as the algorithm for public key authentication.
  - `prefer-ctos-cipher 3des`: Specifies `3des-cbc` as the preferred encryption algorithm from client to server.
  - `prefer-ctos-cipher des`: Specifies `des-cbc` as the preferred encryption algorithm from client to server.
- **prefer-ctos-hmac md5**: Specifies hmac-md5 as the preferred HMAC algorithm from client to server.
- **prefer-ctos-hmac md5-96**: Specifies hmac-md5-96 as the preferred HMAC algorithm from client to server.
- **prefer-kex dh-group-exchange**: Specifies diffie-hellman-group-exchange-sha1 as the preferred key exchange algorithm.
- **prefer-kex dh-group1**: Specifies diffie-hellman-group1-sha1 as the preferred key exchange algorithm.
- **prefer-stoc-cipher 3des**: Specifies 3des-cbc as the preferred encryption algorithm from server to client.
- **prefer-stoc-cipher des**: Specifies des-cbc as the preferred encryption algorithm from server to client.
- **prefer-stoc-hmac md5**: Specifies hmac-md5 as the preferred HMAC algorithm from server to client.
- **prefer-stoc-hmac md5-96**: Specifies hmac-md5-96 as the preferred HMAC algorithm from server to client.

**Modified command: ciphersuite**

**Old syntax**

```
ciphersuite [ rsa_3des_ede_cbc_sha | rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha | rsa_des_cbc_sha | rsa_rc4_128_md5 | rsa_rc4_128_sha ] *
```

**New syntax**

In non-FIPS mode:

```
ciphersuite [ rsa_3des_ede_cbc_sha | rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha | rsa_des_cbc_sha | rsa_rc4_128_md5 | rsa_rc4_128_sha ] *
```

In FIPS mode:

```
ciphersuite [ dhe_rsa_aes_128_cbc_sha | dhe_rsa_aes_256_cbc_sha | rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha ] *
```

**Views**

SSL server policy view

**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

```plaintext
prefer-cipher { rsa_3des_edec_cbc_sha | rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha | rsa_des_cbc_sha | rsa_rc4_128_md5 | rsa_rc4_128_sha }
```

```plaintext
undo prefer-cipher
```

New syntax

In non-FIPS mode:

```plaintext
prefer-cipher { rsa_3des_edec_cbc_sha | rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha | rsa_des_cbc_sha | rsa_rc4_128_md5 | rsa_rc4_128_sha }
```

```plaintext
undo prefer-cipher
```

In FIPS mode:

```plaintext
prefer-cipher { dhe_rsa_aes_128_cbc_sha | dhe_rsa_aes_256_cbc_sha | rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha }
```

```plaintext
undo prefer-cipher
```

Views

SSL client policy view

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_edec_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

```plaintext
certificate request mode { auto [ key-length key-length | password { cipher | simple } password ] | manual }
```

```plaintext
undo certificate request mode
```

Views

PKI domain view

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.
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 ] *
```

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 ] *
```

Views

System view

Change description

This command is not supported in FIPS mode.
Modified command: snmp-agent usm-user { v1 | v2c }

Syntax

```text
snmp-agent usm-user { v1 | v2c } user-name group-name [ acl acl-number | acl 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

```text
snmp-agent calculate-password plain-password mode { 3desmd5 | 3dessha | md5 | sha } { local-engineid | specified-engineid engineid }
```

New syntax

In non-FIPS mode:

```text
snmp-agent calculate-password plain-password mode { 3desmd5 | 3dessha | md5 | sha } { local-engineid | specified-engineid engineid }
```

In FIPS mode:

```text
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

```text
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:

```text
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:

```text
snmp-agent sys-info { contact sys-contact | location sys-location | version v3 }
undo snmp-agent sys-info { contact | location | version v3 }
```
View 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**

```bash
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 \{ 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:

```bash
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 \{ 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:

```bash
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 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 \}
```

View 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**

```bash
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:

```bash
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:
Views
System view

Change description
After modification: In FIPS mode, the keywords md5, 3des, and des56 are deleted.

Modified feature: Displaying RPS status information

Feature change description
Changed the output from the display rps command for 5800-24G Switch (JC100A), 5800-24G TAA Switch (JG255A), 5800-48G Switch with 1 Interface Slot (JC105A), and 5800-48G TAA Switch with 1 Interface Slot (JG258A).

Command changes
Modified command: display rps

Syntax
   display rps [ slot slot-number [ rps-id ] ] [ { begin | exclude | include } regular-expression ]

Views
Any view

Examples
# Display RPS status information.
<Sysname> display rps
Slot 1
   Rps  1
   State : Normal
Slot 2
   Rps  1
   State : Absent

Change description
Before modification: The value of the State field can be:
   • Normal—The DC cable is properly connected and the RPS is providing power.
   • Absent—The DC cable is not connected.
   • Fault—The DC cable is properly connected but the RPS has failed or is not providing power.

After modification: The value of the State field can be:
   • Normal—The DC cable is properly connected and the RPS is providing power.
   • Standby—The DC cable is properly connected but the RPS is not providing power.
   • Absent—The DC cable is not connected, or the DC cable is properly connected but the RPS has failed.
This release has the following changes:

- **New feature**: Disabling MAC entry aging timer refresh based on destination MAC address
- **Modified feature**: Support for MD5 authentication key rollover
- **Modified feature**: Offline detect timer
- **Modified feature**: Configuring the frequency with which the log file is saved

### 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Disable MAC entry aging</td>
<td>By default, MAC entry aging timer refresh based on</td>
</tr>
<tr>
<td></td>
<td>timer refresh based on destination MAC address.</td>
<td>destination MAC address is enabled.</td>
</tr>
<tr>
<td></td>
<td>mac-address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>destination-hit disable</td>
<td></td>
</tr>
</tbody>
</table>

### Application example

Microsoft Network Load Balancing (NLB) is a load balancing technology for server clustering developed on Windows Server.

**Figure 9 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
```

Modified feature: Support for MD5 authentication key rollover

Feature change description

Support for MD5 authentication key rollover was added to this release.

Configuring OSPF authentication

Configure OSPF packet authentication to ensure the security of packet exchange.

After authentication is configured, OSPF only receives packets that pass authentication. Failed packets cannot establish neighboring relationships.
To configure OSPF packet authentication, the authentication mode and password for all routers on the same network segment must be identical.

OSPF authentication includes area authentication and interface authentication. Interface authentication has higher priority than area authentication. If you configure interface authentication and area authentication at the same time, the interface authentication configuration takes effect.

To configure OSPF authentication for an area:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ospf [ process-id</td>
<td>router-id router-id</td>
</tr>
<tr>
<td>3.</td>
<td>area area-id</td>
<td>N/A</td>
</tr>
</tbody>
</table>

In OSPF area authentication, to modify MD5/HMAC-MD5 authentication key ID without tearing down OSPF neighbor connections, perform the following key rollover configurations:

1. Configure a new MD5/HMAC-MD5 authentication key ID for the area. If the new key ID is not configured on neighbor devices, MD5 authentication key rollover is triggered. During key rollover, OSPF sends multiple packets that contain both the new and old MD5/HMAC-MD5 authentication key IDs to make sure all neighbor devices can pass the authentication.

2. Configure the new MD5/HMAC-MD5 authentication key ID on all neighbor devices. When the local device receives packets with the new key ID from all neighbor devices, it exits MD5 key rollover.

3. Delete the old MD5/HMAC-MD5 authentication key ID from the local device and all its neighbors.

HP recommends that you not retain multiple MD5/HMAC-MD5 authentication key IDs for an area. After you modify the MD5/HMAC-MD5 authentication key ID, delete the old key ID in time. This helps prevent attacks from devices that use the old key ID for communication and reduce system resources and bandwidth consumption caused by key rollover.

To configure OSPF authentication for an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
</tbody>
</table>

In OSPF area authentication, to modify MD5/HMAC-MD5 authentication key ID without tearing down OSPF neighbor connections, perform the following key rollover configurations:

1. Configure a new MD5/HMAC-MD5 authentication key ID for the area. If the new key ID is not configured on neighbor devices, MD5 authentication key rollover is triggered. During key rollover, OSPF sends multiple packets that contain both the new and old MD5/HMAC-MD5 authentication key IDs to make sure all neighbor devices can pass the authentication.

2. Configure the new MD5/HMAC-MD5 authentication key ID on all neighbor devices. When the local device receives packets with the new key ID from all neighbor devices, it exits MD5 key rollover.

3. Delete the old MD5/HMAC-MD5 authentication key ID from the local device and all its neighbors.

HP recommends that you not retain multiple MD5/HMAC-MD5 authentication key IDs for an area. After you modify the MD5/HMAC-MD5 authentication key ID, delete the old key ID in time. This helps prevent attacks from devices that use the old key ID for communication and reduce system resources and bandwidth consumption caused by key rollover.
In OSPF interface authentication, to modify MD5/HMAC-MD5 authentication key ID without tearing down OSPF neighbor connections, perform the following key rollover configurations:

1. Configure a new MD5/HMAC-MD5 authentication key ID for the interface. If the new key ID is not configured on neighbor devices, MD5 authentication key rollover is triggered. During key rollover, OSPF sends multiple packets that contain both the new and old MD5/HMAC-MD5 authentication key IDs to make sure all neighbor devices can pass the authentication.

2. Configure the new MD5/HMAC-MD5 authentication key ID on all neighbor devices. When the local device receives packets with the new key ID from all neighbor devices, it exits MD5 key rollover.

3. Delete the old MD5/HMAC-MD5 authentication key ID from the local device and all its neighbors.

HP recommends that you not retain multiple MD5/HMAC-MD5 authentication key IDs for an interface. After you modify the MD5/HMAC-MD5 authentication key ID, delete the old key ID in time. This helps prevent attacks from devices that use the old key ID for communication and reduce system resources and bandwidth consumption caused by key rollover.

OSPF virtual link authentication and OSPF sham link authentication also support MD5/HMAC-MD5 authentication key rollover. The configuration procedure is similar to that of the OSPF area authentication.

**Modified command: authentication-mode**

**Old syntax**

```
authentication-mode { md5 | simple }
undo authentication-mode
```

**New syntax**

For MD5/HMAC-MD5 authentication:

```
authentication-mode { hmac-md5 | md5 } key-id { cipher | plain } password
undo authentication-mode [ { hmac-md5 | md5 } key-id ]
```

For simple authentication mode:

```
authentication-mode simple { cipher | plain } password
undo authentication-mode
```

**Views**

OSPF area view

**Change description**

Before modification: You can configure only the authentication mode.

After modification: You can configure both the authentication mode and password.

**Modified feature: Offline detect timer**

**Feature change description**

Changed the value range for the offline detect timer.
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 offline detect timer is in the range of 60 to 65535.
After modification: The offline detect timer is in the range of 60 to 2147483647.

Modified feature: Configuring the frequency with which the log file is saved

Feature change description

The frequency value range for log file saving is now 3600 to 86400.

Command changes

Modified command: info-center logfile frequency

Syntax

info-center logfile frequency freq-sec

Views

System view

Change description

Before modification: The frequency value range for log file saving is 1 to 86400.
After modification: The frequency value range for log file saving is 3600 to 86400.
This release has the following changes:

- **Modified feature: Default configuration**

## Modified feature: Default configuration

### Feature change description

The following changes are made to the default configuration in this release:

- The `telnet server enable` command is deleted and Telnet service is disabled.
- The `interface vlan-interface1` command is deleted and VLAN-interface 1 does not exist.
- The `ip address dhcp-alloc client-identifier mac Vlan-interface1` command is deleted and VLAN-interface 1 does not apply for an IP address.
- The `undo 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
This release has the following changes:

- New feature: Configuring an 802.1X VLAN group
- New feature: Configuring common global CAR
- New feature: Exchange of IP address information with CDP neighbors
- New feature: Configuring the VPN instance of the sFlow collector
- New feature: Setting the subnet mask length to be 31
- New Feature: Displaying per-port queue-based traffic statistics
- New feature: Specifying a fixed verification code for Web login
- New feature: Specifying the authentication mode for users trying to log in to the device through HTTPS
- New feature: Setting the Web user connection timeout time
- New feature: Setting the size of the buffer for Web login logging
- New feature: Configuring and displaying brand information
- New feature: Displaying the software and hardware copyright statements
- New feature: Creating a bidirectional MPLS TE tunnel
- New feature: Configuring DM
- New feature: Configuring static VPLS
- New feature: Configuring traffic policing for VPLS
- New feature: Enabling VPLS statistics
- New feature: Configuring SVC MPLS L2VPN for a service instance or on a Layer 3 interface
- New feature: Configuring traffic policing for an AC
- New feature: Enabling traffic statistics for an AC
- New feature: Configuring a user-defined ACL
- New feature: Configuring ECN for a queue
- New feature: Configuring IPv6 portal
- New feature: Specifying an ISP domain for users with unknown domain names
- New feature: MVRP
- New feature: Enabling sending ICMPv6 redirect messages
- New feature: Configuring DHCPv6 snooping to support Option 18 and Option 37
- New feature: Configuring the DHCPv6 server to assign IPv6 addresses to DHCPv6 clients
- New feature: Specifying a destination server for a private network
- New feature: Configuring the uplink port to permit multiple isolate-user-VLANs
- Modified feature: Displaying information about static CR-LSPs on a node
- Modified feature: Configuring Martini MPLS L2VPN
- Modified feature: Configuring the URL for the CRL distribution point
- Modified feature: Creating and displaying IPsec transform sets
- Modified feature: Specifying a transform set referenced by the IPsec policy
- Modified feature: Specifying the encryption algorithm for the ESP
- Modified feature: Enabling DHCPv6 server on an interface
• Modified feature: Setting a password for local authentication
• 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: Configuring an 802.1X VLAN group

Configuring an 802.1X VLAN group

For more information about 802.1X VLAN group configurations, see "Configuring 802.1X" in HP 5820X & 5800 Security Configuration Guide-F1805.

Command reference

New commands: vlan-group and vlan-list
For more information about the commands, see "802.1X commands" in HP 5820X & 5800 Security Command Reference-F1805.

New feature: Configuring common global CAR

Configuring common global CAR

For more information about common global CAR configuration, see "Configuring global CAR" in HP 5820X & 5800 ACL and QoS Configuration Guide-F1805.

Command reference

New commands: qos car
For more information about common global CAR configuration commands, see "Global CAR commands" in HP 5820X & 5800 ACL and QoS Command Reference-F1805.

New feature: Exchange of IP address information with CDP neighbors

Enabling LLDP to exchange IP address information with CDP neighbors

To enable this feature, you only need to enable LLDP and CDP-compatible LLDP.
For more information about LLDP and CDP-compatible LLDP, see "Configuring LLDP" in HP 5820X & 5800 Layer 2—LAN Switching Configuration Guide-F1805.

Command reference

You can use the display lldp neighbor-information command to view the IP address information of 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 11 Command output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDP neighbor-information of port 2</td>
<td>CDP information received through port 2.</td>
</tr>
<tr>
<td>CDP neighbor index</td>
<td>Index of the CDP neighboring device.</td>
</tr>
<tr>
<td>Chassis ID</td>
<td>Name of the CDP neighboring device.</td>
</tr>
<tr>
<td>Address</td>
<td>IPv4 address of the port that connects the CDP neighboring device to the local device.</td>
</tr>
<tr>
<td>Port ID</td>
<td>ID of the port that connects the CDP neighboring device to the local device.</td>
</tr>
<tr>
<td>Software version</td>
<td>Software version of the CDP neighboring device.</td>
</tr>
<tr>
<td>Platform</td>
<td>Model of the CDP neighboring device.</td>
</tr>
<tr>
<td>Duplex</td>
<td>Duplex state of the port that connects the CDP neighboring device to the local device.</td>
</tr>
</tbody>
</table>

New feature: Configuring the VPN instance of the sFlow collector

Configuring the VPN instance of the sFlow collector

For more information about configuring the VPN instance of the sFlow collector, see "Configuring sFlow" in *HP 5820X & 5800 Network Management and Monitoring Configuration Guide-F1805.*
Command reference

Modified command: Option `vpn-instance vpn-instance-name` was added to the `sflow collector` command.

For more information about configuring the VPN instance of the sFlow collector commands, see "sFlow configuration commands" in HP 5820X & 5800 Network Management and Monitoring Command Reference-F1805.

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: 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:

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display per-port queue-based traffic statistics.</td>
<td><code>display qos queue-statistics interface</code></td>
<td>Available in any view</td>
</tr>
<tr>
<td></td>
<td>`{ interface-type interface-number } [ outbound ] [</td>
<td></td>
</tr>
<tr>
<td></td>
<td>{ begin</td>
<td>exclude</td>
</tr>
</tbody>
</table>
Command reference

display qos queue-statistics

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.

Description

Use display qos queue-statistics interface to display statistics collected for an interface on a per-queue basis.

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

<table>
<thead>
<tr>
<th>Queue</th>
<th>Queued packets</th>
<th>Passed packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2,689</td>
<td>94,816,515</td>
<td>94,851,667</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>26</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 12 Command output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface for which queue-based traffic statistics are displayed.</td>
</tr>
</tbody>
</table>
### New feature: Specifying a fixed verification code for Web login

Specifying a fixed verification code for Web login

For more information about specifying a fixed verification code for Web login configuration, see “Login Management Configuration” in Fundamentals Configuration Guide of HP 5820X & 5800 Fundamentals Configuration Guide-F1805.

#### Command reference

**New command: `web captcha`**

For more information about this command, see “Login Management commands” in Fundamentals Command Reference of HP 5820X & 5800 Fundamentals Command Reference-F1805.

### New feature: Specifying the authentication mode for users trying to log in to the device through HTTPS

Specifying the authentication mode for users trying to log in to the device through HTTPS

For more information about specifying the authentication mode for users trying to log in to the device through HTTPS configuration, see “Login Management Configuration” in Fundamentals Configuration Guide of HP 5820X & 5800 Fundamentals Configuration Guide-F1805.

#### Command reference

**New command: `web https-authorization mode`**

For more information about this command, see “Login Management commands” in Fundamentals Command Reference of HP 5820X & 5800 Fundamentals Command Reference-F1805.

### New feature: Setting the Web user connection timeout time

Setting the Web user connection timeout time

For more information about setting the Web user connection timeout time configuration, see “Login Management Configuration” in Fundamentals Configuration Guide of HP 5820X & 5800 Fundamentals Configuration Guide-F1805.
Command reference

New command: **web idle-timeout**

For more information about this command, see “Login Management commands” in *Fundamentals Command Reference of HP 5820X & 5800 Fundamentals Command Reference-F1805*.

**New feature: Setting the size of the buffer for Web login logging**

Setting the size of the buffer for Web login logging

For more information about setting the size of the buffer for Web login logging configuration, see “Login Management Configuration” in *Fundamentals Configuration Guide of HP 5820X & 5800 Fundamentals Configuration Guide-F1805*.

Command reference

New command: **web logbuffer size**

For more information about this command, see “Login Management commands” in *Fundamentals Command Reference of HP 5820X & 5800 Fundamentals Command Reference-F1805*.

**New feature: Configuring and displaying brand information**

Configuring and displaying brand information


Command reference

New commands: **brand, display brand**

For more information about these commands, see “Device Management commands” in *Fundamentals Command Reference of HP 5820X & 5800 Fundamentals Command Reference-F1805*.

**New feature: Displaying the software and hardware copyright statements**

Displaying the software and hardware copyright statements

For more information about displaying alarm information configuration, see “Device Management Configuration” in *Fundamentals Configuration Guide of HP 5820X & 5800 Fundamentals Configuration Guide-F1805*.
Command reference

New command: **display copyright**
For more information about this command, see “Device Management commands” in Fundamentals Command Reference of HP 5820X & 5800 Fundamentals Command Reference-F1805.

**New feature: Creating a bidirectional MPLS TE tunnel**

Creating a bidirectional MPLS TE tunnel
For more information about creating a bidirectional MPLS TE tunnel, see "Configuring MPLS TE" in HP 5820X & 5800 MPLS Configuration Guide-F1805.

Command reference

New command: **mpls te bidirectional**.
For more information about bidirectional MPLS TE tunnel configuration commands, see "MPLS TE configuration commands" in HP 5820X & 5800 MPLS Command Reference-F1805.

**New feature: Configuring DM**

Configuring DM
For more information about DM configuration, see "Configuring MPLS TE" in HP 5820X & 5800 MPLS Configuration Guide-F1805.

Command reference

New command: **moam-dm**.
For more information about DM configuration commands, see "MPLS TE configuration commands" in HP 5820X & 5800 MPLS Command Reference-F1805.

**New feature: Configuring static VPLS**

Configuring static VPLS
For more information about static VPLS configuration, see "Configuring VPLS" in HP 5820X & 5800 MPLS Configuration Guide-F1805.

Command reference

New commands:
- **static backup-label**
- **static label** (L2VPN peer view)
Modified command: **pwsignal**.
The static keyword was added to the pwsignal command. For more information about static VPLS configuration commands, see "VPLS configuration commands" in HP 5820X & 5800 MPLS Command Reference-F1805.

New feature: Configuring traffic policing for VPLS

Configuring traffic policing for VPLS

For more information about traffic policing for VPLS configuration, see "Configuring VPLS" in HP 5820X & 5800 MPLS Configuration Guide-F1805.

Command reference

New commands: car and qos car.

For more information about traffic policing for VPLS configuration commands, see "VPLS configuration commands" in HP 5820X & 5800 MPLS Command Reference-F1805.

New feature: Enabling VPLS statistics

Enabling VPLS statistics

For more information about VPLS statistics configuration, see "Configuring VPLS" in HP 5820X & 5800 MPLS Configuration Guide-F1805.

Command reference

New commands:

• display mpls statistics pw
• reset mpls statistics pw
• reset service-instance statistics
• statistics
• statistics enable.

For more information about VPLS statistics configuration commands, see "VPLS configuration commands" in HP 5820X & 5800 MPLS Command Reference-F1805.

New feature: Configuring SVC MPLS L2VPN for a service instance or on a Layer 3 interface

Configuring SVC MPLS L2VPN for a service instance or on a Layer 3 interface

You can configure SVC MPLS L2VPN for a service instance or on a Layer 3 interface.

For more information about SVC MPLS L2VPN configuration, see "Configuring MPLS L2VPN" in HP 5820X & 5800 MPLS Configuration Guide-F1805.
Command reference

New commands:
- `mpls static-l2vc`
- `static label` (static-L2VC view, static-xpeer view)
- `xconnect static-peer`

For more information about SVC MPLS L2VPN configuration commands, see "MPLS L2VPN configuration commands" in HP 5820X & 5800 MPLS Command Reference-F1805.

**New feature: Configuring traffic policing for an AC**

Configuring traffic policing for an AC

For more information about AC traffic policing configuration, see "Configuring MPLS L2VPN" in HP 5820X & 5800 MPLS Configuration Guide-F1805.

Command reference

New commands: `car`

For more information about AC traffic policing configuration commands, see "MPLS L2VPN configuration commands" in HP 5820X & 5800 MPLS Command Reference-F1805.

**New feature: Enabling traffic statistics for an AC**

Enabling traffic statistics for an AC

For more information about AC traffic statistics configuration, see "Configuring MPLS L2VPN" in HP 5820X & 5800 MPLS Configuration Guide-F1805.

Command reference

New commands: `statistics`

For more information about AC traffic statistics configuration commands, see "MPLS L2VPN configuration commands" in HP 5820X & 5800 MPLS Command Reference-F1805.

**New feature: Configuring a user-defined ACL**

Configuring a user-defined ACL

For more information about user-defined ACL configuration, see "Configuring ACLs" in HP 5820X & 5800 ACL and QoS Configuration Guide-F1805.

Command reference

New command: `rule` (user-defined ACL view)

The user-defined ACL number ranges from 5000 to 5999 in the following commands: `acl`, `acl copy`, `display acl`, `packet-filter`, and `reset acl counter`. 
The following commands can be executed in user-defined ACL view: rule comment and rule remark.

For more information about user-defined ACL configuration commands, see "ACL configuration commands" in HP 5820X & 5800 ACL and QoS Command Reference-F1805.

New feature: Configuring ECN for a queue

Configuring ECN for a queue

For more information about ECN configuration, see "Configuring congestion avoidance" in HP 5820X & 5800 ACL and QoS Configuration Guide-F1805.

Command reference

New commands: queue ecn

For more information about ECN configuration commands, see "Congestion avoidance commands" in HP 5820X & 5800 ACL and QoS Command Reference-F1805.

New feature: Configuring IPv6 portal

Configuring IPv6 portal

For more information about configuring IPv6 portal, see "Configuring portal authentication" in HP 5820X & 5800 Security Configuration Guide-F1805.

Command reference

IPv6 related parameters were added to the following commands:

- portal auth-network
- portal delete-user
- portal domain
- portal free-rule
- portal nas-ip
- portal server

For more information about these commands, see "Portal configuration commands" in HP 5820X & 5800 Security Command Reference-F1805.

New feature: Specifying an ISP domain for users with unknown domain names

Specifying an ISP domain for users with unknown domain names

For more information about specifying an ISP domain for users with unknown domain names, see "Configuring AAA" in HP 5820X & 5800 Security Configuration Guide-F1805.
Command reference

New command: `domain if-unknown`.
For more information about this command, see "AAA configuration commands" in *HP 5820X & 5800 Security Command Reference-F1805*.

New feature: MVRP

Configuring MVRP

For more information about "Configuring MVRP", see *HP 5820X & 5800 Layer 2—LAN Switching Configuration Guide-F1805*.

Command reference

For more information about "MVRP commands", see *HP 5820X & 5800 Layer 2—LAN Switching Command Reference-F1805*.

New feature: Enabling sending ICMPv6 redirect messages

Enabling sending ICMPv6 redirect messages

For more information about enabling sending ICMPv6 redirect messages, see "Configuring IPv6 basics" in *HP 5820X & 5800 Layer 3—IP Services Configuration Guide-F1805*.

Command reference

New command: `ipv6 redirects enable`.
For more information about this command, see "IPv6 basics configuration commands" in *HP 5820X & 5800 Layer 3—IP Services Command Reference-F1805*.

New feature: Configuring DHCPv6 snooping to support Option 18 and Option 37

Configuring DHCPv6 snooping to support Option 18 and Option 37

For more information about configuring DHCPv6 snooping to support Option 18 and Option 37, see "Configuring DHCPv6 snooping" in *HP 5820X & 5800 Layer 3—IP Services Configuration Guide-F1805*.

Command reference

New commands:
- `ipv6 dhcp snooping option interface-id enable`
- `ipv6 dhcp snooping option interface-id enable`
- `ipv6 dhcp snooping option remote-id enable`
New feature: Configuring the DHCPv6 server to assign IPv6 addresses to DHCPv6 clients

Configuring the DHCPv6 server to assign IPv6 addresses to DHCPv6 clients

For more information about configuring the DHCPv6 server to assign IPv6 addresses to DHCPv6 clients, see "Configuring DHCPv6 server" in HP 5820X & 5800 Layer 3—IP Services Configuration Guide-F1805.

Command reference

New commands:
- static-bind address
- network
- display ipv6 dhcp server conflict
- display ipv6 dhcp server conflict
- display ipv6 dhcp server ip-in-use
- reset ipv6 dhcp server conflict
- reset ipv6 dhcp server conflict

For more information about these commands, see "DHCPv6 configuration commands" in HP 5820X & 5800 Layer 3—IP Services Command Reference-F1805.

New feature: Specifying a destination server for a private network

Specifying a destination server for a private network

For more information about specifying a destination server for a private network, see "Configuring UDP helper" in HP 5820X & 5800 Layer 3—IP Services Configuration Guide-F1805.

Command reference

Option **vpn-instance vpn-instance-name** was added to the **udp-helper server** command to specify the VPN to which the destination server belongs.

For more information about this command, see "UDP helper configuration commands" in HP 5820X & 5800 Layer 3—IP Services Command Reference-F1805.
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 Table 12 and Figure 10, 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-VLAN 2, 3, and 4 pass through the uplink port (the port connecting Device B to Device A in Table 12 and Figure 10) tagged. Device A identifies only VLANs 2, 3, and 4.

Figure 10 Application scenario

Configuration procedure

To configure the uplink port to permit packets from multiple isolate-user-VLANs to pass through tagged:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a VLAN and enter VLAN view.</td>
<td>vlan vlan-id</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the VLAN as an isolate-user-VLAN.</td>
<td>isolate-user-vlan enable</td>
</tr>
<tr>
<td>4.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>5.</td>
<td>Configure multiple VLANs in batch.</td>
<td>vlan { vlan-id1 [ to vlan-id2 ]</td>
</tr>
<tr>
<td>6.</td>
<td>Isolate ports in the same secondary</td>
<td>isolated-vlan enable</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>VLAN at Layer 2.</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>7.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
</tbody>
</table>
| 8. | Configure the uplink port. | a. Enter Layer-2 Ethernet interface view or Layer-2 aggregate interface view: `interface interface-type interface-number`  
  b. Configure the port to operate in promiscuous mode in the specified VLANs: `port isolate-user-vlan vlan-list trunk promiscuous` | By default, a port does not operate in promiscuous mode. |
| 9. | Configure the downlink port. | a. Enter Layer-2 Ethernet interface view or Layer-2 aggregate interface view: `interface interface-type interface-number`  
  b. (Optional.) Configure the link type of the port: `port link-type { access | hybrid | trunk }`  
  c. Assign the downlink port to the specified secondary VLANs (use one of the commands depending on the link type): `port access vlan vlan-id`  
  Or `port trunk permit vlan { vlan-list | all }`  
  Or `port hybrid vlan vlan-list { tagged | untagged }`  
  d. Configure the downlink port to operate in host mode: `port isolate-user-vlan host` | By default, a port does not operate in host mode. |
| 10. | Return to system view. | quit | N/A |
| 11. | Associate the specified secondary VLANs with an isolate-user-VLAN. | `isolate-user-vlan isolate-user-vlan-id secondary secondary-vlan-id [ to secondary-vlan-id ]` | By default, no isolate-user-VLAN is associated with a secondary VLAN. |

⚠️ **CAUTION:**

The `port isolate-user-vlan vlan-list trunk promiscuous` command and the `port isolate-user-vlan vlan-id promiscuous` command are mutually exclusive. The two commands are different as follows:

- The former configures a port to permit packets from multiple isolate-user-VLANs to pass through tagged.
- The latter configures a port to permit packets from only one isolate-user-VLAN to pass through untagged.
NOTE:
For more information about the isolate-user-VLAN configuration, see Layer 2—LAN Switching Configuration Guide.

Configuration example

Network requirements

As shown in Figure 11, 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 11 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

# 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 2 and 3 with isolate-user-VLAN 5.
[DeviceB] isolate-user-vlan 5 secondary 2 to 3

# 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
#
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

Modified feature: Displaying information about static CR-LSPs on a node

Feature change description

You can specify the egress, ingress, or transit keyword to display information about static CR-LSPs on a node acting as egress, ingress, or transit LSR.

Command changes

Modified command: display mpls static-cr-lsp

Old syntax

```
display mpls static-cr-lsp [ lsp-name lsp-name ] [ { include | exclude } ip-address prefix-length ] [ verbose ] [ { begin | exclude | include } regular-expression ]
```

New syntax

```
display mpls static-cr-lsp [ lsp-name lsp-name ] [ egress | ingress | transit ] [ { include | exclude } ip-address prefix-length ] [ verbose ] [ { begin | exclude | include } regular-expression ]
```

Views

Any view

Change description

Before modification: The display mpls static-cr-lsp command can only display information about all static CR-LSPs on the node.

After modification: After you specify the egress, ingress, or transit keyword, this command can display information about static CR-LSPs on a node acting as an egress, ingress, or transit LSR.

Modified feature: Configuring Martini MPLS L2VPN

Feature change description

Ethernet and VLAN were added to the PW encapsulation types for Martini MPLS L2VPN on a Layer 3 interface.

Command changes

Modified command: mpls static-l2vc destination

Old syntax

```
    mpls static-l2vc destination destination-router-id transmit-vpn-label transmit-label-value receive-vpn-label receive-label-value [ tunnel-policy tunnel-policy-name ]
```
New syntax

mpls static-l2vc destination destination-router-id transmit-vpn-label transmit-label-value receive-vpn-label receive-label-value [ { ethernet | vlan } | tunnel-policy tunnel-policy-name ] *

Views

Interface view

Change description

Before modification: The **ethernet** and **vlan** keywords are not supported.

After modification: The **ethernet** and **vlan** keywords are available to specify the PW encapsulation type as Ethernet or VLAN.

**Modified feature: Configuring the URL for the CRL distribution point**

Feature change description

Changed the length of the URL.

Command changes

Modified command: crl url

Syntax

crl url url-string

Views

PKI domain view

Change description

Before modification: The URL specified by the **url-string** argument is a case-insensitive string of 1 to 127 characters.

After modification: The URL specified by the **url-string** argument is a case-insensitive string of 1 to 255 characters.

**Modified feature: Creating and displaying IPsec transform sets**

Feature change description

- Changed the command for creating IPsec transform sets.
- Changed the command for displaying IPsec transform sets.
Command changes

Modified command: display ipsec transform-set

Old syntax

display ipsec proposal [ proposal-name ] [ | { begin | exclude | include } regular-expression ]

New syntax

display ipsec transform-set [ transform-set-name ] [ | { begin | exclude | include } regular-expression ]

Views

Any view

Change description

Before modification: display ipsec proposal
After modification: display ipsec transform-set

Modified command: ipsec transform-set

Old syntax

ipsec proposal proposal-name

New syntax

ipsec transform-set transform-set-name

Views

System view

Change description

Before modification: ipsec proposal
After modification: ipsec transform-set

Modified feature: Specifying a transform set referenced by the IPsec policy

Feature change description

Changed the command for specifying a transform set referenced by the IPsec policy.

Command changes

Modified command: transform-set

Old syntax

proposal proposal-name

New syntax

transform-set transform-set-name
Modified feature: Specifying the encryption algorithm for the ESP

Feature change description

Changed the available parameters for the AES-CBC algorithm for the ESP.

Command changes

Modified command: esp encryption-algorithm

Old syntax

esp encryption-algorithm { 3des | aes [ key-length ] | des } *

New syntax

esp encryption-algorithm { 3des | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | des } *

Modified feature: Enabling DHCPv6 server on an interface

Feature change description

To enable the switch (DHCPv6 server) to assign IPv6 prefixes to clients, specify the apply pool pool-number option. This option is optional when the DHCPv6 server assigns only IPv6 addresses to clients.
Command changes

Modified command: ipv6 dhcp server

Old syntax

```
ipv6 dhcp server apply pool pool-number [ allow-hint | preference preference-value | rapid-commit ] *
undo ipv6 dhcp server apply pool
```

New syntax

```
ipv6 dhcp server [ allow-hint | apply pool pool-number | preference preference-value | rapid-commit ] *
undo ipv6 dhcp server
```

Views

Interface view

Change description

Before modification: Option `apply pool pool-number` is required.
After modification: Option `apply pool pool-number` is optional.

**Modified feature: Setting a password for local authentication**

Feature change description

A password configured by the `set authentication password` command for local authentication can now be hashed.

Command changes

Modified command: set authentication password

Old syntax

```
set authentication password { simple | cipher } password
```

New syntax

```
set authentication password [ hash ] { simple | cipher } password
```

Views

User interface view

Change description

Before modification: A password cannot be hashed when configured by using the `set authentication password` command.
After modification: A password can be hashed when configured by using the `set authentication password` command.
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 `undo ip http enable` command is added and HTTP service is disabled.

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
This release has the following changes:

- New Feature: Setting the DSCP value for multiple types of protocol packets
- New feature: Setting a DSCP value for an ISP domain
- New feature: Delaying the MAC authentication
- Modified feature: tunnel bandwidth
- Modified feature: Establishing a connection to an SCP server to transfer files with the server
- Modified feature: Configuring the maximum number of routes in a VPN instance
- Modified feature: Configuring PBR to support next hops in VPN instances
- Modified feature: Commands related to password
- Modified feature: Setting the IRF link down report delay

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 BGP, IPv6 BGP, OSPF, RIP, DHCP, DHCPv6, DNS, and IPv6 DNS.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>bgp as-number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP-VPN instance view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. bgp as-number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. ipv4-family</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vpn-instance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vpn-instance-name</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Set the DSCP value for BGP protocol packets sent to the specified BGP peer or BGP peer group.</td>
<td>peer { group-name</td>
</tr>
</tbody>
</table>
Setting the DSCP value for IPv6 BGP protocol packets

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>bgp as-number</td>
<td>Required.</td>
</tr>
<tr>
<td>3.</td>
<td>ipv6-family</td>
<td>N/A</td>
</tr>
<tr>
<td>4.</td>
<td>peer (ipv6-group-name</td>
<td>dscp dscp-value</td>
</tr>
</tbody>
</table>

Setting the DSCP value for OSPF protocol packets

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ospf [process-id]</td>
<td>router-id</td>
</tr>
<tr>
<td>3.</td>
<td>dscp dscp-value</td>
<td>Optional. The default value is 48.</td>
</tr>
</tbody>
</table>

Setting the DSCP value for RIP protocol packets

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>5.</td>
<td>rip [process-id]</td>
<td>[vpn-instance]</td>
</tr>
<tr>
<td>6.</td>
<td>dscp dscp-value</td>
<td>Optional. The default value is 48.</td>
</tr>
</tbody>
</table>

Setting the DSCP value for DHCPv6 protocol packets

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ipv6 dhcp dscp dscp-value</td>
<td>Optional. The default value is 56.</td>
</tr>
</tbody>
</table>
### Setting the DSCP value for DHCP protocol packets

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>dhcp dscp $dscp-value$</td>
<td>Optional. The default value is 56.</td>
</tr>
<tr>
<td>3.</td>
<td>dhcp client dscp $dscp-value$</td>
<td>Optional. The default value is 56.</td>
</tr>
</tbody>
</table>

### Setting the DSCP value for DNS protocol packets

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>dns dscp $dscp-value$</td>
<td>Optional. The default value is 0.</td>
</tr>
</tbody>
</table>

### Setting the DSCP value for IPv6 DNS protocol packets

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>dns ipv6 dscp $dscp-value$</td>
<td>Optional. The default value is 0.</td>
</tr>
</tbody>
</table>

### Setting the ToS value for packets sent by the TCP/UDP listening service on the NQA server

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>nqa server (tcp-connect</td>
<td>udp-echo ) tos $tos$</td>
</tr>
</tbody>
</table>
### Setting the ToS value for NQA probe packets

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>nqa entry admin-name operation-tag</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>type dhcp</td>
<td>Required.</td>
</tr>
<tr>
<td>4.</td>
<td>tos value</td>
<td>Optional. The default value is 0.</td>
</tr>
</tbody>
</table>

### Setting the DSCP value for NTP protocol packets

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ntp-service dscp dscp-value</td>
<td>Optional. The default value is 16.</td>
</tr>
</tbody>
</table>

### Setting the DSCP value for SNMP trap packets

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>snmp-agent target-host trap address udp-domain { ip-address</td>
<td>ipv6 ipv6-address } [ udp-port port-number ] [ dscp dscp-value ] [ vpn-instance vpn-instance-name</td>
</tr>
</tbody>
</table>

### Setting the DSCP value for SNMP response packets

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>snmp-agent packet response dscp dscp-value</td>
<td>Optional. The default value is 0.</td>
</tr>
</tbody>
</table>

### Setting the DSCP value for the protocol packets sent to the log host
### Step 1
Enter system view.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Step 2
Set the DSCP value for the protocol packets sent to the log host.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>`info-center loghost [ vpn-instance vpn-instance-name ] { host-ipv4-address</td>
<td>ipv6 host-ipv6-address } [ port port-number ] [ dscp dscp-value ] [ channel { channel-number</td>
</tr>
</tbody>
</table>

### Setting the DSCP value for RADIUS protocol packets

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Set the DSCP value for IPv4 RADIUS protocol packets.</td>
<td><code>radius dscp dscp-value</code></td>
</tr>
<tr>
<td>3.</td>
<td>Set the DSCP value for IPv6 RADIUS protocol packets.</td>
<td><code>radius ipv6 dscp dscp-value</code></td>
</tr>
</tbody>
</table>

### Setting the DSCP value for VRRP protocol packets

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Set the DSCP value for IPv4 VRRP protocol packets.</td>
<td><code>vrrp dscp dscp-value</code></td>
</tr>
<tr>
<td>3.</td>
<td>Set the DSCP value for IPv6 VRRP protocol packets.</td>
<td><code>vrrp ipv6 dscp dscp-value</code></td>
</tr>
</tbody>
</table>

### Setting the DSCP value for IGMP protocol packets sent by IGMP snooping

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter IGMP-snooping view.</td>
<td><code>igmp-snooping</code></td>
</tr>
<tr>
<td>3.</td>
<td>Set the DSCP value for IGMP protocol packets sent by IGMP snooping.</td>
<td><code>dscp dscp-value</code></td>
</tr>
</tbody>
</table>
### Setting the DSCP value for IGMP protocol packets

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter public network IGMP view or VPN instance IGMP view.</td>
<td>igmp [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Set the DSCP value for IGMP protocol packets.</td>
<td>dscp dscp-value</td>
</tr>
</tbody>
</table>

### Setting the DSCP value for PIM protocol packets

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter public network IGMP view or VPN instance PIM view.</td>
<td>pim [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Set the DSCP value for PIM protocol packets.</td>
<td>dscp dscp-value</td>
</tr>
</tbody>
</table>

### Setting the DSCP value for MLD protocol packets sent by MLD snooping

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter MLD-snooping view.</td>
<td>mld-snooping</td>
</tr>
<tr>
<td>3.</td>
<td>Set the DSCP value for MLD protocol packets transmitted.</td>
<td>dscp dscp-value</td>
</tr>
</tbody>
</table>

### Setting the DSCP value for MLD protocol packets

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter public network MLD view or VPN instance MLD view.</td>
<td>mld [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Set the DSCP value for MLD protocol packets.</td>
<td>dscp dscp-value</td>
</tr>
</tbody>
</table>
### Setting the DSCP value for IPv6 PIM protocol packets

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>pim ipv6 [ vpn-instance vpn-instance-name ]</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 3.   | dscp dscp-value | Optional.  
|      |          | The default value is 48. |

### Setting DSCP values for SSH protocol packets

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 2.   | ssh server dscp dscp-value | Optional.  
|      |          | The default value is 16. |
| 3.   | ssh server ipv6 dscp dscp-value | Optional.  
|      |          | The default value is 0. |
| 4.   | ssh client dscp dscp-value | Optional.  
|      |          | The default value is 16. |
| 5.   | ssh client ipv6 dscp dscp-value | Optional.  
|      |          | The default value is 0. |
| 6.   | sftp client dscp dscp-value | Optional.  
|      |          | The default value is 16. |
| 7.   | sftp client ipv6 dscp dscp-value | Optional.  
|      |          | The default value is 8. |

### Setting the DSCP value for outgoing LDP packets

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>mpls ldp</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>dscp dscp-value</td>
<td>The default value is 48.</td>
</tr>
</tbody>
</table>

### Setting the DSCP value for outgoing RSVP packets
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter MPLS view.</td>
<td>mpls</td>
</tr>
<tr>
<td>3.</td>
<td>Set the DSCP value for outgoing RSVP packets.</td>
<td>mpls rsvp-te dscp dscp-value</td>
</tr>
</tbody>
</table>

**Setting the DSCP value for IPv4 packets sent by the FTP server**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the DSCP value for IPv4 packets sent by the FTP server.</td>
<td>ftp server dscp dscp-value</td>
</tr>
</tbody>
</table>

**Setting the DSCP value for packets sent by the FTP client**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the DSCP value for IPv4 packets sent by the FTP client.</td>
<td>ftp client dscp dscp-value</td>
</tr>
<tr>
<td>3.</td>
<td>Set the DSCP value for IPv6 packets sent by the FTP client.</td>
<td>ftp client ipv6 dscp dscp-value</td>
</tr>
</tbody>
</table>

**Setting the DSCP value for packets sent by the TFTP client**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the DSCP value for IPv4 packets sent by the TFTP client.</td>
<td>tftp client dscp dscp-value</td>
</tr>
<tr>
<td>3.</td>
<td>Set the DSCP value for IPv6 packets sent by the TFTP client.</td>
<td>tftp client ipv6 dscp dscp-value</td>
</tr>
</tbody>
</table>

**Setting the DSCP value for outgoing HTTP packets**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the DSCP value for outgoing IPv4 HTTP packets.</td>
<td>ip http dscp dscp-value</td>
</tr>
</tbody>
</table>
### Setting the DSCP value for packets sent by the Telnet server

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Set the DSCP value for outgoing IPv6 HTTP packets.</td>
<td>ipv6 http dscp dscp-value</td>
</tr>
</tbody>
</table>

Optional.  The default value is 0.

### Setting the DSCP value for packets sent by the Telnet client

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Set the DSCP value for IPv6 packets sent by the Telnet server.</td>
<td>telnet server ipv6 dscp dscp-value</td>
</tr>
</tbody>
</table>

The default value is 0.

### Added commands

dhcp client dscp

**Syntax**

```
dhcp client dscp dscp-value
undo dhcp client dscp
```

**View**

System view

**Default level**

2: System level

**Parameters**

*dscp-value*: DSCP value in the DHCP protocol packets transmitted, in the range of 0 to 63.

**Description**

Use the `dhcp client dscp` command to set the DSCP value for DHCP protocol packets sent by the DHCP client.
Use the `undo dhcp client dscp` command to restore the default.

By default, the DSCP value in DHCP protocol packets sent by the DHCP client is 56.

**Examples**

```
# Set DSCP 30 for DHCP protocol packets sent by the DHCP client.
<Sysname> system-view
<Sysname> dhcp client dscp 30
```

dhcp dscp

**Syntax**

```
dhcp dscp dscp-value
undo dhcp dscp
```

**View**

System view

**Default level**

2: System level

**Parameters**

`dscp-value`: DSCP value in the DHCP protocol packets transmitted, in the range of 0 to 63.

**Description**

Use the `dhcp dscp` command to set the DSCP value for DHCP protocol packets sent by the DHCP server and DHCP relay agent.

Use the `undo dhcp dscp` command to restore the default.

By default, the DSCP value in DHCP protocol packets sent by the DHCP server and DHCP relay agent is 56.

**Examples**

```
# Set DSCP 30 for DHCP protocol packets transmitted.
<Sysname> system-view
<Sysname> dhcp dscp 30
```

dns dscp

**Syntax**

```
dns dscp dscp-value
undo dns dscp
```

**View**

System view

**Default level**

2: System level

**Parameters**

`dscp-value`: DSCP value in the DNS protocol packets transmitted, in the range of 0 to 63.

**Description**

Use the `dns dscp` command to set the DSCP value for DNS protocol packets transmitted.
Use the `undo dns dscp` command to restore the default.

By default, the DSCP value in DNS protocol packets transmitted is 0.

**Examples**

```
# Set DSCP 30 for DNS protocol packets transmitted.
<Sysname> system-view
<Sysname> dns dscp 30
```

dns ipv6 dscp

**Syntax**

```
dns ipv6 dscp dscp-value
undo dns ipv6 dscp
```

**View**

System view

**Default level**

2: System level

**Parameters**

- `dscp-value`: DSCP value in the IPv6 DNS protocol packets transmitted, in the range of 0 to 63.

**Description**

Use the `dns ipv6 dscp` command to set the DSCP value for IPv6 DNS protocol packets transmitted. Use the `undo dns ipv6 dscp` command to restore the default.

By default, the DSCP value in IPv6 DNS protocol packets transmitted is 0.

**Examples**

```
# Set DSCP 30 for IPv6 DNS protocol packets transmitted.
<Sysname> system-view
<Sysname> dns ipv6 dscp 30
```

dscp (IGMP view)

**Syntax**

```
dscp dscp-value
undo dscp
```

**View**

Public network IGMP view, VPN instance IGMP view

**Default level**

2: System level

**Parameters**

- `dscp-value`: DSCP value in the protocol packets, in the range of 0 to 63.

**Description**

Use the `dscp` command to set the DSCP value for IGMP protocol packets. Use the `undo dscp` command to restore the default.
By default, the DSCP value in IGMP protocol packets is 48.

Examples

# Set DSCP 63 for IGMP protocol packets in the public network.
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] dscp 63

# Set DSCP 63 for IGMP protocol packets in the VPN instance named mvpn.
<Sysname> system-view
[Sysname] igmp vpn-instance mvpn
[Sysname-igmp-mvpn] dscp 63

dscp (IGMP-Snooping view)

Syntax

dscp dscp-value
undo dscp

View

IGMP-snooping view

Default level

2: System level

Parameters

dscp-value: DSCP value in the IGMP protocol packets transmitted, in the range of 0 to 63.

Description

Use the dscp command to set the DSCP value for IGMP protocol packets transmitted.
Use the undo dscp command to restore the default.
By default, the DSCP value in IGMP protocol packets transmitted is 48.

Examples

# Set DSCP 63 for IGMP protocol packets transmitted.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] dscp 63

dscp (IPv6 PIM view)

Syntax

dscp dscp-value
undo dscp

View

Public network IPv6 PIM view, VPN instance IPv6 PIM view

Default level

2: System level
Parameters

dscp-value: DSCP value in the protocol packets, in the range of 0 to 63.

Description

Use the dscp command to set the DSCP value for IPv6 PIM protocol packets.
Use the undo dscp command to restore the default.
By default, the DSCP value in IPv6 PIM protocol packets is 48.

Examples

# Set DSCP 63 for IPv6 PIM protocol packets in the public network.
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] dscp 63

# Set DSCP 63 for IPv6 PIM protocol packets in the VPN instance named mvpn.
<Sysname> system-view
[Sysname] pim ipv6 vpn-instance mvpn
[Sysname-pim6-mvpn] dscp 63

dscp (MLD view)

Syntax

dscp dscp-value
undo dscp

View

Public network MLD view, VPN instance MLD view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, in the range of 0 to 63.

Description

Use the dscp command to set the DSCP value for MLD protocol packets.
Use the undo dscp command to restore the default.
By default, the DSCP value in MLD protocol packets is 48.

Examples

# Set DSCP 63 for MLD protocol packets in the public network.
<Sysname> system-view
[Sysname] mld
[Sysname-mld] dscp 63

# Set DSCP 63 for MLD protocol packets in the VPN instance named mvpn.
<Sysname> system-view
[Sysname] mld vpn-instance mvpn
[Sysname-mld-mvpn] dscp 63
dscp (MLD-Snooping view)

Syntax

```
dscp dscp-value
undo dscp
```

View

MLD-snooping view

Default level

2: System level

Parameters

- `dscp-value`: DSCP value in the MLD protocol packets transmitted, in the range of 0 to 63.

Description

Use the `dscp` command to set the DSCP value for MLD protocol packets transmitted. Use the `undo dscp` command to restore the default. By default, the DSCP value in MLD protocol packets transmitted is 48.

Examples

```
# Set DSCP 63 for MLD protocol packets transmitted by MLD-snooping.
<Sysname> system-view
<Sysname> mld-snooping
<Sysname-mld-snooping> dscp 63
```

dscp (MPLS LDP view)

Syntax

```
dscp dscp-value
undo dscp
```

View

MPLS LDP view

Default level

2: System level

Parameters

- `dscp-value`: DSCP value for outgoing LDP packets, in the range of 0 to 63.

Description

Use `dscp` to set the DSCP value for outgoing LDP packets. Use `undo dscp` to restore the default. By default, the DSCP value for outgoing LDP packets is 48.

Examples

```
# Set the DSCP for outgoing LDP packets to 56.
<Sysname> system-view
<Sysname> mpls lsr-id 1.1.1.1
<Sysname-mpls> mpls
```
dscp (OSPF view)

Syntax

dscp dscp-value
undo dscp

View

OSPF view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, in the range of 0 to 63.

Description

Use the dscp command to set the DSCP value for OSPF protocol packets.
Use the undo dscp command to restore the default.
By default, the DSCP value in OSPF protocol packets is 48.

Examples

# Set DSCP 63 for OSPF protocol packets sent by OSPF process 1.
<Sysname> system-view
<Sysname> ospf
<Sysname-ospf-1] dscp 63

dscp (PIM view)

Syntax


dscp dscp-value
undo dscp

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, in the range of 0 to 63.

Description

Use the dscp command to set the DSCP value for PIM protocol packets.
Use the undo dscp command to restore the default.
By default, the DSCP value in PIM protocol packets is 48.

Examples

# Set DSCP 63 for PIM protocol packets in the public network.
dscp (RIP view)

**Syntax**

```
dscp dscp-value
undo dscp
```

**View**

RIP view

**Default level**

2: System level

**Parameters**

- `dscp-value`: DSCP value in the protocol packets, in the range of 0 to 63.

**Description**

Use the `dscp` command to set the DSCP value for RIP protocol packets.

Use the `undo dscp` command to restore the default.

By default, the DSCP value in RIP protocol packets is 48.

**Examples**

```
# Set DSCP 63 for RIP protocol packets sent by RIP process 1.
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1] dscp 63
```

**ftp client dscp**

**Syntax**

```
ftp client dscp dscp-value
undo ftp client dscp
```

**View**

System view

**Default level**

2: System level

**Parameters**

- `dscp-value`: DSCP value, in the range of from 0 to 63.

**Description**

Use the `ftp client dscp` command to set the DSCP value for IPv4 packets sent by the FTP client.
Use the `undo ftp client dscp` command to restore the default.

By default, the DSCP value in IPv4 packets sent by the FTP client is 0.

**Examples**

```
# Set DSCP 30 for IPv4 packets sent by the FTP client.
<Sysname> system-view
[Sysname] ftp client dscp 30
```

**ftp client ipv6 dscp**

**Syntax**

```
ftp client ipv6 dscp dscp-value
undo ftp client ipv6 dscp
```

**View**

System view

**Default level**

2: System level

**Parameters**

`dscp-value`: DSCP value, in the range of 0 to 63.

**Description**

Use the `ftp client ipv6 dscp` command to set the DSCP value for IPv6 packets sent by the IPv6 FTP client.

Use the `undo ftp client ipv6 dscp` command to restore the default.

By default, the DSCP value in IPv6 packets sent by the IPv6 FTP client is 0.

**Examples**

```
# Set DSCP 30 for IPv6 packets sent by the IPv6 FTP client.
<Sysname> system-view
[Sysname] ftp client ipv6 dscp 30
```

**ftp server dscp**

**Syntax**

```
ftp server dscp dscp-value
undo ftp server dscp
```

**View**

System view

**Default level**

2: System level

**Parameters**

`dscp-value`: DSCP value in the protocol packets, in the range of 0 to 63.

**Description**

Use the `ftp server dscp` command to set the DSCP value for IPv4 packets sent by the FTP server.

Use the `undo ftp server dscp` command to restore the default.
By default, the DSCP value in IPv4 packets sent by the FTP server is 0.

Examples

# Set DSCP 30 for IPv4 packets sent by the FTP server.
<Sysname> system-view
[Sysname] ftp server dscp 30

ip http dscp

Syntax

   ip http dscp dscp-value

undo ip http dscp

View

System view

Default level

2: System level

Parameters

  dscp-value: DSCP value, in the range of 0 to 63.

Description

Use the ip http dscp command to set the DSCP value for outgoing IPv4 HTTP packets.
Use the undo ip http dscp command to restore the default.
By default, the DSCP value in outgoing IPv4 HTTP packets is 16.

Examples

  # Set DSCP 30 for outgoing IPv4 HTTP packets.
  <Sysname> system-view
  [Sysname] ip http dscp 30

ipv6 dhcp client dscp

Syntax

   ipv6 dhcp client dscp dscp-value

undo ipv6 dhcp client dscp

View

System view client dscp

Default level

2: System level

Parameters

  dscp-value: DSCP value in the DHCPv6 protocol packets transmitted, in the range of 0 to 63.

Description

Use the ipv6 dhcp client dscp command to set the DSCP value for DHCPv6 protocol packets sent by the DHCPv6 client.
Use the undo ipv6 dhcp client dscp command to restore the default.
By default, the DSCP value in DHCPv6 protocol packets sent by the DHCPv6 client is 56.
Examples

# Set DSCP 30 for DHCPv6 protocol packets sent by the DHCPv6 client.

<Sysname> system-view
[Sysname] ipv6 dhcp client dscp 30

ipv6 dhcp dscp

Syntax

ipv6 dhcp dscp dscp-value
undo ipv6 dhcp dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the DHCPv6 protocol packets transmitted, in the range of 0 to 63.

Description

Use the ipv6 dhcp dscp command to set the DSCP value for DHCPv6 protocol packets sent by the DHCPv6 server and DHCPv6 relay agent.

Use the undo ipv6 dhcp dscp command to restore the default.

By default, the DSCP value in DHCPv6 protocol packets sent by the DHCPv6 server and DHCPv6 relay agent is 56.

Examples

# Set DSCP 30 for the DHCPv6 protocol packets sent by the DHCPv6 server and DHCPv6 relay agent.

<Sysname> system-view
[Sysname] ipv6 dhcp dscp 30

ipv6 http dscp

Syntax

ipv6 http dscp dscp-value
undo ipv6 http dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value, in the range of 0 to 63.

Description

Use the ipv6 http dscp command to set the DSCP value for outgoing IPv6 HTTP packets.

Use the undo ipv6 http dscp command to restore the default.
By default, the DSCP value in outgoing IPv6 HTTP packets is 0.

**Examples**

```
# Set DSCP 30 for outgoing IPv6 HTTP packets.
<Sysname> system-view
[Sysname] ipv6 http dscp 30
```

**mpls rsvp-te dscp**

**Syntax**

```
mpls rsvp-te dscp dscp-value
undo mpls rsvp-te dscp
```

**View**

MPLS view

**Default level**

2: System level

**Parameters**

- `dscp-value`: DSCP value for outgoing RSVP packets, in the range of 0 to 63.

**Description**

Use `mpls rsvp-te dscp` to set the DSCP value for outgoing RSVP packets.

Use `undo mpls rsvp-te dscp` to restore the default.

By default, the DSCP value for outgoing RSVP packets is 48.

**Examples**

```
# Set DSCP 56 for RSVP packets.
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] mpls rsvp-te dscp 56
```

**nqa server tos**

**Syntax**

```
nqa server (tcp-connect | udp-echo) tos tos
undo nqa server (tcp-connect | udp-echo) tos
```

**View**

System view

**Default level**

2: System level

**Parameters**

- `tos`: Type of Service (ToS) field value, in the range of 0 to 255. Starting from 0, every four consecutive ToS values corresponds to a DSCP value, which is used by network devices for packet classification.

**Description**

Use the `nqa server tos` command to set the ToS value for packets sent by the TCP/UDP listening service on the NQA server.
Use the `undo nqa server tos` command to restore the default.

By default, the ToS value in the packets sent by the TCP/UDP listening service on the NQA server is 0.

**Examples**

```shell
# Set ToS 30 for packets sent by the TCP listening service on the NQA server.
<Sysname> system-view
[Sysname] nqa server tcp-connect tos 30
```

**ntp-service dscp**

**Syntax**

```shell
ntp-service dscp dscp-value
undo ntp-service dscp
```

**View**

System view

**Default level**

2: System level

**Parameters**

`dscp-value`: DSCP value in the protocol packets, in the range of 0 to 63.

**Description**

Use the `ntp-service dscp` command to set the DSCP value for NTP protocol packets.

Use the `undo ntp-service dscp` command to restore the default.

By default, the DSCP value in NTP protocol packets is 16.

**Examples**

```shell
# Set DSCP 30 for NTP protocol packets.
<Sysname> system-view
[Sysname] ntp-service dscp 30
```

**peer dscp (BGP/BGP-VPN instance view)**

**Syntax**

```shell
peer { group-name | ip-address } dscp dscp-value
undo peer { group-name | ip-address } dscp
```

**View**

BGP view, BGP VPN instance view

**Default level**

2: System level

**Parameters**

- `group-name`: Peer group name, a string of 1 to 47 characters.
- `ip-address`: IP address of a peer.
- `dscp-value`: DSCP value in the protocol packets, in the range of 0 to 63.
Description

Use the `peer dscp` command to set the DSCP value for BGP protocol packets sent to the specified BGP peer or BGP peer group.

Use the `undo peer dscp` command to cancel the configuration.

By default, the DSCP value in BGP protocol packets is 48.

Make sure that the specified BGP peer or BGP peer group already exists.

Examples

```plaintext
# In BGP view, set the DSCP value 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 63 for BGP protocol packets sent to the BGP peer group named test, which already exists. (You must create VPN instance vpn1 first)
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer test dscp 63
```

peer dscp (IPv6 address family view)

Syntax

```
peer { ipv6-group-name | ipv6-address } dscp dscp-value
undo peer { ipv6-group-name | ipv6-address } dscp
```

View

IPv6 address family view

Default level

2: System level

Parameters

- `%ipv6-group-name`: Peer group name, a string of 1 to 47 characters.
- `%ipv6-address`: IPv6 address of a peer.
- `%dscp-value`: DSCP value in the protocol packets, in the range of 0 to 63.

Description

Use the `peer dscp` command to set the DSCP value for IPv6 BGP protocol packets sent to the specified IPv6 peer or IPv6 peer group.

Use the `undo peer dscp` command to cancel the configuration.

By default, the DSCP value in IPv6 BGP protocol packets is 48.

Make sure that the specified IPv6 peer or IPv6 peer group already exists.

Examples

```plaintext
# Set DSCP 63 for IPv6 BGP protocol packets sent to the EBGP peer group named test.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
```
radius dscp

Syntax

radius dscp  dscp-value
undo radius dscp

View
System view

Default level
2: System level

Parameters

dscp-value: DSCP value in the protocol packets, in the range of 0 to 63.

Description
Use the radius dscp command to set the DSCP value for IPv4 RADIUS protocol packets.
Use the undo radius dscp command to restore the default.
By default, the DSCP value in IPv4 RADIUS protocol packets is 0.

Examples
# Set DSCP 6 for IPv4 RADIUS protocol packets.
<Sysname> system-view
<Sysname> radius dscp 6

radius ipv6 dscp

Syntax

radius ipv6 dscp  dscp-value
undo radius ipv6 dscp

View
System view

Default level
2: System level

Parameters

dscp-value: DSCP value in the protocol packets, in the range of 0 to 63.

Description
Use the radius ipv6 dscp command to set the DSCP value for IPv6 RADIUS protocol packets.
Use the undo radius ipv6 dscp command to restore the default.
By default, the DSCP value in IPv6 RADIUS protocol packets is 0.

Examples
# Set DSCP 6 for IPv6 RADIUS protocol packets.
<Sysname> system-view
<Sysname> radius ipv6 dscp 6
sftp client dscp

Syntax

    sftp client dscp  dscp-value
    undo sftp client dscp

View

    System view

Default level

    2: System level

Parameters

    dscp-value: DSCP value in the protocol packets, in the range of 0 to 63.

Description

    Use the `sftp client dscp` command to set the DSCP value for IPv4 protocol packets sent by the SFTP client.
    
    Use the `undo sftp client dscp` command to restore the default.
    
    By default, the DSCP value in IPv4 protocol packets sent by the SFTP client is 16.

Examples

    # Set DSCP 30 for IPv4 protocol packets sent by the SFTP client.
    <Sysname> system-view
    [Sysname] sftp client dscp 30

sftp client ipv6 dscp

Syntax

    sftp client ipv6 dscp  dscp-value
    undo sftp client ipv6 dscp

View

    System view

Default level

    2: System level

Parameters

    dscp-value: DSCP value in the protocol packets, in the range of 0 to 63.

Description

    Use the `sftp client ipv6 dscp` command to set the DSCP value for IPv6 protocol packets sent by the SFTP client.
    
    Use the `undo sftp client ipv6 dscp` command to restore the default.
    
    By default, the DSCP value in IPv6 protocol packets sent by the SFTP client is 8.

Examples

    # Set DSCP 30 for IPv6 protocol packets sent by the SFTP client.
    <Sysname> system-view
    [Sysname] sftp client ipv6 dscp 30
snmp-agent packet response dscp

Syntax

snmp-agent packet response dscp dscp-value
undo snmp-agent packet response dscp

View

System view

Default level

3: Manage level

Parameters

dscp-value: DSCP value in the SNMP response packets, in the range of 0 to 63.

Description

Use the **snmp-agent packet response dscp** command to set the DSCP value for SNMP response packets.

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

By default, the DSCP value in SNMP response packets is 0.

Examples

# Set DSCP 45 for SNMP response packets.
 SYSNAME> system-view
 [Sysname] snmp-agent packet response dscp 45

ssh client dscp

Syntax

ssh client dscp dscp-value
undo ssh client dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, in the range of 0 to 63.

Description

Use the **ssh client dscp** command to set the DSCP value for IPv4 protocol packets sent by the Stelnet client.

Use the **undo ssh client dscp** command to restore the default.

By default, the DSCP value in IPv4 protocol packets sent by the Stelnet client is 16.

Examples

# Set DSCP 30 for IPv4 protocol packets sent by the Stelnet client.
 SYSNAME> system-view
 [Sysname] ssh client dscp 30
ssh client ipv6 dscp

Syntax

```
ssh client ipv6 dscp dscp-value
undo ssh client ipv6 dscp
```

View

System view

Default level

2: System level

Parameters

```
dscp-value: DSCP value in the protocol packets, in the range of 0 to 63.
```

Description

Use the `ssh client ipv6 dscp` command to set the DSCP value for IPv6 protocol packets sent by the Stelnet client.

Use the `undo ssh client ipv6 dscp` command to restore the default.

By default, the DSCP value in IPv6 protocol packets sent by the Stelnet client is 0.

Examples

```
# Set DSCP 30 for IPv6 protocol packets sent by the Stelnet client.
<Sysname> system-view
[Sysname] ssh client ipv6 dscp 30
```

ssh server dscp

Syntax

```
ssh server dscp dscp-value
undo ssh server dscp
```

View

System view

Default level

2: System level

Parameters

```
dscp-value: DSCP value in the protocol packets, in the range of 0 to 63.
```

Description

Use the `ssh server dscp` command to set the DSCP value for IPv4 protocol packets sent by the SSH server.

Use the `undo ssh server dscp` command to restore the default.

By default, the DSCP value in IPv4 protocol packets sent by the SSH server is 16.

Examples

```
# Set DSCP 30 for IPv4 protocol packets sent by the SSH server.
<Sysname> system-view
[Sysname] ssh server dscp 30
```
ssh server ipv6 dscp

Syntax

ssh server ipv6 dscp dscp-value
undo ssh server ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, in the range of 0 to 63.

Description

Use the ssh server ipv6 dscp command to set the DSCP value for IPv6 protocol packets sent by the SSH server.

Use the undo ssh server ipv6 dscp command to restore the default.

By default, the DSCP value in IPv6 protocol packets sent by the SSH server is 0.

Examples

# Set DSCP 30 for IPv6 protocol packets sent by the SSH server.
<Sysname> system-view
<Sysname> ssh server ipv6 dscp 30

telnet client dscp

Syntax

telnet client dscp dscp-value
undo telnet client dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, in the range of 0 to 63.

Description

Use the telnet client dscp command to set the DSCP value for IPv4 packets sent by the Telnet client.

Use the undo telnet client dscp command to restore the default.

By default, the DSCP value in IPv4 packets sent by the Telnet client is 16.

Examples

# Set DSCP 30 for IPv4 packets sent by the Telnet client.
<Sysname> system-view
<Sysname> telnet client dscp 30
telnet client ipv6 dscp

Syntax

telnet client ipv6 dscp dscp-value
undo telnet client ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value, in the range of 0 to 63.

Description

Use the telnet client ipv6 dscp command to set the DSCP value for IPv6 packets sent by the IPv6 Telnet client.

Use the undo telnet client ipv6 dscp command to restore the default.

By default, the DSCP value in IPv6 packets sent by the IPv6 Telnet client is 0.

Examples

# Set DSCP 0 for IPv6 packets sent by the IPv6 Telnet client.
<Sysname> system-view
[Sysname] telnet client ipv6 dscp 30

telnet server dscp

Syntax

telnet server dscp dscp-value
undo telnet server dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value, in the range of 0 to 63.

Description

Use the telnet server dscp command to set the DSCP value for IPv4 packets sent by the Telnet server.

Use the undo telnet server dscp command to restore the default.

By default, the DSCP value in IPv4 packets sent by the Telnet server is 48.

Examples

# Set DSCP 30 for IPv4 packets sent by the Telnet server.
<Sysname> system-view
[Sysname] telnet server dscp 30
telnet server ipv6 dscp

Syntax

telnet server ipv6 dscp dscp-value
undo telnet server ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value, in the range of 0 to 63.

Description

Use the telnet server ipv6 dscp command to set the DSCP value for IPv6 packets sent by the IPv6 Telnet server.

Use the undo telnet server ipv6 dscp command to restore the default.

By default, the DSCP value in IPv6 packets sent by the IPv6 Telnet server is 0.

Examples

# Set DSCP 30 for IPv6 packets sent by the IPv6 Telnet server.
<Sysname> system-view
<Sysname> telnet server ipv6 dscp 30

tftp client dscp

Syntax

ftp client dscp dscp-value
undo ftp client dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value, in the range of 0 to 63.

Description

Use the tftp client dscp command to set the DSCP value for IPv4 packets sent by the TFTP client.

Use the undo tftp client dscp command to restore the default.

By default, the DSCP value in IPv4 packets sent by the TFTP client is 0.

Examples

# Set DSCP 30 for IPv4 packets sent by the TFTP client.
<Sysname> system-view
<Sysname> tftp client dscp 30
tftp client ipv6 dscp

Syntax

    tftp client ipv6 dscp dscp-value
    undo tftp client ipv6 dscp

View

    System view

Default level

    2: System level

Parameters

    dscp-value: DSCP value, in the range of 0 to 63.

Description

Use the tftp client ipv6 dscp command to set the DSCP value for IPv6 packets sent by the IPv6 TFTP client.

Use the undo tftp client ipv6 dscp command to restore the default.

By default, the DSCP value in IPv6 packets sent by the IPv6 TFTP client is 0.

Examples

    # Set DSCP 30 for IPv6 packets sent by the IPv6 TFTP client.
    <Sysname> system-view
    [Sysname] tftp client ipv6 dscp 30

tos (DHCP operation type view)

Syntax

    tos value
    undo tos

View

    DHCP operation type view

Default level

    2: System level

Parameters

    value: ToS value in the NQA probe packets, in the range of 0 to 255.

Description

Use the tos command to set the ToS value for NQA probe packets.

Use the undo tos command to restore the default.

By default, the ToS value in NQA probe packets is 0.

Examples

    # Set ToS 1 for NQA probe packets.
    <Sysname> system-view
    [Sysname] nqa entry admin test
    [Sysname-nqa-admin-test] type dhcp
    [Sysname-nqa-admin-test-dhcp] tos 1
vrrp dscp

Syntax

vrrp dscp dscp-value
undo vrrp dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value, in the range of 0 to 63.

Description

Use the vrrp dscp command to set the DSCP value for IPv4 VRRP protocol packets.
Use the undo vrrp dscp command to restore the default.
By default, the DSCP value in IPv4 VRRP protocol packets is 48.

Examples

# Set DSCP 30 for IPv4 VRRP protocol packets transmitted.
<Sysname> system-view
[Sysname] vrrp dscp 30

vrrp ipv6 dscp

Syntax

vrrp ipv6 dscp dscp-value
undo vrrp ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value, in the range of 0 to 63.

Description

Use the vrrp ipv6 dscp command to set the DSCP value for IPv6 VRRP protocol packets.
Use the undo vrrp ipv6 dscp command to restore the default.
By default, the DSCP value in IPv6 VRRP protocol packets is 56.

Examples

# Set DSCP 30 for IPv6 VRRP protocol packets transmitted.
<Sysname> system-view
[Sysname] vrrp ipv6 dscp 30
Modified commands

info-center loghost

Old syntax

```plaintext
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

```plaintext
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

Before modification: The `dscp dscp-value` option is not available.

After modification: The `dscp dscp-value` option is available. The DSCP value ranges from 0 to 63 and defaults to 0. You can use this option to set the DSCP value for packet sent to the log host.

ping ipv6

Old syntax

```plaintext
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

```plaintext
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

Before modification: The `-tos tos` option is not available.

After modification: The `-tos tos` option is available. The ToS value ranges from 0 to 255 and defaults to 0. You can use this option to set the ToS value for ICMPv6 echo requests.

snmp-agent target-host

Old syntax

```plaintext
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

```plaintext
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 ]
```
**Change description**

Before modification: The **dscp dscp-value** option is not available.

After modification: The **dscp dscp-value** option is available. The DSCP value ranges from 0 to 63 and defaults to 0. You can use this option to set the DSCP value for SNMP trap packets.

**tracert**

**Old syntax**

```
tracert [ -a source-ip | -f first-ttl | -m max-ttl | -p port | -q packet-number | -vpn-instance vpn-instance-name | -w timeout ] * host
```

**New syntax**

```
tracert [ -a source-ip | -f first-ttl | -m max-ttl | -p port | -q packet-number | -vpn-instance vpn-instance-name | -w timeout | -tos tos ] * host
```

**New feature: 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 12.

**Figure 12 Determining the ISP domain of a user by the username**

![Figure 12 Determining the ISP domain of a user by the username](image)

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."

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>Enter ISP domain view.</td>
<td><code>domain isp-name</code></td>
<td>N/A</td>
</tr>
<tr>
<td>Set a DSCP value for the ISP domain.</td>
<td><code>dscp dscp-value</code></td>
<td>Optional. By default, no DSCP is specified for an ISP domain.</td>
</tr>
</tbody>
</table>

**Command reference**

**dscp (ISP domain view)**

Use `dscp` to set a DSCP value for an ISP domain.

Use `undo dscp` to restore the default.

**Syntax**

```
dscp dscp-value
undo dscp
```

**Default**

No DSCP value is specified for an ISP domain.

**Views**

ISP domain view
Default command level

2: System level

Parameters

dscp-value: Specifies a DSCP value, in the range of 0 to 63.

Usage guidelines

The device sets the specified DSCP value in IP packets from authenticated users in that domain.

Examples

# Set DSCP 6 for ISP domain aaa.
<Sysname> system-view
[Sysname] domain aaa
[Sysname-isp-aaa] dscp 6

display domain

Use display domain to display the configuration of ISP domains.

Syntax

display domain [isp-name] [ | {begin | exclude | include} regular-expression]

Views

Any view

Default command level

1: Monitor level

Parameters

isp-name: Name of an existing ISP domain, a string of 1 to 24 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 ISP domain, the command displays the configuration of all ISP domains.

Examples

# Display the configuration of all ISP domains.
<Sysname> display domain
0  Domain : system
   State :  Active
   Access-limit :  Disabled
   Accounting method :  Required
   Default authentication scheme :  local
   Default authorization scheme :  local
   Default accounting scheme :  local
   DSCP :  63
   Domain User Template:
Idle-cut : Disabled
Self-service : Disabled
Authorization attributes :

1 Domain : test
State : Active
Access-limit : Disabled
Accounting method : Required
Default authentication scheme : local
Default authorization scheme : local
Default accounting scheme : local
DSCP : 63
Lan-access authentication scheme : radius:test, local
Lan-access authorization scheme : hwtacacs:hw, local
Lan-access accounting scheme : local

Domain User Template:
Idle-cut : Disabled
Self-service : Disabled
Authorization attributes :
User-profile : profile1

Default Domain Name: system
Total 2 domain(s).

Table 13 Command output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>ISP domain name.</td>
</tr>
<tr>
<td>State</td>
<td>Status of the ISP domain: active or blocked. Users in an active ISP domain can request network services, and users in a blocked ISP domain cannot.</td>
</tr>
<tr>
<td>Access-limit</td>
<td>Limit on the number of user connections. If there is no limit on the number, this field displays Disabled.</td>
</tr>
<tr>
<td>Accounting method</td>
<td>Indicates whether accounting is required. If accounting is required, when no accounting server is available or when communication with the accounting server fails, user connections are torn down. Otherwise, users can continue to use network services.</td>
</tr>
<tr>
<td>Default authentication scheme</td>
<td>Default authentication method.</td>
</tr>
<tr>
<td>Default authorization scheme</td>
<td>Default authorization method.</td>
</tr>
<tr>
<td>Default accounting scheme</td>
<td>Default accounting method.</td>
</tr>
<tr>
<td>DSCP</td>
<td>DSCP value in IP packets from authenticated users in the ISP domain.</td>
</tr>
<tr>
<td>Lan-access authentication scheme</td>
<td>Authentication method for LAN users.</td>
</tr>
<tr>
<td>Lan-access authorization scheme</td>
<td>Authorization method for LAN users.</td>
</tr>
<tr>
<td>Lan-access accounting scheme</td>
<td>Accounting method for LAN users.</td>
</tr>
<tr>
<td>Domain User Template</td>
<td>Indicates some functions and attributes set for users in the domain.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Idle-cut</td>
<td>Indicates whether the idle cut function is enabled. With the idle cut</td>
</tr>
<tr>
<td></td>
<td>function enabled for a domain, the system logs out any user in the domain</td>
</tr>
<tr>
<td></td>
<td>whose traffic is less than the specified minimum traffic during the idle</td>
</tr>
<tr>
<td></td>
<td>timeout period.</td>
</tr>
<tr>
<td>Self-service</td>
<td>Indicates whether the self-service function is enabled. With the self-</td>
</tr>
<tr>
<td></td>
<td>service function enabled, users can launch a browser and enter the self-</td>
</tr>
<tr>
<td></td>
<td>service URL in the address bar to access the self-service pages and perform</td>
</tr>
<tr>
<td></td>
<td>self-service operations.</td>
</tr>
<tr>
<td>Authorization</td>
<td>Default authorization attributes for the ISP domain.</td>
</tr>
<tr>
<td>User-profile</td>
<td>Default authorization user profile.</td>
</tr>
</tbody>
</table>

**New feature: Delaying the MAC authentication**

When both 802.1X authentication and MAC authentication are enabled on a port, you can delay the MAC authentication, so that 802.1X authentication is preferentially triggered. Configure the function as needed according to the network conditions.

**Configuring the MAC authentication delay**

To configure the MAC authentication delay:

1. Enter system view.
   ```
   system-view
   ```
   Remarks: N/A

2. Enter Layer 2 Ethernet interface view.
   ```
   interface interface-type interface-number
   ```
   Remarks: N/A

3. Configure the MAC authentication delay.
   ```
   mac-authentication timer auth-delay time
   ```
   Remarks: By default, MAC authentication is not delayed.

**Command reference**

mac-authentication timer auth-delay

**Syntax**

```
mac-authentication timer auth-delay time
undo mac-authentication timer auth-delay
```

**Views**

Layer 2 Ethernet port view

**Default command level**

2: System level

**Parameters**

`time`: Specifies the MAC authentication delay, in the range of 1 to 180 seconds.

**Description**

Use `mac-authentication timer auth-delay` to configure the MAC authentication delay.

Use `undo mac-authentication timer auth-delay` to restore the default.
By default, MAC authentication is not delayed.

**Examples**

```
# Set the MAC authentication delay to 30 seconds on port GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication timer auth-delay 30
```

**Modified feature: tunnel bandwidth**

**Feature change description**

The value range for the `bandwidth-value` argument changes.

**Command changes**

Modified command: tunnel bandwidth

**Syntax**

```
tunnel bandwidth bandwidth-value
```

**Views**

- Tunnel interface view

**Change description**

Before modification: The `bandwidth-value` argument ranges from 1 to 10000000.

After modification: The `bandwidth-value` argument ranges from 1 to 40000000.

**Modified feature: Establishing a connection to an SCP server to transfer files with the server**

**Feature change description**

Changed the string length for the `server` argument.

**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 { 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 } ] *
```

**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 the maximum number of routes in a VPN instance

Feature change description
The maximum number of routes in a VPN instance changed.

Command changes
Modified command: routing-table limit
Syntax
    routing-table limit number { warn-threshold | simply-alert }
Views
    VPN instance view, IPv4 VPN view, IPv6 VPN view
Change description
Before modification: The number argument ranges from 1 to 6144 in VPN instance view, from 1 to 12288 in IPv4 VPN view, and from 1 to 6144 in IPv6 VPN view.
After modification: The number argument ranges from 1 to 8192 in VPN instance view, from 1 to 16384 in IPv4 VPN view, and from 1 to 8192 in IPv6 VPN view.

Modified feature: Configuring PBR to support next hops in VPN instances

Feature change description
In the previous releases, the next hop specified in a policy must be in the public network. From this release, you can specify next hops in the MPLS L3VPN for a policy.

Command changes
Modified command: apply ip-address default next-hop
Old syntax
    apply ip-address default next-hop ip-address [ track track-entry-number ] [ ip-address [ track track-entry-number ] ]
New syntax
    apply ip-address default next-hop [ vpn-instance vpn-instance-name ] ip-address [ track track-entry-number ] [ ip-address [ track track-entry-number ] ]
Views
  Policy node view

Change description
  Before modification: The \texttt{vpn-instance vpn-instance-name} option is not supported, and the default next hop must be in a public network.

  After modification: The \texttt{vpn-instance vpn-instance-name} option is supported, and you can specify the MPLS L3VPN that the default next hop belongs to.

Modified command: apply ip-address next-hop

Old syntax
  \begin{verbatim}
  apply ip-address next-hop ip-address [ direct ] [ track track-entry-number ] [ ip-address [ direct ] [ track track-entry-number ] ]
  \end{verbatim}

New syntax
  \begin{verbatim}
  apply ip-address next-hop [ vpn-instance vpn-instance-name ] ip-address [ direct ] [ track track-entry-number ] [ ip-address [ direct ] [ track track-entry-number ] ]
  \end{verbatim}

Views
  Policy node view

Change description
  Before modification: The \texttt{vpn-instance vpn-instance-name} option is not supported, and the next hop must be in a public network.

  After modification: The \texttt{vpn-instance vpn-instance-name} option is supported, and you can specify the MPLS L3VPN that the next hop belongs to.

Modified feature: Commands related to password

Feature change description
  The arguments and argument descriptions related to security were standardized. Therefore, the commands that contain the \texttt{key} or \texttt{password} keyword were changed. For secrecy, all passwords, including passwords configured in plain text, are saved in cipher text.

Command changes

Modified command: area-authentication-mode

Old syntax
  \begin{verbatim}
  area-authentication-mode \{ md5 \{ simple \} password [ ip | \texttt{osi} ]
  \end{verbatim}

New syntax
  \begin{verbatim}
  area-authentication-mode \{ md5 \{ simple \} [ cipher ] password [ ip | \texttt{osi} ]
  \end{verbatim}

Views
  IS-IS view

Change description
  Before modification:
  \begin{itemize}
  \item For MD5 authentication, a ciphertext password must comprise 24 characters.
  \end{itemize}
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
```

**View**

DHCP address pool view

**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

**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

**Change description**

Before modification: If `cipher` is specified, you can set 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: cluster-snmp-agent usm-user v3

Old syntax

```text
cluster-snmp-agent usm-user v3 user-name group-name [ authentication-mode { md5 | sha } auth-password [ privacy-mode des56 priv-password ]]
```

New syntax

```text
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

Change description

Before modification: The `cipher` and `simple` keywords are not supported. You can directly enter a plaintext password of 1 to 16 characters or a ciphertext password of 24 characters.

After modification: You can use the `cipher` keyword to set a ciphertext password of 1 to 53 characters or use the `simple` keyword to set a plaintext password of 1 to 16 characters. If neither `cipher` nor `simple` is specified, you set a plaintext password.

Modified command: cwmp acs password

Old syntax

```text
cwmp acs password passwd
```

New syntax

```text
cwmp acs password [ cipher | simple ] passwd
```

View

CWMP view

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. If neither `cipher` nor `simple` is specified, you set a plaintext password string.

Modified command: cwmp cpe password

Old syntax

```text
cwmp cpe password passwd
```

New syntax

```text
cwmp cpe password [ cipher | simple ] passwd
```

View

CWMP view

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. If neither `cipher` nor `simple` is specified, you set a plaintext password string.
Modified command: dldp authentication-mode

Old syntax

dldp authentication-mode { md5 md5-password | none | simple simple-password }

New syntax

dldp authentication-mode { none | { md5 | simple } password }

View

System view

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

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

Change description

Before modification: If cipher is specified, you can set a plaintext password of 1 to 16 characters, or a ciphertext password of 24 characters.

After modification: If cipher is specified, you must enter a ciphertext password of 1 to 53 characters.
Modified command: isis authentication-mode

**Old syntax**

isis authentication-mode \{ md5 | simple \} \textit{password} \[ level-1 | level-2 \] \[ ip | osi \]

**New syntax**

isis authentication-mode \{ md5 | simple \} \{ cipher \} \textit{password} \[ level-1 | level-2 \] \[ ip | osi \]

**Views**

Interface view

**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 \texttt{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 \} \textit{key}

**Views**

HWTACACS scheme view

**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 \} \textit{key}

**Views**

RADIUS scheme view

**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

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

View

MPLS LDP view, MPLS LDP VPN instance view

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

View

Interface view

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

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

**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

**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

**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

Change description
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

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

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

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 53 characters.
Modified command: primary accounting (RADIUS scheme view)

Syntax

```plaintext
primary accounting { ipv4-address | ipv6 ipv6-address } [ port-number | key [ cipher | simple ] key [ vpn-instance vpn-instance-name ] ] *
```

Views

RADIUS scheme view

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

```plaintext
primary authentication { ipv4-address | ipv6 ipv6-address } [ port-number | key [ cipher | simple ] key [ vpn-instance vpn-instance-name ] ] *
```

Views

RADIUS scheme view

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

```plaintext
radius-server client-ip ip-address [ key string ]
```

New syntax

```plaintext
radius-server client-ip ip-address [ key [ cipher | simple ] string ]
```

Views

System view

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

```plaintext
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

**Change description**

Before modification:
- For MD5 authentication, a ciphertext password comprises 1 to 24 characters.
- For simple authentication, you can only 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

**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

**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

```plaintext
sa string-key { inbound | outbound } { ah | esp } string-key
```

New syntax

```plaintext
sa string-key { inbound | outbound } { ah | esp } [ cipher | simple ] string-key
```

Views

IPsec policy view

**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

```plaintext
secondary accounting { ipv4-address | ipv6 ipv6-address } [ port-number | key [ cipher | simple ]
key | vpn-instance vpn-instance-name ] *
```

Views

RADIUS scheme view

**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

```plaintext
secondary authentication { ipv4-address | ipv6 ipv6-address } [ port-number | key [ cipher | simple ]
key | vpn-instance vpn-instance-name ] *
```

Views

RADIUS scheme view

**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

```plaintext
set authentication password { cipher | simple } password
```

Views

User interface view
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

```
```

Views

OSPF area view

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 community

Old syntax

```
snmp-agent community { read | write } community-name [ mib-view view-name ] [ acl acl-number | acl ipv6 ipv6-acl-number ] *
```

New syntax

```
snmp-agent community { read | write } [ cipher ] community-name [ mib-view view-name ] [ acl acl-number | acl ipv6 ipv6-acl-number ] *
```

Views

System view

Change description

Before modification: You can only set a plaintext community name.

After modification: You can set either a plaintext or ciphertext community name of 1 to 73 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

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 Encrypted authentication key length requirements for the ciphertext authentication key length requirements.

**Table 14 Encrypted authentication key length requirements**

<table>
<thead>
<tr>
<th>Authentication algorithm</th>
<th>Hexadecimal string</th>
<th>Non-hexadecimal string</th>
</tr>
</thead>
<tbody>
<tr>
<td>MD5</td>
<td>32 characters</td>
<td>53 characters</td>
</tr>
<tr>
<td>SHA</td>
<td>40 characters</td>
<td>57 characters</td>
</tr>
</tbody>
</table>

- See Encrypted privacy key length requirements for the ciphertext privacy key length requirements.

**Table 15 Encrypted privacy key length requirements**

<table>
<thead>
<tr>
<th>Authentication algorithm</th>
<th>Encryption algorithm</th>
<th>Hexadecimal string</th>
<th>Non-hexadecimal string</th>
</tr>
</thead>
<tbody>
<tr>
<td>MD5</td>
<td>3DES</td>
<td>64 characters</td>
<td>73 characters</td>
</tr>
<tr>
<td>MD5</td>
<td>AES128 or DES-56</td>
<td>32 characters</td>
<td>53 characters</td>
</tr>
<tr>
<td>SHA</td>
<td>3DES</td>
<td>80 characters</td>
<td>73 characters</td>
</tr>
<tr>
<td>SHA</td>
<td>AES128 or DES-56</td>
<td>40 characters</td>
<td>53 characters</td>
</tr>
</tbody>
</table>

Modified command: super password

Syntax

```
super password [ level user-level ] { cipher | simple } password
```

Views

System view

Change description

Before modification: If cipher is specified, you can enter a plaintext password of 1 to 16 characters or a ciphertext password of 24 characters.
After modification: If cipher is specified, you must enter 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

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

View

Interface view

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

View

Interface view

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: Setting the IRF link down report delay

Feature change description

The value range and default value for the *interval* argument (IRF link down report delay time) were changed.

Command changes

Modified command: `irf link-delay`

Syntax

```
irf link-delay interval
```

Views

System view

Change description

Before modification: The *interval* argument ranges from 200 to 2000 in milliseconds. By default, the IRF ports immediately report the link down events.

After modification: The *interval* argument ranges from 0 to 30000 in milliseconds. By default, the delay for the IRF ports to report a link down event is 4 seconds.
This release has the following changes:

- New feature: M6VPE
- New feature: Disabling the USB port

### New feature: M6VPE

**Configuring M6VPE**

For more information about configuring M6VPE, see "Configuring multicast VPN" in *HP 5820X & 5800 IP Multicast Configuration Guide-F1805*.

### Command reference

None

### New feature: Disabling the USB port

A HP 5820X & 5800 switch has one USB port, through which you can upload and download files. By default, the USB port is enabled. You can use the following command to disable it as needed.

**Configuring the Disabling the USB port**

To configure the Disabling the USB port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Disabling the USB port</td>
<td>usb disable</td>
<td>By default, the USB port on a device are enabled.</td>
</tr>
</tbody>
</table>

### Command reference

**usb disable**

**Syntax**

- `usb disable`
- `undo usb disable`

**View**

System view

**Default level**

3: Manage level
Parameters

None

Description

Use the **usb disable** command to disable the USB port on the device.
Use the **undo usb disable** command to enable the USB port on the device.
By default, the USB port on a device are enabled.

Examples

```
# Disable the USB port on the device.
<Sysname> system-view
<Sysname> usb disable
```

**Removed feature: Setting the password display mode for all local users**

Feature change description

Removed commands

**local-user password-display-mode**

**Syntax**

```
local-user password-display-mode { auto | cipher-force }
undo local-user password-display-mode
```

**View**

System view
This release has the following changes:

- New feature: Displaying information about the patch package
- New feature: Displaying alarm information
- New feature: Configuring LDP NSR
- New feature: Configuring protection switching
- New feature: Configuring byte-count or packet-based WFQ queuing
- New feature: Configuring SP+WFQ queuing
- New feature: Configuring the service type as SCP for SSH users
- New feature: Configuring the device as an SCP client
- New feature: Enabling SSL client weak authentication
- New feature: Configuring a user validity check rule
- New feature: SAVI
- New feature: Blacklist
- New feature: Configuring BFD to detect the indirect next hop of a static route
- New feature: Enabling OSPF ISPF
- New feature: Assigning a high priority to IS-IS routes
- New feature: Configuring IPv6 IS-IS MTR
- New feature: Enabling 4-byte AS number suppression
- New feature: Setting the maximum number of IGMP snooping & MLD snooping forwarding entries
- New feature: Enabling the IGMP snooping & MLD snooping host tracking function
- New feature: PIM snooping & IPv6 PIM snooping
- New feature: Setting the maximum number of forwarding entries for multicast VLANs
- New feature: Setting the maximum number of forwarding entries for IPv6 multicast VLANs
- New feature: Enabling multicast optimization
- New feature: Enabling the IGMP & MLD host tracking function
- New feature: Configuring a password for MD5 authentication used by both MSDP peers to establish a TCP connection
- New feature: BGP MDT
- New feature: Configuring IPv6 multicast routing and forwarding in a VPN instance
- New feature: IPv6 PIM support for VPNs
- New feature: SNMP support for IPv6 ACLs
- New feature: SNMP PIM traps
- New feature: Configuring the source IP address of sFlow packets
- New feature: Bulk interface configuration
- New feature: Configuring a Layer 3 aggregation group
- New feature: Configuring the MTU of a Layer 3 aggregate interface
- New feature: Assigning a port an aggregation priority
- New feature: Configuring MPLS labels as the load sharing criteria for a link aggregation group
- New feature: Setting the guest attribute for a user group
• New feature: Setting the validity time of a local user
• New feature: Specifying the local user as a guest or guest manager
• New feature: Authorizing a local user to use the Web service
• New feature: Configuring status detection for RADIUS authentication/authorization servers
• New feature: Specifying the VPN for the source IPv6 address of outgoing RADIUS packets
• New feature: Specifying the VPN for the IPv6 address of a RADIUS server
• New feature: Configuring 802.1X critical VLAN
• New feature: Specifying supported domain name delimiters
• New feature: Configuring an 802.1X VLAN group
• New feature: Configuring a MAC authentication critical VLAN
• New feature: Enabling inactivity aging
• New feature: Enabling the dynamic secure MAC function
• New feature: PVST
• New feature: Configuring an MTU for a VLAN interface
• New feature: Enabling LLDP to automatically discover IP phones
• New feature: PoE power negotiation through Power Via MDI TLV (supported only on PoE-capable switches)
• New feature: Configuring the VF tracking function to monitor an AVF
• New feature: Enabling client offline detection
• New feature: Configuring DHCP snooping support for sub-option 9 in Option 82
• New feature: Specifying the source interface for DNS packets
• New feature: Configuring TCP path MTU discovery
• New feature: Configuring the interface as an uplink interface and disabling it from learning ND snooping entries
• New feature: Specifying the AFTR address
• New feature: Enabling GRE keepalive and setting the keepalive parameters
• New feature: Enabling dropping of IPv6 packets using IPv4-compatible IPv6 addresses
• Modified feature: Configuring the password for switching from the current user privilege level to a higher one
• Modified feature: Displaying files and folders
• Modified feature: Activating/stopping/deleting/confirming patches
• Modified feature: Loading/installing and running patches
• Modified feature: LACP MAD
• Modified feature: Configuring the maximum number of routes for the VPN instance
• Modified feature: Configuring SVC MPLS L2VPN
• Modified feature: Specifying a community list name to match BGP VPNv4 routing information
• Modified feature: Configuring traffic policing
• Modified feature: Configuring aggregate CAR
• Modified feature: Configuring hierarchical CAR
• Modified feature: Configuring the idle cut function
• Modified feature: Setting the quiet timer for RADIUS servers
• Modified feature: Configuring IP source guard
• Modified feature: Configuring the ABR to advertise a default route to the stub area
• Modified feature: Setting BGP SoO extended community attribute for BGP routing information
• Modified feature: RIPng IPsec command
• Modified feature: OSPFv3 IPsec command
• Modified feature: Setting the register suppression time for PIM/IPv6 PIM
• Modified feature: Setting the maximum delay for sending a hello message in PIM/IPv6 PIM
• Modified feature: Displaying MBGP&IPv6 MBGP routing information matching the specified BGP community list
• Modified feature: Support of voice VLAN for 128 OUI addresses
• Modified feature: Configuring the protected VLANs for the RRPP domain
• Modified feature: Configuring the protected VLANs for a smart link group
• Modified feature: Enabling ND snooping
• Modified feature: Displaying IPv6 information for an interface
• Modified feature: Displaying IPv6 information for tunnel interfaces
• Modified feature: Displaying socket information for a specified task

New feature: Displaying information about the patch package

Displaying information about the patch package

For more information about displaying information about the patch package configuration, see “Software Upgrade Configuration” in Fundamentals Configuration Guide of HP 5820X & 5800 Fundamentals Configuration Guide-F1805.

Command reference

New command: display patch

For more information about this command, see “Software Upgrade commands” in Fundamentals Command Reference of HP 5820X & 5800 Fundamentals Command Reference-F1805.

New feature: Displaying alarm information

Displaying alarm information


Command reference

New command: display alarm

For more information about this command, see “Device Management commands” in Fundamentals Command Reference of HP 5820X & 5800 Fundamentals Command Reference-F1805.
New feature: Configuring LDP NSR

Configuring LDP NSR

For more information about LDP NSR configuration, see "Configuring basic MPLS" in HP 5820X & 5800 MPLS Configuration Guide-F1805.

Command reference

New command: **non-stop-routing**.

For more information about LDP NSR configuration commands, see "Basic MPLS commands" in HP 5820X & 5800 MPLS Command Reference-F1805.

New feature: Configuring protection switching

Configuring protection switching

For more information about protection switching configuration, see "Configuring MPLS TE" in HP 5820X & 5800 MPLS Configuration Guide-F1805.

Command reference

New commands:

- `display mpls te protection tunnel`
- `mpls te protection switch-mode`
- `mpls te protection tunnel`
- `mpls te protect-switch`.

For more information about protection switching configuration commands, see "MPLS TE configuration commands" in HP 5820X & 5800 MPLS Command Reference-F1805.

New feature: Configuring byte-count or packet-based WFQ queuing

Configuring byte-count or packet-based WFQ queuing

For more information about byte-count or packet-based WFQ queuing configuration, see "Configuring congestion management" in HP 5820X & 5800 ACL and QoS Configuration Guide-F1805.

Command reference

Modified command: Keywords **byte-count** and **weight** were added to the **qos wfq** command.

For more information about byte-count or packet-based WFQ queuing configuration commands, see "Congestion management commands" in HP 5820X & 5800 ACL and QoS Command Reference-F1805.
New feature: Configuring SP+WFQ queuing

Configuring SP+WFQ queuing

For more information about SP+WFQ queuing configuration, see "Configuring congestion management" in HP 5820X & 5800 ACL and QoS Configuration Guide-F1805.

Command reference

New commands: qos wfq byte-count and qos wfq group sp.

For more information about SP+WFQ queuing configuration commands, see "Congestion management commands" in HP 5820X & 5800 ACL and QoS Command Reference-F1805.

New feature: Configuring the service type as SCP for SSH users

Configuring the service type as SCP for SSH users

For more information about configuring the service type as SCP for SSH users, see "Configuring SSH" in HP 5820X & 5800 Security Configuration Guide-F1805.

Command reference

The scp keyword was added to the ssh user command.

For more information about this command, see "SSH configuration commands" in HP 5820X & 5800 Security Command Reference-F1805.

New feature: Configuring the device as an SCP client

Configuring the device as an SCP client

For more information about configuring the device as an SCP client, see "Configuring SSH" in HP 5820X & 5800 Security Configuration Guide-F1805.

Command reference

New commands: scp

For more information about this command, see "SSH configuration commands" in HP 5820X & 5800 Security Command Reference-F1805.

New feature: Enabling SSL client weak authentication

Enabling SSL client weak authentication

For more information about enabling SSL client weak authentication, see "Configuring SSL" in HP 5820X & 5800 Security Configuration Guide-F1805.
Command reference

New commands: **client-verify weaken**
For more information about this command, see "SSL configuration commands" in *HP 5820X & 5800 Security Command Reference-F1805.*

**New feature: Configuring a user validity check rule**

Configuring a user validity check rule

For more information about configuring a user validity check rule, see "Configuring ARP attack protection" in *HP 5820X & 5800 Security Configuration Guide-F1805.*

Command reference

New commands: **arp detection**
For more information about this command, see "ARP attack protection configuration commands" in *HP 5820X & 5800 Security Command Reference-F1805.*

**New feature: SAVI**

Configuring SAVI

For more information about configuring SAVI, see *HP 5820X & 5800 Security Configuration Guide-F1805.*

Command reference

For more information about SAVI configuration commands, see *HP 5820X & 5800 Security Command Reference-F1805.*

**New feature: Blacklist**

Configuring blacklist

For more information about configuring blacklist, see *HP 5820X & 5800 Security Configuration Guide-F1805.*

Command reference

For more information about blacklist configuration commands, see *HP 5820X & 5800 Security Command Reference-F1805.*
New feature: Configuring BFD to detect the indirect next hop of a static route

Configuring BFD to detect the indirect next hop of a static route

For more information about this feature, see "Configuring static routing" in HP 5820X & 5800 Layer 3—IP Routing Configuration Guide-F1805.

Command reference

Modified command: Option bfd control-packet [ bfd-source ip-address ] was added to the ip route-static command. This option can be selected only when only a next hop is specified.

For more information about this command, see "Static routing configuration commands" in HP 5820X & 5800 Layer 3—IP Routing Command Reference-F1805.

New feature: Enabling OSPF ISPF

Enabling OSPF ISPF

For more information about this feature, see "Configuring OSPF" in HP 5820X & 5800 Layer 3—IP Routing Configuration Guide-F1805.

Command reference

New command: ispf enable.

For more information about this command, see "OSPF configuration commands" in HP 5820X & 5800 Layer 3—IP Routing Command Reference-F1805.

New feature: Assigning a high priority to IS-IS routes

Assigning a high priority to IS-IS routes

For more information about this feature, see "Configuring IS-IS" in HP 5820X & 5800 Layer 3—IP Routing Configuration Guide-F1805.

Command reference

New command: priority high.

For more information about this command, see "IS-IS configuration commands" in HP 5820X & 5800 Layer 3—IP Routing Command Reference-F1805.

New feature: Configuring IPv6 IS-IS MTR

Configuring IPv6 IS-IS MTR

For more information about this feature, see "Configuring IPv6 IS-IS" in HP 5820X & 5800 Layer 3—IP Routing Configuration Guide-F1805.
Command reference

New command: **multiple-topology ipv6-unicast**.
For more information about this command, see "IPv6 IS-IS configuration commands" in *HP 5820X & 5800 Layer 3—IP Routing Command Reference-F1805*.

**New feature: Enabling 4-byte AS number suppression**

Enabling 4-byte AS number suppression

For more information about this feature, see "Configuring IPv6 BGP" and "Configuring IPv6 BGP" in *HP 5820X & 5800 Layer 3—IP Routing Configuration Guide-F1805*.

Command reference

New command: **peer capability-advertise suppress-4-byte-as**
For more information about this command, see "BGP configuration commands" and "IPv6 BGP configuration commands" in *HP 5820X & 5800 Layer 3—IP Routing Command Reference-F1805*.

**New feature: Setting the maximum number of IGMP snooping & MLD snooping forwarding entries**

Setting the maximum number of IGMP snooping & MLD snooping forwarding entries

For more information about setting the maximum number of IGMP snooping forwarding entries and setting the maximum number of MLD snooping forwarding entries, see "Configuring IGMP snooping" and "Configuring MLD snooping" in *HP 5820X & 5800 IP Multicast Configuration Guide-F1805*.

Command reference

New commands: **entry-limit** (IGMP-Snooping view) and **entry-limit** (MLD-Snooping view).
For more information about these commands, see "IGMP snooping configuration commands" and "MLD snooping configuration commands" in *HP 5820X & 5800 IP Multicast Command Reference-F1805*.

**New feature: Enabling the IGMP snooping & MLD snooping host tracking function**

Enabling the IGMP snooping & MLD snooping host tracking function

For more information about enabling the IGMP snooping host tracking function and enabling the MLD snooping host tracking function, see "Configuring IGMP snooping" and "Configuring MLD snooping" in *HP 5820X & 5800 IP Multicast Configuration Guide-F1805*.
Command reference

New commands:

- display igmp-snooping host
- host-tracking (IGMP-Snooping view)
- igmp-snooping host-tracking
- display mld-snooping host
- host-tracking (MLD-Snooping view)
- mld-snooping host-tracking

For more information about the new commands, see "IGMP snooping configuration commands" and "MLD snooping configuration commands" in HP 5820X & 5800 IP Multicast Command Reference-F1805.

New feature: PIM snooping & IPv6 PIM snooping

Configuring PIM snooping & IPv6 PIM snooping

For more information about configuring PIM snooping and configuring PIM snooping, see HP 5820X & 5800 IP Multicast Configuration Guide-F1805.

Command reference

For more information about PIM snooping configuration commands and IPv6 PIM snooping configuration commands, see HP 5820X & 5800 IP Multicast Command Reference-F1805.

New feature: Setting the maximum number of forwarding entries for multicast VLANs

Setting the maximum number of forwarding entries in a multicast VLAN

For more information about setting the maximum number of forwarding entries for multicast VLANs, see "Configuring multicast VLANs" in HP 5820X & 5800 IP Multicast Configuration Guide-F1805.

Command reference

New command: multicast-vlan entry-limit.

For more information about this command, see "Multicast VLAN configuration commands" in HP 5820X & 5800 IP Multicast Command Reference-F1805.
New feature: Setting the maximum number of forwarding entries for IPv6 multicast VLANs

Setting the maximum number of forwarding entries for IPv6 multicast VLANs

For more information about setting the maximum number of forwarding entries for IPv6 multicast VLANs, see "Configuring IPv6 multicast VLANs" in HP 5820X & 5800 IP Multicast Configuration Guide-F1805.

Command reference

New command: `multicast-vlan ipv6 entry-limit`.
For more information about this command, see "IPv6 multicast VLAN configuration commands" in HP 5820X & 5800 IP Multicast Command Reference-F1805.

New feature: Enabling multicast optimization

Enabling multicast optimization

For more information about enabling multicast optimization, see "Configuring multicast routing and forwarding" in HP 5820X & 5800 IP Multicast Configuration Guide-F1805.

Command reference

New command: `multicast-optimization enable`.
For more information about this command, see "Multicast routing and forwarding configuration commands" in HP 5820X & 5800 IP Multicast Command Reference-F1805.

New feature: Enabling the IGMP & MLD host tracking function

Enabling the IGMP & MLD host tracking function

For more information about enabling the IGMP host tracking function and enabling the MLD host tracking function, see "Configuring IGMP" and "Configuring MLD" in HP 5820X & 5800 IP Multicast Configuration Guide-F1805.

Command reference

New commands:
- `display igmp host interface`
- `display igmp host port-info`
- `display igmp ssm-mapping host interface`
- `host-tracking` (IGMP view)
- `igmp host-tracking`
• display mld host interface
• display mld host port-info
• display mld ssm-mapping host interface
• host-tracking (MLD view)
• mld host-tracking

For more information about these commands, see "IGMP configuration commands" and "MLD configuration commands" in HP 5820X & 5800 IP Multicast Command Reference-F1805.

New feature: Configuring a password for MD5 authentication used by both MSDP peers to establish a TCP connection

Configuring a password for MD5 authentication used by both MSDP peers to establish a TCP connection

For more information about configuring a password for MD5 authentication used by both MSDP peers to establish a TCP connection, see "Configuring MSDP" in HP 5820X & 5800 IP Multicast Configuration Guide-F1805.

Command reference

New command: peer password.

For more information about this command, see "MSDP configuration commands" in HP 5820X & 5800 IP Multicast Command Reference-F1805.

New feature: BGP MDT

Configuring BGP MDT

For more information about configuring BGP MDT, see "Configuring multicast VPN" in HP 5820X & 5800 IP Multicast Configuration Guide-F1805.

Command reference

For more information about configuring BGP MDT commands, see "Multicast VPN configuration commands" in HP 5820X & 5800 IP Multicast Command Reference-F1805.

New feature: Configuring IPv6 multicast routing and forwarding in a VPN instance

Configuring IPv6 multicast routing and forwarding in a VPN instance

For more information about configuring IPv6 multicast routing and forwarding in a VPN instance, see "Configuring IPv6 multicast routing and forwarding" in HP 5820X & 5800 IP Multicast Configuration Guide-F1805.
Command reference

For more information about configuring IPv6 multicast routing and forwarding in a VPN instance commands, see "IPv6 multicast routing and forwarding configuration commands" in HP 5820X & 5800 IP Multicast Command Reference-F1805.

New feature: IPv6 PIM support for VPNs

Configuring IPv6 PIM in a VPN instance

For more information about configuring IPv6 PIM in a VPN instance, see "Configuring IPv6 PIM" in HP 5820X & 5800 IP Multicast Configuration Guide-F1805.

Command reference

For more information about configuring MLD in a VPN instance commands, see "IPv6 PIM configuration commands" in HP 5820X & 5800 IP Multicast Command Reference-F1805.

New feature: SNMP support for IPv6 ACLs

Using IPv6 ACLs with SNMP

IPv6 ACLs can be used in SNMP to control access to the SNMP agent by IPv6 address. For more information, see "Configuring SNMP" in HP 5820X & 5800 Network Management and Monitoring Configuration Guide-F1805.

Command reference

Option acl ipv6 ipv6-acl-number was added to the following commands:

- snmp-agent community
- snmp-agent group
- snmp-agent usm-user { v1 | v2c }
- snmp-agent usm-user v3

For more information, see "SNMP configuration commands" in HP 5820X & 5800 Network Management and Monitoring Command Reference-F1805.

New feature: SNMP PIM traps

Enabling SNMP PIM traps globally

Support for PIM traps was added to SNMP. For more information about enabling SNMP PIM traps globally, see "Configuring SNMP" in HP 5820X & 5800 Network Management and Monitoring Configuration Guide-F1805.

Command reference

Keyword pim was added to the snmp-agent trap enable command.
New feature: Configuring the source IP address of sFlow packets

Configuring the source IP address of sFlow packets

For more information about configuring the source IP address of sFlow packets, see "Configuring sFlow" in HP 5820X & 5800 Network Management and Monitoring Configuration Guide-F1805.

Command reference

New command: `sflow source`

For more information about configuring the source IP address of sFlow packets commands, see "sFlow configuration commands" in HP 5820X & 5800 Network Management and Monitoring Command Reference-F1805.

New feature: Bulk interface configuration

Bulk interface configuration

For more information about bulk interface configuration, see HP 5820X & 5800 Layer 2—LAN Switching Configuration Guide-F1805.

Command reference

For more information about bulk interface configuration commands, see HP 5820X & 5800 Layer 2—LAN Switching Command Reference-F1805.

New feature: Configuring a Layer 3 aggregation group

Configuring a Layer 3 aggregation group

For more information about configuring a Layer 3 aggregation group, see "Configuring Ethernet link aggregation" in HP 5820X & 5800 Layer 2—LAN Switching Configuration Guide-F1805.

Command reference

New command: `interface route-aggregation`.

Modified commands: Keyword `route-aggregation` was added to the following commands:

- `display interface`
- `display link-aggregation load-sharing mode`
- `display link-aggregation verbose`
- `reset counters interface`

For more information about the commands, see "Ethernet link aggregation configuration commands" in HP 5820X & 5800 Layer 2—LAN Switching Command Reference-F1805.
New feature: Configuring the MTU of a Layer 3 aggregate interface

Configuring the MTU of a Layer 3 aggregate interface

For more information about configuring the MTU of a Layer 3 aggregate interface, see "Configuring Ethernet link aggregation" in *HP 5820X & 5800 Layer 2—LAN Switching Configuration Guide-F1805*.

Command reference

For more information about the command for configuring the MTU of a Layer 3 aggregate interface, see "Ethernet link aggregation configuration commands" in *HP 5820X & 5800 Layer 2—LAN Switching Command Reference-F1805*.

New feature: Assigning a port an aggregation priority

Assigning a port an aggregation priority

For more information about assigning a port an aggregation priority, see "Configuring Ethernet link aggregation" in *HP 5820X & 5800 Layer 2—LAN Switching Configuration Guide-F1805*.

Command reference

Added command: `link-aggregation port-priority` (which applies to both dynamic and static aggregation groups).

Deleted command: `lacp port-priority` (which applies to only dynamic aggregation groups).

For more information about this command, see "Ethernet link aggregation configuration commands" in *HP 5820X & 5800 Layer 2—LAN Switching Command Reference-F1805*.

New feature: Configuring MPLS labels as the load sharing criteria for a link aggregation group

Configuring MPLS labels as the load sharing criteria for a link aggregation group

For more information about configuring MPLS labels as the load sharing criteria for a link aggregation group, see "Configuring Ethernet link aggregation" in *HP 5820X & 5800 Layer 2—LAN Switching Configuration Guide-F1805*.

Command reference

Modified command: The `mpls-label1` and `mpls-label2` keywords were added to the `link-aggregation load-sharing mode` command in aggregate interface view.

For more information about this command, see "Ethernet link aggregation configuration commands" in *HP 5820X & 5800 Layer 2—LAN Switching Command Reference-F1805*.
New feature: Setting the guest attribute for a user group

Setting the guest attribute for a user group

For more information about setting the guest attribute for a user group, see "Configuring AAA" in HP 5820X & 5800 Security Configuration Guide-F1805.

Command reference

New command: group-attribute allow-guest.
For more information about this command, see "AAA configuration commands" in HP 5820X & 5800 Security Command Reference-F1805.

New feature: Setting the validity time of a local user

Setting the validity time of a local user

For more information about setting the validity time of a local user, see "Configuring AAA" in HP 5820X & 5800 Security Configuration Guide-F1805.

Command reference

New command: validity-date.
For more information about this command, see "AAA configuration commands" in HP 5820X & 5800 Security Command Reference-F1805.

New feature: Specifying the local user as a guest or guest manager

Specifying the local user as a guest or guest manager

For more information about specifying the local user as a guest or guest manager, see "Configuring AAA" in HP 5820X & 5800 Security Configuration Guide-F1805.

Command reference

Keywords user-role-guest and user-role guest-manager are added to the authorization-attribute (local user view/user group view) command.
For more information about this command, see "AAA configuration commands" in HP 5820X & 5800 Security Command Reference-F1805.
New feature: Authorizing a local user to use the Web service

Authorizing a local user to use the Web service

For more information about authorizing a local user to use the Web service, see "Configuring AAA" in HP 5820X & 5800 Security Configuration Guide-F1805.

Command reference

The **web** keyword is added to the **service-type** command.

The **service-type web** keyword is added to **display local-user** and **undo local-user** commands.

For more information about the commands, see "AAA configuration commands" in HP 5820X & 5800 Security Command Reference-F1805.

New feature: Configuring status detection for RADIUS authentication/authorization servers

Configuring status detection for RADIUS authentication/authorization servers

For more information about configuring status detection for RADIUS authentication/authorization servers, see "Configuring AAA" in HP 5820X & 5800 Security Configuration Guide-F1805.

Command reference

The **probe username name [ interval interval ]** option is added to **primary authentication** (RADIUS scheme view) and **secondary authentication** (RADIUS scheme view) commands.

For more information about the commands, see "AAA configuration commands" in HP 5820X & 5800 Security Command Reference-F1805.

New feature: Specifying the VPN for the source IPv6 address of outgoing RADIUS packets

Specifying the VPN for the source IPv6 address of outgoing RADIUS packets

For more information about specifying the VPN for the source IPv6 address of outgoing RADIUS packets, see "Configuring AAA" in HP 5820X & 5800 Security Configuration Guide-F1805.

Command reference

The **vpn-instance** option is added to the **radius nas-ip** command and supported by the **ipv6** parameter.

For more information about this command, see "AAA configuration commands" in HP 5820X & 5800 Security Command Reference-F1805.
New feature: Specifying the VPN for the IPv6 address of a RADIUS server

Specifying the VPN for the IPv6 address of a RADIUS server

For more information about specifying the VPN for the IPv6 address of a RADIUS server, see "Configuring AAA" in HP 5820X & 5800 Security Configuration Guide-F1805.

Command reference

The `vpn-instance` option is added to and supported by the `ipv6` parameter in the following commands:

- primary accounting (RADIUS scheme view)
- primary authentication (RADIUS scheme view)
- secondary accounting (RADIUS scheme view)
- secondary authentication (RADIUS scheme view)

For more information about the commands, see "AAA configuration commands" in HP 5820X & 5800 Security Command Reference-F1805.

New feature: Configuring 802.1X critical VLAN

Configuring 802.1X critical VLAN

For more information about 802.1X critical VLAN configuration, see "Configuring 802.1X" in HP 5820X & 5800 Security Configuration Guide-F1805.

Command reference

New commands: `dot1x critical vlan`, `dot1x critical recovery-action reinitialize`.

For more information about the commands, see "802.1X commands" in HP 5820X & 5800 Security Command Reference-F1805.

New feature: Specifying supported domain name delimiters

Specifying supported domain name delimiters

For more information about specifying supported domain name delimiters configuration, see "Configuring 802.1X" in HP 5820X & 5800 Security Configuration Guide-F1805.

Command reference

For more information about specifying supported domain name delimiters configuration commands, see "802.1X commands" in HP 5820X & 5800 Security Command Reference-F1805.
New feature: Configuring an 802.1X VLAN group

Configuring an 802.1X VLAN group

For more information about 802.1X VLAN group configuration, see "Configuring 802.1X" in *HP 5820X & 5800 Security Configuration Guide-F1805*.

Command reference

New commands: **vlan-group** and **vlan-list**.
For more information about the commands, see "802.1X commands" in *HP 5820X & 5800 Security Command Reference-F1805*.

New feature: Configuring a MAC authentication critical VLAN

Configuring a MAC authentication critical VLAN

For more information about MAC authentication critical VLAN configuration, see "Configuring MAC authentication" in *HP 5820X & 5800 Security Configuration Guide-F1805*.

Command reference

For more information about MAC authentication critical VLAN configuration commands, see "MAC authentication configuration commands" in *HP 5820X & 5800 Security Command Reference-F1805*.

New feature: Enabling inactivity aging

Enabling inactivity aging

For more information about enabling inactivity aging configuration, see "Configuring port security" in *HP 5820X & 5800 Security Configuration Guide-F1805*.

Command reference

New command: **port-security mac-address aging-type inactivity**.
For more information about this command, see "Port security configuration commands" in *HP 5820X & 5800 Security Command Reference-F1805*.

New feature: Enabling the dynamic secure MAC function

Enabling the dynamic secure MAC function

For more information about the enabling the dynamic secure MAC function configuration, see "Configuring port security" in *HP 5820X & 5800 Security Configuration Guide-F1805*. 
Command reference

New command: \texttt{port-security mac-address dynamic}.
For more information about this command, see "Port security configuration commands" in \textit{HP 5820X & 5800 Security Command Reference-F1805}.

New feature: PVST

Configuring PVST

For more information about PVST configuration, see "Configuring spanning tree protocols" in \textit{HP 5820X & 5800 Layer 2—LAN Switching Configuration Guide-F1805}.

Command reference

Modified commands:

- Keyword \texttt{pvst} was added to the \texttt{stp mode} command.
- Option \texttt{vlan vlan-list} was added to the following commands:
  - \texttt{display stp}
  - \texttt{display stp history}
  - \texttt{display stp tc}
  - \texttt{stp bridge-diameter}
  - \texttt{stp cost}
  - \texttt{stp enable} (in system view)
  - \texttt{stp port priority}
  - \texttt{stp port-log}
  - \texttt{stp priority}
  - \texttt{stp root primary}
  - \texttt{stp root secondary}
  - \texttt{stp timer forward-delay}
  - \texttt{stp timer hello}
  - \texttt{stp timer max-age}

For more information about PVST configuration commands, see "Spanning tree configuration commands" in \textit{HP 5820X & 5800 Layer 2—LAN Switching Command Reference-F1805}.

New feature: Configuring an MTU for a VLAN interface

Configuring an MTU for a VLAN interface

For more information about setting an MTU for a VLAN interface, see "Configuring VLANs" in \textit{HP 5820X & 5800 Layer 2—LAN Switching Configuration Guide-F1805}.

Command reference

New command: \texttt{mtu}.
New feature: Enabling LLDP to automatically discover IP phones

Enabling LLDP to automatically discover IP phones

For more information about enabling LLDP to automatically discover IP phones, see "Configuring LLDP" in HP 5820X & 5800 Layer 2—LAN Switching Configuration Guide-F1805.

Command reference

New command: voice vlan track lldp.

For more information about this command, see "LLDP configuration commands" in HP 5820X & 5800 Layer 2—LAN Switching Command Reference-F1805.

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 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.

For more information about PoE, see "Configuring PoE" in HP 5820X & 5800 Network Management and Monitoring Configuration Guide-F1805.

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.)
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 16 Command output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power type</td>
<td>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.</td>
</tr>
<tr>
<td>Power source</td>
<td>Power supply type of a PSE when the device supports PoE:</td>
</tr>
<tr>
<td></td>
<td>• Unknown—Unknown power supply.</td>
</tr>
<tr>
<td></td>
<td>• Primary—Primary power supply.</td>
</tr>
<tr>
<td></td>
<td>• Backup—Backup power supply.</td>
</tr>
<tr>
<td>Power priority</td>
<td>Power supply priority on a PSE when the device supports PoE:</td>
</tr>
<tr>
<td></td>
<td>• Unknown—Unknown priority.</td>
</tr>
<tr>
<td></td>
<td>• Critical—Priority 1.</td>
</tr>
<tr>
<td></td>
<td>• High—Priority 2.</td>
</tr>
<tr>
<td></td>
<td>• Low—Priority 3.</td>
</tr>
<tr>
<td>PD requested power value</td>
<td>Power (in watts) required by the PD that connects to the port. This field appears only on the devices that support PoE.</td>
</tr>
<tr>
<td>PSE allocated power value</td>
<td>Power (in watts) supplied by the PSE to the connecting port. This field appears only on the devices that support PoE.</td>
</tr>
</tbody>
</table>

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 17 Command output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power type</td>
<td>This field appears only on the devices that support PoE. PD type of an LLDP neighboring device which is a PD device:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type 1 PD</strong>—This type power from 0 to 15.4 W, a voltage from 44 to 57 V, and a maximum current of 350 mA.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type 2 PD</strong>—This type requires power from 0 to 30 W, a voltage from 50 to 57 V, and a maximum current of 600 mA.</td>
</tr>
<tr>
<td>Power source</td>
<td>This field appears only on the devices that support PoE. Power source type of an LLDP neighboring device which is a PD device:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unknown</strong>—Unknown power supply.</td>
</tr>
<tr>
<td></td>
<td>• <strong>PSE</strong>—PSE power supply.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Local</strong>—Local power supply.</td>
</tr>
<tr>
<td></td>
<td>• <strong>PSE and local</strong>—PSE and local power supply.</td>
</tr>
<tr>
<td>Power priority</td>
<td>This field appears only on the devices that support PoE. Powered priority of ports on an LLDP neighboring device which is a PD device:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unknown</strong>—Unknown priority.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Critical</strong>—Priority 1.</td>
</tr>
<tr>
<td></td>
<td>• <strong>High</strong>—Priority 2.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Low</strong>—Priority 3.</td>
</tr>
<tr>
<td>PD requested power value</td>
<td>This field appears only on the devices that support PoE. Power (in watts) requested by the LLDP neighboring device which is a PD device.</td>
</tr>
<tr>
<td>PSE allocated power value</td>
<td>This field appears only on the devices that support PoE. Power (in watts) supplied by the PSE to the LLDP neighboring device which is a PD device.</td>
</tr>
</tbody>
</table>

New feature: Configuring the VF tracking function to monitor an AVF

Configuring the VF tracking function to monitor an AVF

For more information about configuring the VF tracking function to monitor an AVF, see "Configuring VRRP" in HP 5820X & 5800 High Availability Configuration Guide-F1805.

Command reference

Modified commands:
• Option **forwarder-switchover member-ip ip-address** was added to the **vrrp vrid track** command.
• Option **forwarder-switchover member-ip ipv6-address** was added to the **vrrp ipv6 vrid track** command.

For more information about these commands, see "VRRP configuration commands" in *HP 5820X & 5800 High Availability Command Reference-F1805*.

**New feature: Enabling client offline detection**

Enabling client offline detection

For more information about enabling client offline detection, see "Configuring the DHCP server" in *HP 5820X & 5800 Layer 3—IP Services Configuration Guide-F1805*.

**Command reference**

New command: **dhcp server client-detect enable**.

For more information about this command, see "DHCP server configuration commands" in *HP 5820X & 5800 Layer 3—IP Services Command Reference-F1805*.

**New feature: Configuring DHCP snooping support for sub-option 9 in Option 82**

Configuring DHCP snooping support for sub-option 9 in Option 82

For more information about configuring DHCP snooping support for sub-option 9 in Option 82, see "Configuring DHCP snooping" in *HP 5820X & 5800 Layer 3—IP Services Configuration Guide-F1805*.

**Command reference**

New command: **dhcp-snooping information sub-option**.

Modified commands:

• Option **private** and keyword **standard** were added to the **dhcp-snooping information format command**.

• **Keyword append was added to the dhcp-snooping information strategy command**.

For more information about these commands, see "DHCP snooping configuration commands" in *HP 5820X & 5800 Layer 3—IP Services Command Reference-F1805*.

**New feature: Specifying the source interface for DNS packets**

Specifying the source interface for DNS packets

For more information about specifying the source interface for DNS packets, see "Configuring IPv4 DNS" in *HP 5820X & 5800 Layer 3—IP Services Configuration Guide-F1805*. 
Command reference

New command: `dns source-interface`.
For more information about this command, see "IPv4 DNS configuration commands" in HP 5820X & 5800 Layer 3—IP Services Command Reference-F1805.

New feature: Configuring TCP path MTU discovery

Configuring TCP path MTU discovery
For more information about configuring TCP path MTU discovery, see "Configuring IP performance optimization" in HP 5820X & 5800 Layer 3—IP Services Configuration Guide-F1805.

Command reference

New command: `tcp path-mtu-discovery`.
For more information about this command, see "IP performance optimization configuration commands" in HP 5820X & 5800 Layer 3—IP Services Command Reference-F1805.

New feature: Configuring the interface as an uplink interface and disabling it from learning ND snooping entries

Configuring the interface as an uplink interface and disabling it from learning ND snooping entries
For more information about configuring the interface as an uplink interface and disabling it from learning ND snooping entries, see "Configuring IPv6 basics" in HP 5820X & 5800 Layer 3—IP Services Configuration Guide-F1805.

Command reference

New command: `ipv6 nd snooping uplink`.
For more information about this command, see "IPv6 basics configuration commands" in HP 5820X & 5800 Layer 3—IP Services Command Reference-F1805.

New feature: Specifying the AFTR address

Specifying the AFTR address
For more information about specifying the AFTR address, see "Configuring DHCPv6 server" in HP 5820X & 5800 Layer 3—IP Services Configuration Guide-F1805.

Command reference

New command: `ds-lite address`.
New feature: Enabling GRE keepalive and setting the keepalive parameters

Enabling GRE keepalive and setting the keepalive parameters

For more information about enabling GRE keepalive and setting the keepalive parameters, see "Configuring GRE" in HP 5820X & 5800 Layer 3—IP Services Configuration Guide-F1805.

Command reference

New command: `keepalive`.

For more information about this command, see "GRE configuration commands" in HP 5820X & 5800 Layer 3—IP Services Command Reference-F1805.

New feature: Enabling dropping of IPv6 packets using IPv4-compatible IPv6 addresses

Enabling dropping of IPv6 packets using IPv4-compatible IPv6 addresses

For more information about enabling dropping of IPv6 packets using IPv4-compatible IPv6 addresses, see "Configuring tunneling" in HP 5820X & 5800 Layer 3—IP Services Configuration Guide-F1805.

Command reference

New command: `tunnel discard ipv4-compatible-packet`

For more information about this command, see "Tunneling configuration commands" in HP 5820X & 5800 Layer 3—IP Services Command Reference-F1805.

Modified feature: Configuring the password for switching from the current user privilege level to a higher one

Feature change description

A password configured by the `super password` command for user privilege level switching can now be hashed.
Command changes

Modified command: super password

Old syntax

    super password [ level user-level ] { cipher | simple } password

New syntax

    super password [ level user-level ] [ hash ] { cipher | simple } password

Views

    System view

Change description

    Before modification: A local password for user privilege level switching cannot be hashed when configured.
    After modification: A local password for user privilege level switching can be hashed when configured.

Modified feature: Displaying files and folders

Feature change description

    The dir command now can display files and folders in the root directories of all storage media on the switch.

Command changes

Modified command: dir

Old syntax

    dir [ /all ] [ file-url ]

New syntax

    dir [ /all ] [ file-url ] /all-filesystems

Views

    User view

Change description

    Before modification: The dir command can display only a specific file or all files and folders in the current directory.
    After modification: With the newly-added /all-filesystems option, the dir command displays files and folders in the root directories of all storage media on the device.
Modified feature: Activating/stopping/deleting/confirming patches

Feature change description

The following commands can now activate, stop, delete, or confirm all patches in the patch memory area:

- patch active
- patch deactive
- patch delete
- patch run

Command changes

Modified command: patch active

Old syntax

patch active patch-number slot slot-number

New syntax

patch active [ patch-number ] slot slot-number

Views

System view

Change description

Before modification: The patch-number argument is required and the command activates patches whose numbers are equal to or smaller than the specified number.

After modification: The patch-number argument is optional. Without this argument, the command activates all patches in the patch memory area.

Modified command: patch deactive

Old syntax

patch deactive patch-number slot slot-number

New syntax

patch deactive [ patch-number ] slot slot-number

Views

System view

Change description

Before modification: The patch-number argument is required and the command stops running patches whose numbers are equal to or greater than the specified number.

After modification: The patch-number argument is optional. Without this argument, the command stops all running patches in the patch memory area.
Modified command: patch delete

Old syntax

```
patch delete patch-number slot slot-number
```

New syntax

```
patch delete [ patch-number ] slot slot-number
```

Views

System view

Change description

Before modification: The `patch-number` argument is required and the command deletes patches whose numbers are equal to or greater than the specified number.

After modification: The `patch-number` argument is optional. Without this argument, the command deletes all patches in the patch memory area.

Modified command: patch run

Old syntax

```
patch run patch-number [ slot slot-number ]
```

New syntax

```
patch run [ patch-number ] [ slot slot-number ]
```

Views

System view

Change description

Before modification: The `patch-number` argument is required and the command confirms active patches whose numbers are equal to or smaller than the specified number.

After modification: The `patch-number` argument is optional. Without this argument, the command confirms all active patches in the patch memory area.

Modified feature: Loading/installing and running patches

Feature change description

The following commands can now load or install and run the patches in a patch package file:

- `patch load`
- `patch install`

Command changes

Modified command: patch install

Old syntax

```
patch install patch-location
```
New syntax

```
patch install { patch-location | file filename }
```

**Views**

System view

**Change description**

Before modification: The command can only be used to install patches in a specific patch file location.

After modification: With the newly-added `file filename` option, the command installs the patches in a patch package file.

**Modified command:** patch load

**Old syntax**

```
patch load slot slot-number
```

**New syntax**

```
patch load slot slot-number [ file filename ]
```

**Views**

System view

**Change description**

Before modification: The command can only be used to load patches in a specific patch file location.

After modification: With the newly-added `file filename` option, the command loads the patches in a patch package file.

**Modified feature: LACP MAD**

**Feature change description**

LACP MAD can be configured on Layer 3 aggregate interfaces.

**Command changes**

**Modified command:** mad enable

**Syntax**

```
mad enable
```

**Views**

Layer 2 aggregate interface view, Layer 3 aggregate interface view

**Change description**

Before modification: This command is only available in Layer 2 aggregate interface view.

After modification: This command is available in both Layer 2 and Layer 3 aggregate interface views.
Modified feature: Configuring the maximum number of routes for the VPN instance

Feature change description

The maximum number of routes in VPN view changed, and configuration of maximum number of routes in IPv4 VPN view was supported.

Command changes

Modified command: routing-table limit

Syntax

```
routing-table limit number { warn-threshold | simply-alert }
```

Views

VPN instance view, IPv4 VPN view, IPv6 VPN view

Change description

Before modification:

- The `routing-table limit` command can be executed in VPN instance view and IPv6 VPN view.
- The `number` argument ranges from 1 to 12288 in VPN instance view and ranges from 1 to 8192 in IPv6 VPN view.

After modification:

- The `routing-table limit` command can be executed in VPN instance view, IPv4 VPN view, and IPv6 VPN view.
- The `number` argument ranges from 1 to 8192 in VPN instance view, ranges from 1 to 16384 in IPv4 VPN view, and ranges from 1 to 8192 in IPv6 VPN view.

Modified feature: Configuring SVC MPLS L2VPN

Feature change description

Ethernet and VLAN were added to the PW encapsulation types for SVC MPLS L2VPN on a Layer 3 interface.

Command changes

Modified command: mpls l2vc

Old syntax

```
mpls l2vc destination vcid [ tunnel-policy tunnel-policy-name ]
```

New syntax

```
mpls l2vc destination vcid [ { ethernet | vlan } | [ tunnel-policy tunnel-policy-name ] ] *
```

Views

Interface view
Change description

Before modification: The **ethernet** and **vlan** keywords are not supported.

After modification: The **ethernet** and **vlan** keywords are available to specify the PW encapsulation type as Ethernet or VLAN.

**Modified feature: Specifying a community list name to match BGP VPNv4 routing information**

Feature change description

The command that displays BGP VPNv4 routing information changed. The **comm-list-name** argument was added.

Command changes

**Modified command: display bgp vpnv4 all routing-table**

**Old syntax**

```
```

**New syntax**

```
display bgp vpnv4 all routing-table [ [ network-address [ { mask | mask-length } [ longer-prefixes ] ] ] | as-path-acl [ as-path-acl-number ] | cidr | community [ aa:nn ] &<1-13> | no-advertise | no-export | no-export-subconfed ] * [ whole-match ] | community-list { { basic-community-list-number | comm-list-name } | adv-community-list-number } | different-origin-as | peer ip-address { advertised-routes | received-routes } [ statistic ] | statistic ] [ | { begin | exclude | include } regular-expression ] | regular-expression as-regular-expression ]
```

Views

Any view

**Change description**

Before modification:
- The **comm-list-name** argument is not supported.
- The **basic-community-list-number** or **adv-community-list-number** argument can be entered up to 16 times.

After modification:
- The **comm-list-name** argument is supported.
- The **basic-community-list-number**, **comm-list-name** or **adv-community-list-number** argument can be entered only once.
Modified command: display bgp vpnv4 route-distinguisher routing-table

Old syntax

display bgp vpnv4 route-distinguisher route-distinguisher routing-table [[ network-address [ mask | mask-length ] | as-path-acl as-path-acl-number | cidr | community [ aa:nn ]&<1-13> | no-advertise | no-export | no-export-subconfed ] * [ whole-match ] | community-list { basic-community-list-number | whole-match } | adv-community-list-number }&<1-16> | different-origin-as ] [ | [ begin | exclude | include } regular-expression ] | regular-expression as-regular-expression ]

New syntax

display bgp vpnv4 route-distinguisher route-distinguisher routing-table [[ network-address | mask | mask-length ] | as-path-acl as-path-acl-number | cidr | community [ aa:nn ]&<1-13> | no-advertise | no-export | no-export-subconfed ] * [ whole-match ] | community-list { basic-community-list-number | whole-match } | adv-community-list-number }&<1-16> | different-origin-as ] [ | [ begin | exclude | include } regular-expression ] | regular-expression as-regular-expression ]

Views

Any view

Change description

Before modification:

• The comm-list-name argument is not supported.
• The basic-community-list-number or adv-community-list-number argument can be entered up to 16 times.

After modification:

• The comm-list-name argument is supported.
• The basic-community-list-number, comm-list-name or adv-community-list-number argument can be entered only once.

Modified command: display bgp vpnv4 vpn-instance routing-table

Old syntax


New syntax

Views

Any view

Change description

Before modification:

- The \texttt{comm-list-name} argument is not supported.
- The \texttt{basic-community-list-number} or \texttt{adv-community-list-number} argument can be entered up to 16 times.

After modification:

- The \texttt{comm-list-name} argument is supported.
- The \texttt{basic-community-list-number}, \texttt{comm-list-name} or \texttt{adv-community-list-number} argument can be entered only once.

Modified feature: Configuring traffic policing

Feature change description

The value ranges for the CBS and EBS were modified for a traffic policing action.

Command changes

Modified command: \texttt{car}

Syntax

\begin{verbatim}
\texttt{car cir committed-information-rate [ cbs committed-burst-size [ ebs excess-burst-size ] ] [ pir peak-information-rate ] [ green action ] [ yellow action ] [ red action ] [ hierarchy-car hierarchy-car-name [ mode \{ and | or \} ] ]}
\end{verbatim}

Views

Traffic behavior view

Change description

Before modification:

- If you do not specify the \texttt{cbs} keyword, the CBS is \(62.5 \times \text{committed-information-rate}\) by default and cannot exceed 16000000.
- If you specify the \texttt{cbs} keyword, the CBS ranges from 512 to 16000000.
- The \texttt{excess-burst-size} argument ranges from 0 to 16000000.

After modification:

- If you do not specify the \texttt{cbs} keyword, the CBS is \(62.5 \times \text{committed-information-rate}\) by default and cannot exceed 256000000.
- If you specify the \texttt{cbs} keyword, the CBS ranges from 512 to 256000000.
- The \texttt{excess-burst-size} argument ranges from 0 to 256000000.
Modified feature: Configuring aggregate CAR

Feature change description

The value ranges for the CBS and EBS were modified for an aggregate CAR action. The actions to take on green packets and yellow packets are supported.

Command changes

Modified command: qos car aggregative

Old syntax

qos car car-name aggregative cir committed-information-rate [ cbs committed-burst-size [ ebs excess-burst-size ] ] [ pir peak-information-rate ] [ red action ]

New syntax

qos car car-name aggregative cir committed-information-rate [ cbs committed-burst-size [ ebs excess-burst-size ] ] [ pir peak-information-rate ] [ green action ] [ yellow action ] [ red action ]

Views

System view

Change description

Before modification:

- If you do not specify the cbs keyword, the CBS is $62.5 \times committed-information-rate$ by default and cannot not exceed 16000000.
- If you specify the cbs keyword, the CBS ranges from 512 to 16000000.
- The excess-burst-size argument ranges from 0 to 16000000.
- The green and yellow keywords are not supported.

After modification:

- If you do not specify the cbs keyword, the CBS is $62.5 \times committed-information-rate$ by default and cannot not exceed 256000000.
- If you specify the cbs keyword, the CBS ranges from 512 to 256000000.
- The excess-burst-size argument ranges from 0 to 256000000.
- The green and yellow keywords are supported.

Modified feature: Configuring hierarchical CAR

Feature change description

The value ranges for the CBS and EBS were modified for a hierarchical CAR action.

Command changes

Modified command: qos car aggregative

Syntax

qos car car-name hierarchy cir committed-information-rate [ cbs committed-burst-size ]
Views
  System view
Change description
  Before modification: The committed-burst-size (CBS) ranges from 4096 to 16000000 and defaults to 4096.
  After modification:
  • If you do not specify the cbs keyword, the CBS is \(62.5 \times \text{committed-information-rate}\) by default and cannot exceed 256000000.
  • If you specify the cbs keyword, the CBS ranges from 512 to 256000000.

Modified feature: Configuring the idle cut function

Feature change description
  The value range of the idle timeout period is changed.

Command changes
Modified command: idle-cut enable

Syntax
  idle-cut enable minute [ flow ]

Views
  ISP domain view
Change description
  The previous value range of the minute argument is from 1 to 120, in minutes.
  The current value range of the minute argument is from 1 to 600, in minutes.

Modified feature: Setting the quiet timer for RADIUS servers

Feature change description
  The value range of the server quiet period is changed.

Command changes
Modified command: timer quiet

Syntax
  timer quiet minutes

Views
  RADIUS scheme view
Change description

The previous value range of the minutes argument is from 1 to 255, in minutes.
The current value range of the minutes argument is from 0 to 255, in minutes.

Modified feature: Configuring IP source guard

Feature change description

• Changed the commands for displaying IP source guard binding entries.
• Changed the commands for configuring static IPv4/IPv6 source guard binding entries.
• Changed the commands for enabling the IPv4/IPv6 source guard function.
• Changed the commands for setting the maximum number of IPv4/IPv6 source guard binding entries.
• Removed the commands for configuring the exceptional ports for the global static IP source guard binding entries.

Command changes

Modified command: display ip source binding

Old syntax

display ip check source [ interface interface-type interface-number | ip-address ip-address | mac-address mac-address ] [ slot slot-number ] [ { begin | exclude | include } regular-expression ]

New syntax

display ip source binding [ static ] [ interface interface-type interface-number | ip-address ip-address | mac-address mac-address ] [ slot slot-number ] [ { begin | exclude | include } regular-expression ]

Views

Any view

Change description

Before modification: display ip check source
After modification: display ip source binding

Modified command: display ipv6 source binding

Old syntax

display ip check source ipv6 [ interface interface-type interface-number | ip-address ip-address | mac-address mac-address ] [ slot slot-number ] [ { begin | exclude | include } regular-expression ]

New syntax

display ipv6 source binding [ static ] [ interface interface-type interface-number | ipv6-address ipv6-address | mac-address mac-address ] [ slot slot-number ] [ { begin | exclude | include } regular-expression ]

Views

Any view
Change description
Before modification: display ip check source ipv6
After modification: display ipv6 source binding

Modified command: ip source binding (system view)

Old syntax
user-bind ip-address ip-address mac-address mac-address
undo user-bind { all | ip-address ip-address mac-address mac-address }

New syntax
ip source binding ip-address ip-address mac-address mac-address
undo ip source binding { all | ip-address ip-address mac-address mac-address }

Views
System view

Change description
Before modification: user-bind (system view)
After modification: ip source binding(system view)

Modified command: ipv6 source binding (system view)

Old syntax
user-bind ipv6 ip-address ip-address mac-address mac-address
undo user-bind ipv6 { all | ip-address ip-address mac-address mac-address }

New syntax
ipv6 source binding ipv6-address ipv6-address mac-address mac-address
undo ipv6 source binding { all | ipv6-address ipv6-address mac-address mac-address }

Views
System view

Change description
Before modification: user-bind ipv6(system view)
After modification: ipv6 source binding(system view)

Modified command: ip source binding (interface view)

Old syntax
user-bind [ ipv6 ] { ip-address ip-address | ip-address ip-address mac-address mac-address | mac-address mac-address } [ vlan vlan-id ]
undo user-bind [ ipv6 ] { ip-address ip-address | ip-address ip-address mac-address mac-address | mac-address mac-address } [ vlan vlan-id ]

New syntax
ip source binding { ip-address ip-address | ip-address ip-address mac-address mac-address | mac-address mac-address } [ vlan vlan-id ]
undo ip source binding { ip-address ip-address | ip-address ip-address mac-address mac-address | mac-address mac-address } [ vlan vlan-id ]

Views
Layer 2 Ethernet interface view

Change description
Before modification: user-bind (interface view)
After modification: ip source binding (interface view)

Modified command: ipv6 source binding (interface view)

Old syntax
user-bind ipv6 { ip-address ip-address | ip-address ip-address mac-address mac-address | mac-address mac-address } [ vlan vlan-id ]
undo user-bind ipv6 { ip-address ip-address | ip-address ip-address mac-address mac-address | mac-address mac-address } [ vlan vlan-id ]

New syntax
ipv6 source binding { ipv6-address ipv6-address | ipv6-address ipv6-address mac-address mac-address | mac-address mac-address } [ vlan vlan-id ]
undo ipv6 source binding { ipv6-address ipv6-address | ipv6-address ipv6-address mac-address mac-address | mac-address mac-address } [ vlan vlan-id ]

Views
Layer 2 Ethernet interface view

Change description
Before modification: user-bind ipv6 (interface view)
After modification: ipv6 source binding (interface view)

Modified command: ip verify source

Old syntax
ip check source { ip-address | ip-address mac-address | mac-address }
undo ip check source

New syntax
ip verify source { ip-address | ip-address mac-address | mac-address }
undo ip verify source

Views
Layer 2 Ethernet interface view, VLAN interface view, port group view

Change description
Before modification: ip check source
After modification: ip verify source
Modified command: ipv6 verify source

Old syntax
   ip check source ipv6 { ip-address | ip-address mac-address | mac-address }
   undo ip check source ipv6

New syntax
   ipv6 verify source { ipv6-address | ipv6-address mac-address | mac-address }
   undo ipv6 verify source

Views
   Layer 2 Ethernet interface view, port group view

Change description
   Before modification: ipv6 check source
   After modification: ipv6 verify source

Modified command: ip verify source max-entries

Old syntax
   ip check source max-entries number
   undo ip check source max-entries

New syntax
   ip verify source max-entries number
   undo ip verify source max-entries

Views
   Layer 2 Ethernet interface view

Change description
   Before modification: ip check source max-entries
   After modification: ip verify source max-entries

Modified command: ipv6 verify source max-entries

Old syntax
   ip check source ipv6 max-entries number
   undo ip check source ipv6 max-entries

New syntax
   ipv6 verify source max-entries number
   undo ipv6 verify source max-entries

Views
   Layer 2 Ethernet interface view

Change description
   Before modification: ipv6 check source max-entries
   After modification: ipv6 verify source max-entries
Removed command: display user-bind

Syntax

    display user-bind [ ipv6 ] [ interface interface-type interface-number | ip-address ip-address | mac-address mac-address ] [ slot slot-number ] [ | { begin | exclude | include } regular-expression ]

Views

    Any view

Removed command: user-bind uplink

Syntax

    user-bind uplink
    undo user-bind uplink

Views

    Interface view

**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 up state.
Modified feature: Setting BGP SoO extended community attribute for BGP routing information

Feature change description

Setting Site of Origin (SoO) extended community attribute is supported in this release.

Command changes

Modified command: apply extcommunity

Old syntax

apply extcommunity { rt route-target }&<1-16> [ additive ]

New syntax

apply extcommunity { { rt route-target }&<1-16> [ additive ] | soo site-of-origin additive }

Views

Routing policy view

Change description

Before modification: The soo keyword is not supported.
After modification: The soo keyword is supported.

Modified command: ip extcommunity-list

Old syntax

ip extcommunity-list ext-comm-list-number { deny | permit } { rt route-target }&<1-16>

New syntax

ip extcommunity-list ext-comm-list-number { deny | permit } { rt route-target | soo site-of-origin }&<1-16>

Views

System view

Change description

Before modification: The soo keyword is not supported.
After modification: The soo keyword is supported.

Modified feature: RIPng IPsec command

Feature change description

The command that applies an IPsec policy to a RIPng process changed.
Command changes

Modified command: ipsec-policy

Old syntax
   ipsec-policy policy-name
   undo ipsec-policy

New syntax
   enable ipsec-policy policy-name
   undo enable ipsec-policy

Views
   RIPng view

Change description
   The command changed from ipsec-policy to enable ipsec-policy.

Modified feature: OSPFv3 IPsec command

Feature change description
   The command that applies an IPsec policy to the OSPFv3 area changed.

Command changes

Modified command: ipsec-policy

Old Syntax
   ipsec-policy policy-name
   undo ipsec-policy

New Syntax
   enable ipsec-policy policy-name
   undo enable ipsec-policy

Views
   OSPFv3 area view

Change description
   The command changed from ipsec-policy to enable ipsec-policy.

Modified feature: Setting the register suppression time for PIM/IPv6 PIM

Feature change description
   Changed the register suppression time.
Command changes

Modified command: register-suppression-timeout

Syntax
register-suppression-timeout interval

Views
Public network PIM view, VPN instance PIM view, public network IPv6 PIM view

Change description
Before modification: The \textit{interval} argument ranges from 1 to 3600.
After modification: The \textit{interval} argument ranges from 1 to 65535.

\textbf{Modified feature: Setting the maximum delay for sending a hello message in PIM/IPv6 PIM}

Feature change description
Changed the maximum delay for sending a hello message.

Command changes

Modified command: pim triggered-hello-delay

Syntax
\texttt{pim triggered-hello-delay interval}

Views
Interface view

Change description
Before modification: The \textit{interval} argument ranges from 1 to 5.
After modification: The \textit{interval} argument ranges from 1 to 60.

Modified command: pim ipv6 triggered-hello-delay

Syntax
\texttt{pim ipv6 triggered-hello-delay interval}

Views
Interface view

Change description
Before modification: The \textit{interval} argument ranges from 1 to 5.
After modification: The \textit{interval} argument ranges from 1 to 60.
Modified feature: Displaying MBGP&IPv6 MBGP routing information matching the specified BGP community list

Feature change description

The command that displays MBGP&IPv6 MBGP routing information matching the specified BGP community list changed.

Command changes

Modified command: display bgp multicast routing-table community-list

Old syntax

display bgp multicast routing-table community-list { basic-community-list-number [ whole-match ] | adv-community-list-number } &<1-16> [ | { begin | exclude | include } regular-expression ]

New syntax

display bgp multicast routing-table community-list { { basic-community-list-number | comm-list-name } [ whole-match ] | adv-community-list-number } [ | { begin | exclude | include } regular-expression ]

Views

Any view

Change description

Before modification:

- The comm-list-name argument is not supported.
- The basic-community-list-number or adv-community-list-number argument can be entered up to 16 times.

After modification:

- The comm-list-name argument is supported.
- The basic-community-list-number, comm-list-name or adv-community-list-number argument can be entered only once.

Modified command: display bgp ipv6 multicast routing-table community-list

Old syntax

display bgp ipv6 multicast routing-table community-list { basic-community-list-number [ whole-match ] | adv-community-list-number } &<1-16> [ | { begin | exclude | include } regular-expression ]

New syntax

display bgp ipv6 multicast routing-table community-list { { basic-community-list-number | comm-list-name } [ whole-match ] | adv-community-list-number } [ | { begin | exclude | include } regular-expression ]

Views

Any view

Change description

Before modification:
- The `comm-list-name` argument is not supported.
- The `basic-community-list-number` or `adv-community-list-number` argument can be entered up to 16 times.

After modification:
- The `comm-list-name` argument is supported.
- The `basic-community-list-number`, `comm-list-name` or `adv-community-list-number` argument can be entered only once.

**Modified feature: 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 the protected VLANs for the RRPP domain**

**Feature change description**

The `protected-vlan` command configures the protected VLANs for the RRPP domain by referencing MSTIs. As PVST is introduced in this release, the value range of the `instance-id-list` argument changes accordingly.

**Command changes**

Modified command: `protected-vlan`

**Syntax**

```
protected-vlan reference-instance instance-id-list
undo protected-vlan [ reference-instance instance-id-list ]
```
Views

RRPP domain view

Change description

Before modification: The instance-id-list argument ranges from 0 to 32.
After modification: The instance-id-list argument ranges from 0 to 128.

Modified feature: Configuring the protected VLANs for a smart link group

Feature change description

The protected-vlan command configures the protected VLANs for a smart link group by referencing MSTIs. As PVST is introduced in this release, the value range of the instance-id-list argument changes accordingly.

Command changes

Modified command: protected-vlan

Syntax

protected-vlan reference-instance instance-id-list
undo protected-vlan [ reference-instance instance-id-list ]

Views

Smart link group view

Change description

Before modification: The instance-id-list argument ranges from 0 to 32.
After modification: The instance-id-list argument ranges from 0 to 128.

Modified feature: Enabling ND snooping

Feature change description

The device with the new feature can create ND snooping entries based on DAD NS messages that contain link local addresses or global unicast addresses. Configure at least one type of ND snooping.

Command changes

New command: ipv6 nd snooping enable global

Use the ipv6 nd snooping enable global command to enable ND snooping based on global unicast addresses. The device uses DAD NS messages containing global unicast addresses to create ND snooping entries.

Use the undo nd snooping enable global command to restore the default.

Syntax

ipv6 nd snooping enable global
undo ipv6 nd snooping enable global

Default
ND snooping based on global unicast addresses is disabled.

Views
System view

Default command level
2: System level

Parameters
None

Examples
# Enable NS snooping based on global unicast addresses.
<Sysname> system-view
<Sysname> ipv6 nd snooping enable global

New command: ipv6 nd snooping enable link-local

Use the ipv6 nd snooping enable link-local command to enable ND snooping based on link local addresses. The device uses DAD NS messages containing link local addresses to create ND snooping entries.

Use the undo nd snooping enable link-local command to restore the default.

Syntax
ipv6 nd snooping enable link-local
undo ipv6 nd snooping enable link-local

Default
ND snooping based on link local addresses is disabled.

Views
System view

Default command level
2: System level

Parameters
None

Examples
# Enable ND snooping based on link local addresses.
<Sysname> system-view
<Sysname> ipv6 nd snooping enable link-local

Modified feature: Displaying IPv6 information for an interface

Feature change description
The keyword in the display ipv6 interface command changes.
Command changes

Modified command: display ipv6 interface

Old syntax

display ipv6 interface [ interface-type [ interface-number ] ] [ verbose ] [ | begin | exclude | include } regular-expression ]

New syntax

display ipv6 interface [ interface-type [ interface-number ] ] [ brief ] [ | begin | exclude | include } regular-expression ]

Views

Any view

Change description

Before modification: Keyword verbose is used to display detailed information for an interface.

After modification: Keyword verbose is replaced with keyword brief to display brief information for an interface.

Modified feature: Displaying IPv6 information for tunnel interfaces

Feature change description

The keyword in the display ipv6 interface tunnel command changes.

Command changes

Modified command: display ipv6 interface tunnel

Old syntax

display ipv6 interface tunnel [ number ] [ verbose ] [ | begin | exclude | include } regular-expression ]

New syntax

display interface tunnel number [ brief ] [ | begin | exclude | include } regular-expression ]

Views

Any view

Change description

Before modification: Keyword verbose is used to display detailed information for tunnel interfaces.

After modification: Keyword verbose is replaced with keyword brief to display brief information for tunnel interface.
Modified feature: Displaying socket information for a specified task

Feature change description

  The value range for the task id argument changes.

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 value for the task-id argument ranges from 1 to 100.
  After modification: The value for the task-id argument ranges from 1 to 150.
This release has no feature changes.
This release has the following changes:

- New feature: NTPv4
- New feature: Restoring default settings for a VLAN interface

**New feature: NTPv4**

Configuring NTPv4

Added NTP version 4

**Command reference**

**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 \textit{number} argument ranges from 1 to 3.
After modification: The value of the \textit{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 \textit{number} argument ranges from 1 to 3.
After modification: The value of the \textit{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.

New feature: Restoring default settings for a VLAN interface

Restoring default settings for a VLAN interface

For more information about restoring default settings for a VLAN interface, see "Configuring VLANs" in HP 5820X & 5800 Layer 2—LAN Switching Configuration Guide-F1805.

Command reference

New command: default.

For more information about this command, see "VLAN configuration commands" in HP 5820X & 5800 Layer 2—LAN Switching Command Reference-F1805.
A5800_5820X-CMW520-R1211

This release has no feature changes.