Switch 4210 V3.01.15 Release Notes

Keywords: Unresolved problems, resolved problems, software upgrading.

Abstract: This release notes describes the Switch 4210 V3.01.15 release with respect to version information, updating, unresolved problems, and solved problems.

Acronyms:

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full spelling</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL</td>
<td>Access Control List</td>
</tr>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
</tr>
<tr>
<td>BPDU</td>
<td>Bridge Protocol Data Unit</td>
</tr>
<tr>
<td>BPS</td>
<td>Bit Per Second</td>
</tr>
<tr>
<td>CLI</td>
<td>Command Line Interface</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DSCP</td>
<td>Differentiated Services Codepoint Priority</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>EPON</td>
<td>Ethernet Passive Optical Network</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>GARP</td>
<td>Generic Attribute Registration Protocol</td>
</tr>
<tr>
<td>GVRP</td>
<td>GARP VLAN Registration Protocol</td>
</tr>
<tr>
<td>HGMP</td>
<td>Huawei Group Management Protocol</td>
</tr>
<tr>
<td>HQ</td>
<td>High-Priority Queuing</td>
</tr>
<tr>
<td>HGMP</td>
<td>Huawei Group Management Protocol</td>
</tr>
<tr>
<td>IGMP</td>
<td>Internet Group Management Protocol</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>LACP</td>
<td>Link Aggregation Control Protocol</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>MIB</td>
<td>Manage Information Base</td>
</tr>
<tr>
<td>MSTP</td>
<td>Multiple Spanning Tree Protocol</td>
</tr>
<tr>
<td>NDP</td>
<td>Neighbor Discover Protocol</td>
</tr>
<tr>
<td>NTDP</td>
<td>Neighbor Topology Discovery Protocol</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>Acronym</td>
<td>Full spelling</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>ONU</td>
<td>Optical Network Unit</td>
</tr>
<tr>
<td>PEAP</td>
<td>Protected Extensible Authentication Protocol</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-In User Service</td>
</tr>
<tr>
<td>RMON</td>
<td>Remote Monitoring</td>
</tr>
<tr>
<td>RSPAN</td>
<td>Remote Switched Port Analyzer</td>
</tr>
<tr>
<td>RSTP</td>
<td>Rapid Spanning Tree Protocol</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>STP</td>
<td>Spanning Tree Protocol</td>
</tr>
<tr>
<td>TCP</td>
<td>Transfer Control Protocol</td>
</tr>
<tr>
<td>TFTP</td>
<td>Trivial File Transfer Protocol</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>VCT</td>
<td>Virtual Cable Test</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>VFS</td>
<td>Virtual File System</td>
</tr>
<tr>
<td>WRR</td>
<td>Weighted Round Robin</td>
</tr>
</tbody>
</table>
Table of Contents

Version Information.............................................................................................................. 6
  Version Number .................................................................................................................. 6
  Version History .................................................................................................................. 6
  Hardware and Software Compatibility Matrix .................................................................. 7
Restrictions and Cautions ..................................................................................................... 8
Feature List ........................................................................................................................... 8
  Hardware Features ............................................................................................................. 8
  Software Features ............................................................................................................. 10
Version Updates .................................................................................................................... 11
  Feature Updates ................................................................................................................ 11
  Command Line Updates ................................................................................................... 14
  MIB Updates ..................................................................................................................... 22
  Configuration Changes ..................................................................................................... 23
    Configuration Changes in V3.01.15 ............................................................................... 23
    Configuration Changes in V3.01.14 ............................................................................... 23
    Configuration Changes in V3.01.13 ............................................................................... 23
    Configuration Changes in V3.01.12 ............................................................................... 24
    Configuration Changes in V3.01.10 ............................................................................... 24
    Configuration Changes in V3.01.09 ............................................................................... 25
    Configuration Changes in V3.01.06 ............................................................................... 25
    Configuration Changes in V3.01.04 ............................................................................... 26
Open Problems and Workarounds ....................................................................................... 26
List of Resolved Problems .................................................................................................... 27
  Resolved Problems in V3.01.15 ....................................................................................... 27
  Resolved Problems in V3.01.14 ....................................................................................... 27
  Resolved Problems in V3.01.13 ....................................................................................... 27
  Resolved Problems in V3.01.12 ....................................................................................... 34
  Resolved Problems in V3.01.11 ....................................................................................... 34
  Resolved Problems in V3.01.10 ....................................................................................... 35
  Resolved Problems in V3.01.09 ....................................................................................... 35
  Resolved Problems in V3.01.08 ....................................................................................... 36
  Resolved Problems in V3.01.06 ....................................................................................... 37
  Resolved Problems in V3.01.05 ....................................................................................... 41
  Resolved Problems in V3.01.04 ....................................................................................... 41
  Resolved Problems in V3.01.03 ....................................................................................... 44
  Resolved Problems in V3.01.02 ....................................................................................... 45
  Resolved Problems in V3.01.01 ....................................................................................... 45
Software Upgrading

- Remote Upgrading through CLI
- Boot Menu
- Software Upgrading via Console Port (Xmodem Protocol)
- Software Upgrading via Ethernet Interface (FTP/TFTP)
  - Using TFTP Through an Ethernet Interface
  - Using FTP Through an Ethernet Interface

Appendix

- Details of Modified CLI Commands in V3.01.15
  - key (HWTACACS scheme view)
  - key (RADIUS scheme view)
  - local-server nas-ip
  - mac-authentication authmode username asmacaddress
  - mac-authentication authpassword
  - ntp-service authentication-keyid
  - password (Remote-ping test group view)
  - password (local user view)
  - primary accounting (RADIUS scheme view)
  - primary authentication (RADIUS scheme view)
  - secondary accounting (RADIUS scheme view)
  - secondary authentication (RADIUS scheme view)
  - set authentication password
  - snmp-agent usm-user v3
  - super password

- Details of Added CLI Commands in V3.01.13
  - dot1x mandatory-domain
  - accounting lan-access
  - accounting login
  - authentication lan-access
  - authentication login
  - authorization login
  - scheme lan-access
  - scheme login
  - primary accounting
  - primary authentication
  - secondary accounting
  - secondary authentication
  - state primary
  - state secondary
  - cut connection
  - display connection
  - nas-ip
  - radius nas-ip
  - port-security timer autolearn
List of Tables

Table 1 Version history .............................................................................................................................. 6
Table 2 Hardware and software compatibility matrix ............................................................................... 7
Table 3 Hardware features (1) ................................................................................................................... 8
Table 4 Hardware features (2) ................................................................................................................... 9
Table 5 Software features ........................................................................................................................ 10
Table 6 Feature updates ........................................................................................................................... 11
Table 7 Command line updates ................................................................................................................ 14
Table 8 MIB updates ............................................................................................................................... 22
Table 9 Encrypted authentication key length requirements ..................................................................... 62
Table 10 Encrypted privacy key length requirements ............................................................................ 62
Table 11 Description of the Port NO field ............................................................................................. 80
Version Information

Version Number

Version Information:

3Com OS V3.01.15s168

Note: To view version information, use the display version command in any view. See Note①.

Version History

Table 1 Version history

<table>
<thead>
<tr>
<th>Version number</th>
<th>Last version</th>
<th>Release Date</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>V3.01.15s168</td>
<td>V3.01.14s168</td>
<td>2012-12-17</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.14s168</td>
<td>V3.01.13s168</td>
<td>2012-10-19</td>
<td>Usage version</td>
</tr>
<tr>
<td>V3.01.13s56</td>
<td>V3.01.12s56</td>
<td>2010-08-03</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.12s168</td>
<td>V3.01.11s168</td>
<td>2009-07-16</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.11s56</td>
<td>V3.01.10s56</td>
<td>2009-05-26</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.11s168</td>
<td>V3.01.10s168</td>
<td>2009-05-26</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.10s56</td>
<td>V3.01.09s56</td>
<td>2009-03-19</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.10s168</td>
<td>V3.01.09s168</td>
<td>2009-03-19</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.09s56</td>
<td>V3.01.08s56</td>
<td>2009-02-25</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.09s168</td>
<td>V3.01.08s168</td>
<td>2009-02-25</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.08s56</td>
<td>V3.01.06s56</td>
<td>2008-12-04</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.08s168</td>
<td>V3.01.06s168</td>
<td>2008-12-04</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.06s56</td>
<td>V3.01.05s56</td>
<td>2008-06-23</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.06s168</td>
<td>V3.01.05s168</td>
<td>2008-06-23</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.05s56</td>
<td>V3.01.04s56</td>
<td>2008-05-05</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.05s168</td>
<td>V3.01.04s168</td>
<td>2008-05-05</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.04s56</td>
<td>V3.01.03s56</td>
<td>2007-12-21</td>
<td>Support for Switch 4210 52-port</td>
</tr>
<tr>
<td>V3.01.04s168</td>
<td>V3.01.03s168</td>
<td>2007-12-21</td>
<td>Support for Switch 4210 52-port</td>
</tr>
<tr>
<td>V3.01.03s56</td>
<td>V3.01.02s56</td>
<td>2007-09-18</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.03s168</td>
<td>V3.01.02s168</td>
<td>2007-09-18</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.02s56</td>
<td>V3.01.01s56</td>
<td>2007-09-05</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.02s168</td>
<td>V3.01.01s168</td>
<td>2007-09-05</td>
<td>None</td>
</tr>
</tbody>
</table>
Hardware and Software Compatibility Matrix

<table>
<thead>
<tr>
<th>Item</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Product family</strong></td>
<td>Switch 4210 series</td>
</tr>
<tr>
<td><strong>Hardware platform</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Switch 4210 9-Port</td>
</tr>
<tr>
<td></td>
<td>● Switch 4210 18-port</td>
</tr>
<tr>
<td></td>
<td>● Switch 4210 26-port</td>
</tr>
<tr>
<td></td>
<td>● Switch 4210 PWR 9-port</td>
</tr>
<tr>
<td></td>
<td>● Switch 4210 PWR 18-port</td>
</tr>
<tr>
<td></td>
<td>● Switch 4210 PWR 26-port</td>
</tr>
<tr>
<td></td>
<td>● Switch 4210 PWR 52-port</td>
</tr>
<tr>
<td><strong>Minimum memory requirements</strong></td>
<td>64 MB</td>
</tr>
<tr>
<td><strong>Minimum Flash requirements</strong></td>
<td>8 MB</td>
</tr>
<tr>
<td><strong>Boot ROM version</strong></td>
<td>V4.10 or higher (You can view the version number with the display version command in any view. Please see Note ②)</td>
</tr>
<tr>
<td><strong>Host software</strong></td>
<td>s4o03_01_15s168.app</td>
</tr>
<tr>
<td><strong>iMC version</strong></td>
<td>iMC PLAT 5.1 SP1 (E0202P05)</td>
</tr>
<tr>
<td></td>
<td>iMC UAM 5.1SP1 (E0301P03)</td>
</tr>
<tr>
<td></td>
<td>iMC QoSM 5.1 (E0201)</td>
</tr>
<tr>
<td></td>
<td>iMC TAM5.1 (E0301)</td>
</tr>
<tr>
<td><strong>iNode version</strong></td>
<td>iNode PC 5.1 (E0304)</td>
</tr>
<tr>
<td><strong>Web version</strong></td>
<td>s4p01_016</td>
</tr>
<tr>
<td><strong>Remarks</strong></td>
<td>The web file and application file (.bin) are two different files. Quidview and iMC should be purchased separately. When using Quidview to upgrade the device’s software, you need to select the latest software version manually.</td>
</tr>
</tbody>
</table>

Sample: Display the version number of the software and boot ROM of the switch:

```
<4210>display version
3Com Corporation
3Com Switch 4210 PWR 18-Port Software Version 3Com OS V3.01.15s168
------- Note①
Copyright (c) 2004-2012 3Com Corporation and its licensors, All rights reserved.
3Com Switch 4210 PWR 18-Port uptime is 0 week, 0 day, 5 hours, 49 minutes
```
3Com Switch 4210 FWR 18-Port with 1 Processor
64M bytes SDRAM
8M bytes Flash Memory
Config Register points to FLASH

Hardware Version is REV.A
Bootrom Version is 4.10 ------ Note②
CPLD Version is 001

[Subslot 0] 16FE+2Combo SFP Hardware Version is REV.A

Restrictions and Cautions

1) When 802.1X or centralized MAC authentication is enabled on the device, it is recommended to enable attack protection on the access ports to protect the CPU from attacks.

2) Problems of packet forwarding and MIB statistics
   - The packets whose source MAC address is a multicast address or all-zero can be forwarded and the all-zero MAC address can be learned in ARL, but the zero MAC address cannot be displayed.
   - Wire-speed traffic from multiple ports is output through a half-duplex port and is not load shared, and error packets are counted. When traffic speed goes lower than the wire speed, above problems disappear.
   - Packets larger than 1518 bytes are counted as jumbo packets.
   - The etherStatsUndersizePkts MIB statistics are not precise for packets smaller than 64 bytes.

3) When a port has learned the maximum MAC addresses, it drops the BPDU protocol suite packets, including STP, Dot1X and NDP packets.

4) A version prior to V3.01.15 might not support the cipher and simple keywords or use a different password encryption algorithm than V3.01.15 or a later version. If you downgrade the software from V3.01.15 or a later version to a version prior to V3.01.15, or upgrade it to V3.01.15 or a later version and roll it back after saving the configuration file, the relevant configuration commands might get lost or the passwords might become invalid. For more information, see the change descriptions for the commands.

Feature List

Hardware Features

Table 3 Hardware features (1)

<table>
<thead>
<tr>
<th>Item</th>
<th>Switch 4210 9-Port</th>
<th>Switch 4210 18-port</th>
<th>Switch 4210 26-port</th>
<th>Switch 4210 52-port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dimensions (H × W × D)</td>
<td>43.6mm × 230mm × 160mm (1.72 × 9.06 × 6.30 in.)</td>
<td>43.6mm × 360mm × 160mm (1.72 × 14.17 × 6.30 in.)</td>
<td>43.6mm × 440mm × 160mm (1.72 × 17.32 × 6.30 in.)</td>
<td>43.6mm × 440mm × 230mm (1.72 × 17.32 × 9.06 in.)</td>
</tr>
<tr>
<td>Physical dimensions</td>
<td>≤ 3 kg</td>
<td>≤ 3 kg</td>
<td>≤ 3 kg</td>
<td>≤ 5.5 kg</td>
</tr>
<tr>
<td>Weight</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Table 4 Hardware features (2)

<table>
<thead>
<tr>
<th>Item</th>
<th>Switch 4210 PWR 9-port</th>
<th>Switch 4210 PWR 18-port</th>
<th>Switch 4210 PWR 26-port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service ports</td>
<td>8 10/100Base-TX ports and 1 Combo port</td>
<td>16 10/100Base-TX ports and 2 Combo ports</td>
<td>24 10/100Base-TX ports and 2 Combo ports</td>
</tr>
<tr>
<td>Input voltage</td>
<td>AC:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Rated voltage range: 100 VAC to 240 VAC (50Hz to 60Hz)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Max Voltage range: 90 VAC to 264 VAC (47Hz to 63Hz)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum power consumption</td>
<td>10W</td>
<td>12W</td>
<td>14W</td>
</tr>
<tr>
<td>Operating temperature</td>
<td>0°C to 45°C (32°F to 113°F)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating humidity</td>
<td>10% to 90%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Dimensions (H × W × D)**

- **Physical dimensions (length * width * height)**
  - Switch 4210 PWR 9-port: 43.6mm × 300mm × 220mm (1.72 × 11.81 × 8.66 in.)
  - Switch 4210 PWR 18-port: 43.6mm × 300mm × 260mm (1.72 × 11.81 × 10.24 in.)
  - Switch 4210 PWR 26-port: 43.6mm × 440mm × 420mm (1.72 × 17.32 × 16.54 in.)

- **Weight**
  - ≤ 3 kg
  - ≤ 3.5 kg
  - ≤ 6.5 kg

- **Service ports**
  - 8 10/100Base-TX ports and 1 Combo port
  - 16 10/100Base-TX ports and 2 Combo ports
  - 24 10/100Base-TX ports and 2 Combo ports

- **Input voltage**
  - Switch 4210 PWR 26-port supports both AC and DC(RPS) input, while the others just support AC input.
  - **AC:**
    - Rated voltage range: 100 VAC to 240 VAC (50Hz to 60Hz)
    - Max Voltage range: 90 VAC to 264 VAC (47Hz to 63Hz)
  - **DC(RPS):**
    - Rated voltage range: -52 VDC to -56 VDC

- **Maximum power consumption**
  - 95 W, PoE: 65 W
  - 160 W, PoE: 125 W
  - AC: 465W, PoE: 370W
  - DC: 400W, PoE: 370W

- **Operating temperature**
  - 0°C to 45°C (32°F to 113°F)

- **Operating humidity**
  - 10% to 90%
# Software Features

## Table 5 Software features

<table>
<thead>
<tr>
<th>Category</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switching mode</td>
<td>Store and forward</td>
</tr>
<tr>
<td>VLAN</td>
<td>Up to 4K IEEE 802.1Q VLANs</td>
</tr>
<tr>
<td>VLAN interface</td>
<td>One VLAN interface</td>
</tr>
<tr>
<td>Broadcast suppression</td>
<td>Broadcast suppression based on port bandwidth percentage</td>
</tr>
</tbody>
</table>
| Multicast                        | - IGMP v1/v2/v3 snooping  
- 256 multicast entries                                                                   |
| Unknown multicast drop           | Supported                                                                                                                               |
| STP                              | STP/RSTP/MSTP                                                                                                                           |
| Port mirroring                   | Support one to multiple mirroring (one monitor port, multiple mirrored ports that are not limited)                                      |
| Link-aggregation                 | - LACP  
- Manual aggregation  
- Up to 8 ports per aggregation group  
- Switch 4210 26-port and Switch 4210 PWR 26-port support up to 3 aggregation groups; the others support 2 aggregation groups.  
- Switch 4210 52-port supports up to 6 aggregation groups, each of which supports up to 8 ports. |
| Port isolate                     | Supported                                                                                                                               |
| Loopback-detection               | Supported                                                                                                                               |
| Port internal and external loopback test | Supported                                                                                           |
| MAC address table                | - Automatic MAC address learning  
- Compliant with IEEE 802.1D  
- Up to 8K MAC addresses  
- Up to 1K static MAC addresses  
- Dynamic and static unicast MAC addresses and black-hole MAC addresses supported |
| Flow-control                     | - IEEE 802.3x flow-control (full duplex)  
- Back-pressure based flow control (half duplex)                                                   |
| Software upload and upgrade      | Software upload and upgrade through the XMODEM protocol, FTP or TFTP                                                                  |
| Management                       | CLI; Telnet; Console; SNMP; RMON 1,2,3,9 group MIB; HGMP V2; QuidView network management; web network management; logging; alarming; IPv6 management |
| Maintenance                      | - Debugging  
- ping, traceroute  
- Telnet  
- VCT  
- Remote ping                                                                                   |
| QoS/ACL                          | 4 output queues per port                                                                                                                |
### Version Updates

#### Feature Updates

<table>
<thead>
<tr>
<th>Table 6 Feature updates</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Version number</th>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>V3.01.15</td>
<td>Hardware feature updates</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Software feature updates</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.14</td>
<td>Hardware feature updates</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Software feature updates</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.13</td>
<td>Hardware feature updates</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Software feature updates</td>
<td>New features:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Telnet fail trap</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Mandatory 802.1X authentication domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Multiple secondary RADIUS servers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• AAA servers per user type</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IPv6-supported 802.1X authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• MAC aging for port security auto-learn</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deleted features: None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modified features: None</td>
</tr>
<tr>
<td>V3.01.12</td>
<td>Hardware feature updates</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Software feature updates</td>
<td>New features:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Re-accounting after re-authentication user name changed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• LACP MAD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deleted features: None</td>
</tr>
<tr>
<td>Version number</td>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>V3.01.11</td>
<td>Hardware feature updates</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Software feature updates</td>
<td>New features:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Command alias</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deleted features: None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modified features: None</td>
</tr>
<tr>
<td>V3.01.10</td>
<td>Hardware feature updates</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Software feature updates</td>
<td>New features: None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deleted features: None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modified features: None</td>
</tr>
<tr>
<td>V3.01.09</td>
<td>Hardware feature updates</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Software feature updates</td>
<td>New features:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• RADIUS attribute–ignore feature</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Line rate limit assigned by RADIUS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deleted features: None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modified features: None</td>
</tr>
<tr>
<td>V3.01.08</td>
<td>Hardware feature updates</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Software feature updates</td>
<td>New features:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Auto VLAN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Speed-auto</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Auto power-down</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PoE time on/off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• GVRP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• MVR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Storm suppression</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• LLDPP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• VLAN VPN (Tunnel)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HWTACACS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DHCP snooping server guard</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IGMP snooping non-flooding</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PKI</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DHCP auto-configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deleted features: None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modified features: None</td>
</tr>
<tr>
<td>Version number</td>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>V3.01.06</td>
<td>Hardware feature updates</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Software feature updates</td>
<td>New features:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Link delay</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Boot ROM MIB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Stop-accounting MIB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Batch configuration of loopback-detection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Loopback-detection shutdown mode</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Source MAC address consistency check of ARP packets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Multicast group-specific query for modifying source IP addresses</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DHCP client support for default route assignment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deleted features: None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modified features: None</td>
</tr>
<tr>
<td>V3.01.05</td>
<td>Hardware feature updates</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Software feature updates</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.04</td>
<td>Hardware feature updates</td>
<td>New device:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Switch 4210 52-port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deleted features: None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modified features: None</td>
</tr>
<tr>
<td></td>
<td>Software feature updates</td>
<td>New features:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• FTP disconnect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• RSA import key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deleted features: None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modified features: None</td>
</tr>
<tr>
<td>V3.01.03</td>
<td>Hardware feature updates</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Software feature updates</td>
<td>New features:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Support for adding multicast MAC addresses manually</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Support for 100Base-FX SFP Transceiver - Dual Mode(3CSFP9-81), 100Base-LX10 SFP Transceiver - Dual Mode(3CSFP9-82) SFP module</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deleted features: None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modified features: None</td>
</tr>
<tr>
<td>V3.01.02</td>
<td>Hardware feature updates</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Software feature updates</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.01</td>
<td>Hardware feature updates</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Software feature updates</td>
<td>None</td>
</tr>
</tbody>
</table>
## Command Line Updates

### Table 7 Command line updates

<table>
<thead>
<tr>
<th>Version number</th>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>V3.01.15</td>
<td>New Commands</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Deleted Commands</td>
<td>Command 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Syntax:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>`local-user password-display-mode { auto</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>undo local-user password-display-mode</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>View : system view</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Module of the command: AAA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Description:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The local-user password-display-mode command is not available to set the method for displaying local user passwords.</td>
</tr>
<tr>
<td></td>
<td>Modified Commands</td>
<td>Please refer to <a href="#">Details of Modified CLI Commands in V3.01.15</a></td>
</tr>
<tr>
<td>V3.01.14</td>
<td>New Commands</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Deleted Commands</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Modified Commands</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.13</td>
<td>New Commands</td>
<td>Please refer to <a href="#">Details of Added CLI Commands in V3.01.13</a></td>
</tr>
<tr>
<td></td>
<td>Deleted Commands</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Modified Commands</td>
<td>Command 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Syntax:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>mac-authentication timer offline-detect offline-detect-value</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>View : system view</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Module of the command: MAC authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Description:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In before, the value range for the <code>offline-detect-value</code> argument is 1 to 65535 and now the value range for the <code>offline-detect-value</code> argument is 0 to 3000000. The offline detect timer configured in Ethernet port view takes precedence over the one configured in system view. If the offline-detect-value argument takes the value of 0, the offline detect timer is disabled.</td>
</tr>
<tr>
<td>V3.01.12</td>
<td>New Commands</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Deleted Commands</td>
<td>None</td>
</tr>
<tr>
<td>Version number</td>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>Commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Modified Commands</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.11</td>
<td>New Commands</td>
<td>Command 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Syntax:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>command-alias enable</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>undo command-alias enable</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>View : system view</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Parameters: None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Description:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the <strong>command-alias enable</strong> command to enable the command alias function.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the <strong>undo command-alias enable</strong> command to disable the command alias function.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the command alias function is disabled, that is, you cannot configure command aliases.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td># Enable the command alias function.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[4210] command-alias enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Command 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Syntax:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>command-alias mapping</strong> cmdkey alias</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>undo command-alias mapping</strong> cmdkey</td>
</tr>
<tr>
<td></td>
<td></td>
<td>View : system view</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Parameters:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cmdkey: The complete form of the first keyword of a command for which an alias will be configured.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>alias: Specifies the command alias, which cannot be the same with the first keyword of an existing command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Description:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the <strong>command-alias mapping</strong> command to configure command aliases.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the <strong>undo command-alias mapping</strong> command to delete command aliases.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, a command has no alias.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td># Configure command aliases by specifying <strong>show</strong> as the replacement of the <strong>display</strong> keyword.</td>
</tr>
<tr>
<td>Version number</td>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>[4210] command-alias mapping display show</td>
<td>Command 3</td>
</tr>
<tr>
<td></td>
<td>Syntax:</td>
<td><strong>display command-alias</strong></td>
</tr>
<tr>
<td></td>
<td>View: any view</td>
<td>Parameters: None</td>
</tr>
<tr>
<td></td>
<td>Description:</td>
<td>Use the <strong>display command-alias</strong> command to display defined command aliases and the corresponding commands</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td># Display the defined command aliases and the corresponding commands.</td>
</tr>
<tr>
<td></td>
<td>[4210] display command-alias</td>
<td>Command alias is enabled</td>
</tr>
<tr>
<td></td>
<td>index alias command key</td>
<td>1 show display</td>
</tr>
<tr>
<td></td>
<td>Deleted Commands</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Modified Commands</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.10</td>
<td>New Commands</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Deleted Commands</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Modified Commands</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.09</td>
<td>New Commands</td>
<td>Command 1</td>
</tr>
<tr>
<td></td>
<td>Syntax:</td>
<td><strong>attribute-ignore</strong> { standard</td>
</tr>
<tr>
<td></td>
<td>undo attribute-ignore { all</td>
<td>standard</td>
</tr>
<tr>
<td></td>
<td>Parameters:</td>
<td>vendor-id: Specifies the vendor ID that should be ignored, in the range 1 to 16777215.</td>
</tr>
<tr>
<td></td>
<td>type-value: Specifies the type value that should be ignored, in the range 1 to 255. Up to 8 type values can be specified in one command line.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description:</td>
<td>This command is used to configure the RADIUS attribute-ignore function.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Version number</td>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td># Configure radius scheme &quot;system&quot; to ignore the type 81 standard attribute.</td>
<td>[4210-radius-system]attribute-ignore standard type 81</td>
</tr>
<tr>
<td></td>
<td>[4210-radius-system]attribute-ignore standard type 81</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Deleted Commands</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Modified Commands</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.08</td>
<td>New Commands</td>
<td>Please refer to the manuals.</td>
</tr>
<tr>
<td></td>
<td>Deleted Commands</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Modified Commands</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.06</td>
<td>New Commands</td>
<td>Command 1 Syntax: [undo] link-delay value View: interface view Parameters: value: Specifies the delay time. Description: This command is used to configure the link-down delay time in the range 2 to 10 seconds. Example: # Configure the link-down delay time of Ethernet1/0/1 as 5 seconds. [4210-Ethernet1/0/1] link-delay 5 Command 2 Syntax: [undo] loopback-detection interface-list enable View: system view Parameters: interface-list: Specify a list of ports. interface-list = { interface-type interface-number [ to interface-type interface-number ] }&amp;&lt;1-10&gt; Description: This command is used to configure the loopback-detection function on specified ports. Example: # Enable loopback detection on Ethernet1/0/1 through Ethernet1/0/5. [4210] loopback-detection ethernet1/0/1 to ethernet 1/0/5 enable Command 3 Syntax: [undo] loopback-detection shutdown enable</td>
</tr>
<tr>
<td>Version number</td>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>View : interface view</td>
<td>Parameter: None</td>
</tr>
<tr>
<td></td>
<td>Description: This command is used to configure the loopback-detection shutdown mode. With loopback-detection shutdown enabled, the port will be shut down when a loop occurs to it.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: # Enable loopback detection shutdown on Ethernet1/0/1.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[4210-Ethernet1/0/1] loopback-detection shutdown enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Command 4</td>
<td>Syntax: [undo] arp anti-attack valid-check enable</td>
</tr>
<tr>
<td></td>
<td>View: system view</td>
<td>Parameter: None</td>
</tr>
<tr>
<td></td>
<td>Description: This command is used to configure the source MAC address consistency check of ARP packets, which is disabled by default. With this function enable, the switch drops ARP packets whose source MAC address differs from the sender MAC address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: # Enable the source MAC address consistency check of ARP packets,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[4210] arp anti-attack valid-check enable</td>
<td></td>
</tr>
<tr>
<td>Deleted Commands</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Modified Commands</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>V3.01.05</td>
<td>New Commands</td>
<td>None</td>
</tr>
<tr>
<td>Deleted Commands</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Modified Commands</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>V3.01.04</td>
<td>New Commands</td>
<td>Command1</td>
</tr>
<tr>
<td>Syntax: ftp disconnect user-name</td>
<td>View: system view</td>
<td></td>
</tr>
<tr>
<td>Parameters:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>user-name: Name of the host to be disconnected from the FTP server. The host name is a string comprising 1 to 184 characters.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description: Use the command to tear down a specified user from the FTP server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example: # Disconnect the user named “admin” from the FTP server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Version number</td>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>[4210] ftp disconnect admin</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Command2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Syntax:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>rsa peer-public-key keyname import sshkey filename</code></td>
<td></td>
</tr>
</tbody>
</table>
|                | `undo rsa peer-public-key keyname`                       | View: system view  
Parameters:  
`keyname`: Name of the public key, a string of 1 to 64 characters.  
`filename`: Name of a public key file, a string of 1 to 142 characters.  
Description:  
Use the `rsa peer-public-key import sshkey` command to import a peer public key from the public key file. Use the `undo rsa peer-public-key` command to remove the setting.  
After execution of this command, the system automatically transforms the public key file into PKCS format, and imports the peer public key. This requires that you get a copy of the public key file from the peer through FTP/TFTP.  
Example:  
# Import the public key named 123 from the file abc.  
[4210] rsa peer-public-key 123 import sshkey abc |
<p>|                | Deleted Commands                                         | None                                                                         |
|                | Modified Commands                                        | None                                                                         |</p>
<table>
<thead>
<tr>
<th>Version number</th>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>V3.01.03</td>
<td>New Commands</td>
<td></td>
</tr>
</tbody>
</table>

**Command 1**

Syntax: `display mac-address multicast [ static ] { { mac-address vlan vlan-id } | count } | count ]`

View: Any view

Parameters:

- **static**: Displays static multicast MAC address entries.
- **mac-address vlan vlan-id**: Displays multicast MAC address entries in the specified VLAN.
- **count**: Displays the number of MAC entries.

**Vlan-id**: ID of the specific VLAN.

Description:

Use the `display mac-address multicast` command to display specific multicast MAC address entries manually configured on the switch.

Executing this command with neither mac-address vlan vlan-id nor vlan vlan-id will display all the multicast MAC address entries, each entry including the multicast MAC address, VLAN ID, state of the MAC address, port number and aging time.

Executing this command with vlan vlan-id but without mac-address will display all the multicast MAC address entries in the specified VLAN, each entry including the multicast MAC address, VLAN ID, state of the MAC address, port number and aging time.

Executing this command with both mac-address and vlan vlan-id will display the specified multicast MAC address entry in the specified VLAN, including the multicast MAC address, VLAN ID, state of the MAC address, port number and aging time.

Executing this command with count specified will display the number of specific multicast MAC address entries.

Example:

```
# Display the static multicast MAC address entries in VLAN 1.
<4210> display mac-address multicast static vlan 1
```

**Command 2**

Syntax:

- `mac-address multicast mac-address interface interface-list vlan vlan-id`
- `undo mac-address multicast [ mac-address [ interface interface-list ] vlan vlan-id ]`

View: system view

Parameters:

- **mac-address**: Multicast MAC address.
- **vlan-id**: VLAN ID.
- **interface-list**: Specifies one or multiple forwarding ports. You can
provide up to 10 port lists, by each of which you can specify an individual port in the form of interface-type interface-number, or a port range in the form of interface-type start-interface-number to interface-type end-interface-number, where the end port number must be greater than the start port number. Refer to the parameter description in the “Port Basic Configuration” part in this manual.

Description:

Use the **mac-address multicast** command to add a multicast MAC address entry.

Use the **undo mac-address multicast** command to remove a multicast MAC address entry.

Each multicast MAC address entry contains multicast address, forward port, VLAN ID, and so on.

Related command: **display mac-address multicast static**.

Example:

# Add a multicast MAC address entry, wherein the MAC address is 0100-5e0a-0805, and the outgoing port is Ethernet 1/0/1 in VLAN 1.

[4210] mac-address multicast 0100-5e0a-0805 interface Ethernet 1/0/1 vlan 1

Command 3

Syntax:

**mac-address multicast** mac-address vlan vlan-id

**undo mac-address multicast** [ [ mac-address ] vlan vlan-id ]

View: Ethernet port view

Parameters:

*mac-address*: Multicast MAC address.

*vlan-id*: VLAN ID.

Description:

Use the **mac-address multicast vlan** command to add a multicast MAC address entry on the port.

Use the **undo mac-address multicast vlan** command to remove a multicast MAC address entry from the port.

Each multicast MAC address entry contains multicast address, VLAN ID, and so on.

Related command: display mac-address multicast static.

Example:

# Add a multicast MAC address entry with MAC address 0100-1000-1000 in VLAN 1.

[4210-Ethernet1/0/1] mac-address multicast 0100-1000-1000 vlan 1

### Deleted Commands

None
## MIB Updates

### Table 8 MIB updates

<table>
<thead>
<tr>
<th>Version number</th>
<th>Item</th>
<th>MIB file</th>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>V3.01.15</td>
<td>New</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.14</td>
<td>New</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.13</td>
<td>New</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>V3.01.12</td>
<td>New</td>
<td>H3C-LLDP-EXT-MIB</td>
<td>LLDP</td>
<td>Adding the following private MIB:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(1) h3clldpAdminStatus: Enable/Disable LLDP in global;</td>
</tr>
<tr>
<td></td>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>(2) h3clldpComplianceCDPStatus: LLDP supports CDP in global;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(3) h3clldpPortConfigTable:LLDP port configure table;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(4) h3clldpPortConfigPortNum: LLDP port number;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(5) h3clldpPortConfigCDPComplianceStatus: LLDP supports CDP in port</td>
</tr>
<tr>
<td>V3.01.09</td>
<td>New</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a3com_domain_tree.c</td>
<td>h3cDomainVlanAssignMo</td>
<td>A VLAN assignment mode of vlanlist is added in the new version. There are three</td>
</tr>
</tbody>
</table>
### VLAN assignment modes now:

- **1 (integer)** - Integer VLAN assignment mode.
- **2 (string)** - String VLAN assignment mode.
- **3 (vlanlist)** - VLAN list VLAN assignment mode.

The default mode is integer. The 3rd mode is used to support auto-VLAN feature.

<table>
<thead>
<tr>
<th>Version number</th>
<th>Item</th>
<th>MIB file</th>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>V3.01.08</td>
<td>New</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Modified</td>
<td>IEEE8021-PAE-MIB</td>
<td>Dot1XPaePortInitialize</td>
<td>This node is implemented in the new version. After you set the attribute of the node to true, all 802.1X users on the corresponding port are disconnected, and then the attribute of the module returns to false. If you perform get operations to the node, it always returns “false”.</td>
</tr>
<tr>
<td>V3.01.06</td>
<td>New</td>
<td>h3c-radius.mib</td>
<td>H3C-RADIUS</td>
<td>Accounting-on supported</td>
</tr>
<tr>
<td></td>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

## Configuration Changes

### Configuration Changes in V3.01.15

None

### Configuration Changes in V3.01.14

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

### Configuration Changes in V3.01.13

The operation of ethernet type in loopback-detection packet

In early version:

The ethernet type in loopback-detection packet is 0x9000.

In current version:

The ethernet type in loopback-detection packet is 0x9001.
**Configuration Changes in V3.01.12**

1) The operation of Net2Startup in CONFIG-MAN-MIB

   In early version:

   Executing "Net2Startup" operation in "CONFIG-MAN-MIB", the filename can not contain directory.

   In current version:

   Executing "Net2Startup" operation in "CONFIG-MAN-MIB", the filename can contain directory.

2) Change to the content of option60 field in DHCP packets

   In early version:

   When the switch is configured as a DHCP client, the option60 field in DHCP discover packets sent by the switch is filled only with the product series information.

   In current version:

   When the switch is configured as a DHCP client, the option60 field in DHCP discover packets sent by the switch is filled with the product series information and other more detailed information.

3) The operation about Management address in LLDP packets

   In early version:

   If the LLDP management-address has not been configured, the IP address of the VLAN with smallest ID which the port belongs to will be used. And if the IP address of the VLAN with smallest ID which the port belong to has not been configured, the loopback IP (127.0.0.1) address will be used.

   In current version:

   (1) If the LLDP management-address has not been configured, the IP address of the smallest permitted VLAN whose IP is configured will be used;

   (2) If the LLDP management-address has been configured, and the port belongs to the VLAN with the LLDP management-address, the IP address will be used;

   (3) Otherwise, no IP address will be used.

4) Modification of 802.1X re-authentication with user-name change

   In early version:

   Doing 802.1X re-authentication with a RADIUS server. Even if user-name changes, the device just sends RADIUS Access-Request packet for the latter user-name, but does not send RADIUS Accounting-Stop packet for the former user-name.

   In current version:

   Doing 802.1X re-authentication with a RADIUS server. If user-name changes, the device sends RADIUS Accounting-Stop packet for the former user-name firstly, then sends RADIUS Access-Request packet for the latter user-name.

**Configuration Changes in V3.01.10**

1) DHCP autoconfig operation changes
Before modification:

A device that has no configuration file specified for startup performs autoconfig until either of the following two conditions is met:

- It obtains an IP address and the IP address of a TFTP server from a DHCP server, and then obtains a configuration file from the TFTP server.
- The user terminates the autoconfig operation through the console.

After modification:

Besides the above two conditions, either of the following two conditions can also trigger the end of autoconfig.

- No TFTP server is specified on the DHCP server.
- The TFTP server does not have the configuration file that device wants to get.

When one of conditions B, C and D is met, the device will run the factory default configuration file 3comoscfg.def.

Configuration Changes in V3.01.09

1) Changes to the reboot procedure of a device having a console loopback connector inserted

Before modification:

After a device that has a console loopback connector inserted is rebooted, it looks for a configuration file in the following sequence to complete initialization:

- The specified configuration file
- A configuration file obtained through the DHCP auto-configuration function;
- The factory default configuration file.
- System default settings.

After modification:

- After being rebooted for 15 seconds, the device checks whether the console loopback connector exists. If yes, the LEDs of Ethernet ports flash 3 times.
- Then the device skips the steps of loading the specified configuration file and using DHCP auto-configuration.
- If a factory default configuration file exists, it uses that file to initialize.
- If not, it initializes by using the default settings.

If the device has no console loopback connector inserted, the reboot procedure is the same as before.

Configuration Changes in V3.01.06

1) The MTU is changed from 1522 bytes to 1536 bytes

2) Dot1X timer tx-period command changes

Before modification:

The interval for sending 802.1X multicast requests set with the Dot1X timer tx-period command is in the range 10 to 120 seconds. If a port joins the guest VLAN upon receiving no response for an 802.1X multicast request, the shortest time for the port to join the guest VLAN is about 10 seconds.

After Modification:
The interval for sending 802.1X multicast requests set with the **Dot1X timer tx-period** command is in the range 1 to 120 seconds. If a port joins to the guest VLAN upon receiving no response for an 802.1X multicast request, the shortest time for the port to join the guest VLAN is about 1 second.

3) Modification to the processing of 802.1X client IP address changes

Before modification:

If an 802.1X client has its IP address manually changed after login, the device will force the client to log off.

If an 802.1X client has its IP address changed through DHCP after login, the device that is not enabled with DHCP snooping will force the client to log off.

After modification:

The device will not force the client to log off in the above two cases.

**Configuration Changes in V3.01.04**

Before modification:

The function of ignoring configuration always takes effect after configured.

After modification:

It takes effect only once after configured.

**Open Problems and Workarounds**

**LSOD08166**

- First found-in version: V3.01.12
- Description: At first Device1 learns some dynamics VLAN, and delete part of VLAN that Device1 learnt on Device2. Then Device1 can’t learn any dynamics VLAN, and the VLAN status is also something wrong on Device1.

- Workaround: None
List of Resolved Problems

Resolved Problems in V3.01.15

LSOD010584
- First found-in version: V3.01.14
- Condition: Configure password in ciphertext.
- Description: Because of the weak cryptographic algorithm there is a risk that the stored passwords possibly be cracked.

Resolved Problems in V3.01.14

LSOD010576
- First found-in version: V3.01.13
- Condition: Access the hh3cUserPassword node of hh3cUserInfoTable by SNMP.
- Description: When access the hh3cUserPassword node of hh3cUserInfoTable by SNMP, the device returns the user's password.

Resolved Problems in V3.01.13

LSOD09902
- First found-in version: V3.01.12
- Condition: CPU is busy and there is a lot of trap information in a moment.
- Description: Device reboots abnormally.

LSOD09931
- First found-in version: V3.01.12
- Condition: Configured 'snmp-agent target-host trap address udp-domain A.B.C.D (D>223) params securityname RADAR' in system view.
- Description: Execute 'undo snmp-agent target-host A.B.C.D (D>223) securityname RADAR' unsuccessfully.

ZDD03035
- First found-in version: V3.01.12
- Condition: Some NMS send messages to the device at the same time.
- Description: The device can only process 10 messages in one time, others are dropped.

LSOD10017
- First Found-in Version: V3.01.12
- Condition: The device uses DC power.
- Description: There is 'Power 1: Get Temperature failed' while executing command 'display environment'.
LSOD08491

- First found-in version: V3.01.08
- Condition: Create a VLAN interface and configure an IP address for it on the device. Then ping the IP address on the device.
- Description: The ping operation fails.

LSOD07991

- First found-in version: V3.01.12
- Condition: A large number of Dot1x user login and logoff repeatedly. Then disabled Dot1x through undo dot1x“ command.
- Description: The device can’t delete some users which is login, and the device can’t enable Dot1x any more.

LSOD08988

- First found-in version: V3.01.12
- Condition: One user with privilege level 0 logs in the WEB management interface.
- Description: WEB can not show the page of ‘Help’.

LSOD08866

- First found-in version: V3.01.12
- Condition: Walk the entAliasMappingIdentifer node.
- Description: The multiple entities of walk result have the same index which causes the failure in synchronizing device data through SNMP network management.

LSOD09925

- First Found-in Version: V3.01.12
- Condition: Configure ‘authentication-mode scheme command-authorization’ on VTY scheme. Telnet user passes RADIUS authentication and login the device.
- Description: After login, every command executed by user will cause memory leak.

LSOD09840

- First Found-in Version: V3.01.12
- Condition: Configure port-security userlogin-without mode and send Dot1x packet to the device.
- Description: The Dot1x packet causes the intrusion check which should not do like that.

LSOD09842

- First Found-in Version: V3.01.12
- Condition: Configure loopback-detection on the device and execute the “loopback interval” command.
- Description: Sometimes, the failure of ‘loopback interval’ will occur.

LSOD09865

- First Found-in Version: V3.01.12
- Condition: Both the ‘mac-authentication’ and ‘mac-authentication guest-vlan’ are enabled on the port. User A is online, and user B tries to log in by ‘mac-authentication’.
- Description: User B can not pass the ‘mac-authentication’.

**LSOD09834**

- First Found-in Version: V3.01.12
- Condition: When an HGMP stack is established, two communities named public and private are automatically created for this stack. Create a new SNMP community named public or private, and associate an ACL with this community. Save the configuration. Then reboot the device, or disable and then enable the stack.
- Description: The SNMP community is not associated with an ACL.

**LSOD09831**

- First Found-in Version: V3.01.12
- Condition: The client application does dot1x authentication with TTLS certification.
- Description: By chance, the device reboots abnormally for dead loop.

**LSOD09744**

- First Found-in Version: V3.01.12
- Condition: Port-security port-mode is userlogin-secure-or-mac or userlogin-secure-or-mac-ext, and the port-security guest-VLAN is the same as the MAC-authentication authorizing VLAN. A user enters the port-security guest-VLAN because dot1x authentication fails or MAC-authentication fails, then passes the MAC-authentication and quits the port-security guest-VLAN.
- Description: The user can not access the network.

**LSOD09807**

- First Found-in Version: V3.01.12
- Condition: After the device rebooted, switch Combo port from copper to fiber.
- Description: Occasionally, the fiber ports of some devices can not link up.

**LSOD09783**

- First Found-in Version: V3.01.12
- Condition: Configure link-delay with X seconds on Combo port. Switch Combo port from copper to fiber and then switch from fiber to copper.
- Description: There is no up down information of Combo port.

**LSOD09818**

- First Found-in Version: V3.01.12
- Condition: After startup, the device tries to get configuration by DHCP auto configuration.
- Description: During the device getting configuration, the network would be intermittent.

**LSOD09709**

- First Found-in Version: V3.01.12
- Condition: Configuring 'authentication-mode scheme command-authorization' on the user interface, a user telneting the switch and login in successfully through local authentication mode, then the user running a valid command such as 'quit' through telnet.
- Description: The device will be rebooted abnormally.
LSOD09703
- First Found-in Version: V3.01.12
- Condition: Configure ‘IGMP-snooping nonflooding-enable’ on device and broadcast suppression on port.
- Description: The result of broadcast suppression is not correct.

LSOD09646
- First Found-in Version: V3.01.12
- Condition: The network device acted as SSH server, and received specific SSH attack packets.
- Description: The device will be rebooted abnormally.

LSOD09326
- First Found-in Version: V3.01.12
- Condition: As the following operation:
  1. Create an SSL server policy, example: ssl server-policy myssl1
  2. Https use this SSL server policy, example: ip https ssl-server-policy myssl1
  3. Undo use this SSL server policy, example: undo ip https ssl-server-policy
- Description: This ssl server policy can't be deleted.

LSOD09566
- First Found-in Version: V3.01.12
- Condition: Configure ‘accounting optional’. Configure ‘dot1x timer server-timeout’ to X seconds. Do dot1X authentication with RADIUS server. When logging in, accounting-Start packet from the switch to the RADIUS server gets no response.
- Description: After log out, the client can not log in again until X seconds after.

LSOD09643
- First Found-in Version: V3.01.12
- Condition: Execute the command ‘display diagnostic-information’ on device.
- Description: Sometimes the device reboots abnormally.

LSOD09596
- First Found-in Version: V3.01.12
- Condition: Disable LLDP on device globally. Port X received LLDP packet.
- Description: The LLDP packet is forwarded to the other ports which should be discarded.

LSOD09434
- First Found-in Version: V3.01.12
- Condition: In domain view, configure authentication scheme to be radius scheme, but do not configure accounting scheme. Configure ‘accounting optional’.
- Description: Users can not log-in successfully.
LSOD09447
- First Found-in Version: V3.01.12
- Condition: Do 802.1X authentication with iNode client (whose version is lower than V3.60-E6206) on PC, and *upload IP address* option is chosen. PC gets IP address from DHCP server.
- Description: The switch passes empty user-name to the RADIUS server, and authentication fails.

LSOD09439
- First Found-in Version: V3.01.12
- Condition: Configure port-security auto learn mode on port A. Delete all MAC-address and change the VLAN ID of the port A while there are background traffic.
- Description: The MAC of the old VLAN is left occasionally.

LSOD09268
- First Found-in Version: V3.01.12
- Condition: Connect device to HUAWEI S2300 and running LLDP.
- Description: The device can not find S2300 as LLDP neighbor.

LSOD09537
- First Found-in Version: V3.01.12
- Condition: The user’s MAC item moves from port A to port B in switch. Port A is a single port, port B is in the aggregation group whose master port is down.
- Description: User’s ARP item can not be updated by MAC item.

LSOD09498
- First Found-in Version: V3.01.12
- Condition: Connect with HUAWEI S2300. Enable LLDP and show LLDP neighbor information.
- Description: The ‘Management address OID’ section of neighbor information will be garbage characters.

LSOD09555
- First Found-in Version: V3.01.12
- Condition: On the authentication port Y, execute ‘undo dot1x’ command and then execute ‘dot1x’ command during dot1X authentication.
- Description: In a very small chance, the information ‘Port Y is Processing Last 802.1X command... Please try again later.’ is shown.

LSOD09550
- First Found-in Version: V3.01.12
- Condition: Configure ‘dot1x timer server-timeout’ to X seconds, and configure ‘dot1x authentication-method eap’. Do dot1X authentication. The EAP Request Challenge packet from the switch to the client gets no response.
- Description: The switch will not send EAP Failure packet until (X+80) seconds after.

LSOD09571
- First Found-in Version: V3.01.12
- Condition: Multiple ports join into the same multicast group, and then display MAC address by port.
- Description: The output information is not correct.

**LSOD09280**

- First Found-in Version: V3.01.12
- Condition: Send packets with VLAN tag that increase by the same steps to port A, then configure MAC address maximum count limit on port A.
- Description: The MAC address count that learnt at port A can not reach the maximum count.

**LSOD09170**

- First Found-in Version: V3.01.12
- Condition: Configure RMON statistics on port. View the statistics information through `display rmon statistics` command.
- Description: Only the input data is calculated in the etherStatsOctets and etherStatsPkts items which should also include the output data.

**LSOD09263**

- First Found-in Version: V3.01.12
- Condition: IP address A is not a local IP of the device. Configure A as NAS-IP of the scheme with `nas-ip` command in HWTACACS scheme view; or configure A as global NAS-IP with `hwtacacs nas-ip` command in system-view.
- Description: The command is executed correctly, but it does not give the prompt: 'Warning: This ip address is not a local ip address, maybe it doesn't work.'.

**LSOD09283**

- First Found-in Version: V3.01.12
- Condition: Display local port information of LLDP when protocol VLAN has not been enabled.
- Description: The protocol VLAN ID of LLDP local port information is 1. But according to LLDP standard the VLAN ID should be 0 when there is no protocol VLAN set. This bug also exists in the transmitted LLDP packet.

**LSOD09284**

- First Found-in Version: V3.01.12
- Condition: Move a port in discarding state into a link-aggregation group on which STP is disabled.
- Description: The port moved remains in discarding state and won't change to forwarding.

**LSOD09278**

- First Found-in Version: V3.01.12
- Condition: Firstly, configure PKI domain, PKI entity, PKI certificate attribute group and PKI access control policy and then delete PKI certificate attribute group and PKI access control policy.
- Description: There will be some unknown characters when display current-configuration.

**LSOD09187**

- First Found-in Version: V3.01.12
- Condition: Execute ‘igmp-snooping group-policy XXXX’ and ‘multicast static-group Y.Y.Y.Y vlan Z’. Then add the rule of ACL XXXX, permit the multicast static-group Y.Y.Y.Y.
- Description: There is no entry of group Y.Y.Y.Y in igmp-snooping group table.

**LSOD09052**
- First Found-in Version: V3.01.12
- Condition: Change the system name of the switch.
- Description: The system name recorded by LLDP would update after 30s, which results in slow update of the system name of this switch recorded by neighbor device.

**LSOD09123**
- First Found-in Version: V3.01.12
- Condition: Configure remote server (radius-scheme or hwtacacs-scheme) as authentication scheme. Do not configure accounting scheme. Create local-user A on the device. User-name A can pass authentication on remote server.
- Description: User-name A can successfully logon, although the password configuration of local-user A is null or it is not consistent with remote server.

**LSOD09204**
- First Found-in Version: V3.01.12
- Condition: Connect PC to port A. Configure port-security on port A (the port-mode is mac-and-userlogin-secure, userlogin-secure-or-mac, mac-else-userlogin-secure, userlogin-secure or userlogin-without). Do 802.1X authentication with windows XP client on PC.
- Description: After log-in, windows XP client does re-authentication frequently.

**LSOD09167**
- First Found-in Version: V3.01.12
- Condition: Many 802.1X users are on-line on the same device (about 1000). In system-view, execute ‘undo dot1x’ command, and then execute ‘dot1x’ command.
- Description: Executing the ‘dot1x’ command always fails, and the system prompts ‘Processing Last 802.1X command... Please try again later.’

**LSOD09143**
- First Found-in Version: V3.01.12
- Condition: The device has been configured ‘igmp-snooping non-flooding’ function. The VLAN X is configured igmp-snooping function and configures port Y as static router port. VLAN X receives unknown multicast flow, and then disables igmp-snooping function in VLAN X.
- Description: The port which is not router port can receive unknown multicast flow.

**LSOD09124**
- First Found-in Version: V3.01.12
- Condition: Delete the MAC address after the MAC table of the device is full.
- Description: There is still only one MAC address which can not be deleted.
LSOD09095

- First Found-in Version: V3.01.12
- Condition: Enable Dot1x authentication on a device, and connect a PC to a trunk port of the device through a Netgear switch. The data traffic should be tagged when it passes the trunk port. Then do Dot1x authentication.
- Description: After log-on, PC’s MAC-Address is learnt in the PVID VLAN of the port, not the tagged VLAN. So, the port can not forward the data traffic.

Resolved Problems in V3.01.12

LSOD09059

- First found-in version: V3.01.11
- Condition: Configure "dot1x guest-vlan" on the port. Users succeed in authentication, and authorization VLAN is assigned to the port. After that, configure "undo dot1x" on the port.
- Description: In a very tiny chance, the port remains in the authorization VLAN.

LSOD08977

- First found-in version: V3.01.11
- Condition: Enable mac-authentication and set the offline-detect timer to be larger than one half of mac-address aging timer on the switch. And connect a PC to the switch to do mac-authentication, but the traffic sent from the PC is very small, such as only sending one packet every 2 or 3 minutes.
- Description: The PC may log off probably even though the mac-address of the PC has not aged-out on the switch.

Resolved Problems in V3.01.11

LSOD08894

- First found-in version: V3.01.08
- Condition: Devices installed with V3.01.08 or V3.01.09 or V3.01.10 start up.
- Description: Some of these devices reboot abnormally.

LSOD08517

- First found-in version: V3.01.10
- Condition: The device fails to get ‘crl’ through "pki retrieval-crl domain" command.
- Description: The memory leaks.

LSOD08515

- First found-in version: V3.01.10
- Condition: Import local certification through “pki import-certificate local domain” command.
- Description: The memory leaks.

LSOD08575

- First found-in version: V3.01.08
- Condition: Configure “IGMP-snooping nonflooding” and NTP multicast client.
● Description: The device can not synchronize the timer from NTP server.

**LSOD08818**

● First found-in version: V3.01.10
● Condition: There are many MAC authentication users on device. View these users from WEB.
● Description: If the total character count exceeds 10240, the WEB, console or telnet can not work normally. Sometimes, the device reboots abnormally.

**LSOD08752**

● First found-in version: V3.01.08
● Condition: Plug in 3Com customized SFP module to the device which manufacturer is not 3Com.
● Description: The vendor name information is displayed as "3Com" in command "display transceiver" which should be the actual manufacturer name.

**LSOD08852**

● First found-in version: V3.01.08
● Condition: Access the 4210-52 Port Devices installed with V3.01.08 or V3.01.09 or V3.01.10 through WEB.
● Description: The WEB prompts to not support this device.

**LSOD08951**

● First found-in version: V3.01.10
● Condition: Use “display mac-address” command following VLAN parameter to view MAC address information.
● Description: The device will have no response or display the same MAC address repeatedly.

**LSOD08984**

● First found-in version: V3.01.10
● Condition: The device gets IP address as DHCP client.
● Description: The content of DHCP option60 field is not filled with different product type when the device sends DHCP discover packet.

**Resolved Problems in V3.01.10**

**LSOD08754**

● First found-in version: V3.01.08
● Condition: Devices installed with V3.01.08 or V3.01.09 start up.
● Description: Some of these devices reboot repeatedly.

**Resolved Problems in V3.01.09**

**LSOD08461**

● First found-in version: V3.01.08
● Condition: Connect two devices through aggregate ports. Enable LLDP on both devices. Then, one aggregate port goes down.
● Description: The devices reboot abnormally.
LSOD08410

- First found-in version: V3.01.08
- Condition: The device outputs logs when the PoE card works abnormally.
- Description: There is little probability that the device reboots.

LSOD08392

- First found-in version: V3.01.08
- Condition: After the switch gets an IP address through DHCP, configure a manual link-aggregation group, and then display link-aggregation group detailed information.
- Description: The switch reboots abnormally.

LSOD08510

- First found-in version: V3.01.08
- Condition: The device connects with another device through a 1000M optical port. Configure “speed auto 100”. The optical port goes down. Then configure “undo speed”.
- Description: The optical port cannot go up.

LSOD08639

- First found-in version: V3.01.08
- Condition: Perform a get operation to the MIB node “dot1dTpFdbEntry” and “dot1qTpFdbTable” by using SNMP from the device.
- Description: A get operation failure is returned.

LSOD08628

- First found-in version: V3.01.08
- Condition: Get the MIB variable “lldpRemPortDescription” from the device through SNMP.
- Description: The returned value is not equal to MIB node “ifDesc”.

Resolved Problems in V3.01.08

LSOD08009

- First found-in version: V3.01.06
- Condition: The device acts as an SSH/Telnet server, and the SecureCRT acts as an SSH/Telnet client. Paste a lot of configurations in the client window after successful login.
- Description: Some configurations are lost.

LSOD08193

- First found-in version: V3.01.06
- Condition: Configure password information.
- Description: The password can be displayed in log information, which compromises security.

LSOD07800

- First found-in version: V3.01.06
- Condition: Port A has a VLAN ID assigned dynamically. Copy the configuration of port A to port B by executing the copy configuration command.
- Description: The dynamic VLAN attribute of port A is also copied to port B.

**LSOD08229**

- First found-in version: V3.01.06
- Condition:

![Network Diagram](image)

STP is enabled on devices in the above figure. Some ports on the root bridge go down and up frequently, and at the same time PC 1 pings PC 2 continuously. Lots of STP TC packets are transmitted on the network.

- Description: Some ping packets between PC1 and PC2 are lost.

**LSOD08289**

- First found-in version: V3.01.06
- Condition: Reboot a 4210 52-port device.
- Description: Some ports' LED is turned on while other ports' LED is off during restart.

**LSOD08342**

- First found-in version: V3.01.06
- Condition:

![Network Diagram](image)

In the above figure, the three devices connect with each other through 100Base-SFP. Each optical port is configured with auto-negotiation mode. Reboot device 2.

- Description: After reboot, the optical ports of device 2 cannot forward packets.

**Resolved Problems in V3.01.06**

**LSOD06559**

- First found-in version: V3.01.05
- Condition: Enable Dot1X, re-authentication and Dot1X handshake. Configure the period of Dot1X re-authentication as 60 seconds and the period of handshake as 30 seconds. Set the number of retransmission attempts to 1. A client passes authentication.
- Description: The client logs off automatically after being online for 60 seconds.

**LSOD06992**
- First found-in version: V3.01.05
- Condition: Enable anti-attack function with the command “system-guard enable” on the device.
- Description: The device cannot detect attacks when the threshold is reached.

**LSOD06962**
- First found-in version: V3.01.05
- Condition: Enable LACP on a port, and then execute the **loopback internal** command on that port.
- Description: The internal loopback test of that port fails.

**LSOD05321**
- First found-in version: V3.01.05
- Condition: A client sends an IGMP report packet destined to N.0.0.13 (N is between 224 and 240) to the switch.
- Description: The switch floods the packet to all other ports rather than sends it to the IGMP routing port.

**LSOD06207**
- First found-in version: V3.01.05
- Condition:

![Diagram](image)

Configure Dot1X on port A which does not perform authentication. Configure the PC’s MAC address as a static MAC address on port A.
- Description:
  The PC cannot get an IP address from the DHCP server.

**LSOD06877**
- First found-in version: V3.01.05
- Condition: Configure Dot1X on the device, which performs authentication on a DRCOM client.
- Description: Sometimes, the EAPOL start packet from the client gets no response, and thus authentication cannot succeed. Once authentication succeeds, the client cannot log off because the EAPOL logoff packet from the client gets no response.

**LSOD05492**

- First found-in version: V3.01.05
- Condition: Set the minimum super user password length to N1. Set super user password “password 1” with a length of N2. Then change the minimum super user password length to N3 (N3>N2>N1). Log out and then log in.
- Description: Password 1 can still be used to log in.

**LSOD06871**

- First found-in version: V3.01.05
- Condition: Use the `tftp source-ip` command to set a source IP address for establishing TFTP connections.
- Description: This configuration takes effect at the CLI, but fails on the web interface.

**LSOD06887**

- First found-in version: V3.01.05
- Condition:

```
+---------------------+
|                   | ftp server          |
|                  /   |
|              device|
| (top)       |   A | (bottom)               |
|              |     | pc                      |
```

Configure the outbound rate limit on port A. The PC downloads files from the FTP server.
- Description:

The actual download rate is quite higher than the configured rate limit.

**LSOD07540**

- First found-in version: V3.01.05
- Condition: Configure the `global loopback detection enable` command on the device, and disable it. Then, enable loopback detection on port A.
- Description: Port A still sends loopback detection packets to the neighbor although global loopback detection is disabled.

**LSOD06981**

- First found-in version: V3.01.05
- Condition: The device receives LACP protocol packets not compliant to the protocol (124 bytes).
- Description: These LACP protocol packets are considered invalid and discarded. Thus, the aggregation process fails.

**LSOD07147**

- First found-in version: V3.01.05
- Condition:

    ![Device](image)

    Port A

Disable loopback detection globally on the device, and enable loopback detection on port A. A loop exists on port A.

- Description:

    The device still sends traps showing there is a loop on port A, while correctly it should not send such traps.

**LSOD07375**

- First found-in version: V3.01.05
- Condition: Send UDP packets whose destination port is 1645 or 1646 to the device.
- Description: Each UDP packet causes a memory leak of 32 bytes.

**LSOD07479**

- First found-in version: V3.01.05
- Condition: Disable and enable STP periodically, causing the STP network topology to change frequently.
- Description: The device may reboot without exception information.

**LSOD07571**

- First found-in version: V3.01.05
- Condition: Configure the **IP address dhcp-alloc** command on a VLAN interface.
- Description: The TTL of the DHCP Discovery packet sent by the VLAN interface is 1. When some DHCP relay agent products receive this packet, they may drop the packet for TTL expiration. Thus the DHCP Discovery packet cannot be forwarded to the DHCP server.

**LSOD07676**

- First found-in version: V3.01.05
- Condition: Configure the **IP address dhcp-alloc** command on a VLAN interface.
- Description: The TTL of the DHCP Discovery packet sent by the VLAN interface is 1. When some DHCP relay agent products receive this packet, they may drop the packet for TTL expiration. Thus the DHCP Discovery packet cannot be forwarded to the DHCP server.
In the above figure, the two switches are enabled with loopback-detection. And a loop exists on switch 2.

- **Description:**
  
  Sometimes, switch 1 can find the existence of the loop and thus disable port A. As a result, users connected to switch 2 are cut off.

**LSOD07695**

- First found-in version: V3.01.05
- Condition: For a Dot1X authentication port, the dynamically assigned VLAN ID and the previous PVID are not in the same MSTP instance.
- Description: Dot1X authentication fails.

**Resolved Problems in V3.01.05**

**LSOD07514**

- First found-in version: V3.01.04
- Condition: Devices are powered on.
- Description: Some devices cannot startup, and print “Starting....” repeatedly.

**LSOD06686**

- First found-in version: V3.01.04
- Condition: Reboot a 4210 52-port device.
- Description: The LEDs of all ports on the device may be blinking.

**Resolved Problems in V3.01.04**

**LSOD05430**

- First found-in version: V3.01.03
- Condition: Enable STP on the device. A port learns some ARP entries and then receives STP TC packets.
- Description: The ARP entries on this port are deleted.

**LSOD05769**

- First found-in version: V3.01.03
- Condition: Execute the `flow-interval` command on a port.
- Description: “in second” in the help information should be changed to “in seconds”.

**LSOD05840**

- First found-in version: V3.01.03
- Condition: Enable Dot1X and re-authentication. Configure the period of re-authentication as 60 seconds. A user succeeds in PEAP authentication.
- Description: The user fails re-authentication after being online for about 60 seconds.

**LSOD05809**

- First found-in version: V3.01.03
- Condition: More than two devices form a cluster. Execute the `display cluster` command on one device.
- Description: The output information has grammar problems.

**LSOD05807**

- First found-in version: V3.01.03
- Condition: More than two devices form a cluster. Execute the `reboot member mac-address` command on the administrator to reboot the specified cluster member.
- Description: The cluster member cannot be rebooted.

**LSOD05950**

- First found-in version: V3.01.03
- Condition: Configure 802.1X authentication on the switch. A client gets online through the switch after passing authentication. Then, cut off the online client from the RADIUS server.
- Description: The “Terminate-Cause” field in the packet that the switch sends to the RADIUS server is not correct.

**LSOD05951**

- First found-in version: V3.01.03
- Condition: Configure the switch as the administrator of a cluster. Member switches join and quit the cluster frequently.
- Description: A memory leak occurs.

**LSOD06155**

- First found-in version: V3.01.03
- Condition: More than two devices form a cluster. Display the cluster information on the device.
- Description: The output information has grammar problems.

**LSOD06148**

- First found-in version: V3.01.03
- Description: The device reboots repeatedly when the user starts MAC authentication.
**LSOD05267**

- First found-in version: V3.01.03
- Condition: Enable port security `else` mode on the device. Configure a legal user that can pass both Dot1X and MAC authentication. The user starts Dot1X authentication.
- Description: The user passes Dot1X authentication, and does not go through MAC authentication. The correct process is that the user should pass MAC authentication without going through Dot1X authentication.

**LSOD06181**

- First found-in version: V3.01.03
- Condition: Enable port security `userlogin-withoui` mode and configure the port security OUI MAC address. The PC’s MAC address is different from the OUI MAC address. Configure the user of the PC as a legal Dot1X user.
- Description: The user passes Dot1X authentication, but the device sends a trap showing “An intrusion occurs” repeatedly.

**LSOD06271**

- First found-in version: V3.01.03
- Condition:

  ![Diagram](image)

  Two switches are connected as shown in the figure above and have STP enabled. LSW-A is the STP root bridge. Enable LACP on each port.
- Description:
  Four ports form a link aggregation group, however the link between port 2 of LSW-A and port 1 of LSW-B cannot forward packets.

**LSOD06263**

- First found-in version: V3.01.03
- Condition: Enable MAC-authentication, configure accounting-on in the RADIUS scheme, save the configuration, and then restart the switch. During restart, send packets to the switch to trigger MAC authentication.
- Description: A memory leak occurs.

**LSOD06284**

- First found-in version: V3.01.03
- Condition: Enable Dot1X and configure the EAP authentication mode. Enable Dot1X re-authentication and disable Dot1X hand-shake. A user passes Dot1X authentication.
- Description: After a long time, the user is cut off due to Dot1X re-authentication failure.

**LSOD06432**

- First found-in version: V3.01.03
- Condition: Enable Dot1X and configure the EAP authentication mode. After the user passes Dot1X authentication, send EAP response packets with an abnormal value in the packet length field from the PC to the device.
- Description: The device reboots abnormally.

**LSOD06487**

- First found-in version: V3.01.03
- Condition: Two devices connect with each other. On device 1, ping device 2 all the time. The ping operation is successful. Execute the **save configure file** command on device 2.
- Description: During and after the saving process, the ping operation fails.

**LSOD05267**

- First found-in version: V3.01.03
- Condition: Configure the "else" mode of port-security on the device.
- Description: The else mode does not comply with 3Com's else mode, and cannot ensure performing MAC authentication first.

**LSOD04069**

- First found-in version: V3.01.03
- Condition: Configure the attribute of "User Access Level" on the device, and the device cannot recognize this attribute.
- Description: The telnet user cannot get the access privilege.

**LSOD04154**

- First found-in version: V3.01.03
- Condition: Log in to the device through web.
- Description: The web help page does not help.

**LSOD04364**

- First found-in version: V3.01.03
- Condition: Configure the "and" mode of port-security on the device. A user passes MAC authentication without passing 802.1X authentication.
- Description: The user can ping a peer through the device.

**Resolved Problems in V3.01.03**

**LSOD05700**

- First found-in version: V3.01.02
- Condition: Open and close the debug switch of TCP or UDP packets repeatedly.
- Description: Useless prompts are output.

LSOD05698
- First found-in version: V3.01.02
- Condition: Save the configuration file by using the FTP of the “3Com Enterprise Management Suite” software.
- Description: The name of the saved configuration file does not include the unit ID.

LSOD05701
- First found-in version: V3.01.02
- Condition: Build a cluster, and then configure the same telnet users on the command switch and member switch without passwords. Log in to the command switch through web, and then manage the member switch through web.
- Description: Although access to the member switch succeeds, but “Login Failed” appears.

LSOD05700
- First found-in version: V3.01.02
- Condition: Execute the `debugging udp packet` command twice.
- Description: “This UDP packet debugging switch is on!” appears.

LSOD05698
- First found-in version: V3.01.02
- Condition: Use FTP to download a configuration file without unit number specified.
- Description: The FTP operation fails due to invalid filename.

LSOD05699
- First found-in version: V3.01.02
- Condition: None
- Description: The switch cannot recognize 100Base-LX10 SFP, 100Base-FX SFP, 100Base-BX10-U and D SFP modules.

**Resolved Problems in V3.01.02**

LSOD05400
- First found-in version: V3.01.01
- Condition: Power on a PoE device in a very low temperature environment.
- Description: The device cannot start up normally.

**Resolved Problems in V3.01.01**

None

**Related Documentation**

For the most up-to-date version of documentation:
1) Go to http://www.3Com.com/downloads
2) Select Documentation for Type of File and select Product Category.

Software Upgrading

⚠️ Caution

Upgrade software only when necessary and under the guidance of a technical support engineer.

Normally, the software of Switch 4210 is upgraded via serial port. However, this method is rather slow and very time-consuming. In addition, in this method, users either have to upgrade the switches at the installation sites or gather all the switches to upgrade one by one, whichever will consume enormous manpower. To solve the problem, 4210 Ethernet Switch uses the TFTP and FTP modules, which enable you to upgrade software and download files fast and flexibly.

Remote Upgrading through CLI

You may upgrade the application program and Boot ROM program of a device remotely through the command line interface (CLI). To this end, telnet to the device from a computer (at 10.10.110.1, for example) running FTP server first; and then get the application and Boot ROM program, switch.bin and switch.btm for example, from the FTP server as follows:

```
<H3C> ftp 10.10.110.1
Trying ...  
Connected.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(none):lyt
331 Give me your password, please
Password:
230 Logged in successfully
[ftp] get SWITCH.bin
[ftp] get SWITCH.btm
[ftp] bye
<H3C> boot bootrom SWITCH.btm
please wait ...
Bootrom is updated!
<H3C> boot boot-loader SWITCH.bin
<H3C> display boot-loader
The app to boot at the next time is: flash:/ SWITCH.bin
<H3C> reboot
```

After getting the new application file, reboot the device to validate it.

Note that if you do not have enough Flash space, upgrade the Boot ROM program first, and then download the application file to the device.
The following sections introduce some approaches to local upgrading.

Boot Menu

Upon power-on, the switch runs the Boot ROM program first. The following information will be displayed on the terminal:

Starting......

***********************************************************
*                                                         *
*      Switch 4210 PWR 18-Port BOOTROM, Version 4.10      *
*                                                         *
***********************************************************

Copyright(c) 2004-2010 3Com Corporation and its licensors.
Creation date   : Jul 21 2010, 17:00:56
CPU Clock Speed : 200MHz
BUS Clock Speed : 33MHz
Memory Size     : 64MB
Mac Address     : 000fe2004210

Press Ctrl-B to enter Boot Menu... 2

Note

After the screen displays “Press Ctrl-B to enter Boot Menu...”, you need to press <Ctrl+B> within 5 seconds to access the Boot menu. Otherwise, the system will start program decompression, and then you have to reboot the switch to access the Boot menu.

The system displays:

Password:

Enter the correct password (no password is set by default) to access the Boot menu.

Caution

Please keep in mind the modified Bootrom password.

1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. Modify bootrom password
6. Enter bootrom upgrade menu
7. Skip current configuration file
8. Set bootrom password recovery
9. Set switch startup mode
0. Reboot

Enter your choice(0-9):

Software Upgrading via Console Port (Xmodem Protocol)

**Step1** Enter 1 in the Boot menu. Press <Enter> to access the download program menu.

Please set application file download protocol parameter:
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return

Enter your choice(0-3):3

**Step2** Enter 3 to select the Xmodem protocol and press <Enter>. The following information appears:

Please select your download baudrate:
1. 9600
2. 19200
3. 38400
4. 57600
5. 115200
6. Return

Enter your choice (0-5):

**Step3** Select the appropriate download baud rate. For example, enter 5 to select the download baud rate of 115200 bps. Press <Enter> and the following information appears:

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

**Step4** Configure the same baud rate on the console terminal, disconnect the terminal and reconnect it. Then, press <Enter> to start downloading. The following information appears:

Are you sure to download file to flash? Yes or No(Y/N)y
Now please start transfer file with XMODEM protocol.
If you want to exit,Press <Ctrl+X>.
Downloading ... CCCCC
Note

After the terminal baud rate is modified, it is necessary to disconnect and then re-connect the terminal emulation program to validate the new setting.

Step 5 Select [Transfer\Send File] from the terminal window. Click <Browse> in the pop-up window and select the software to be downloaded. Select Xmodem from the Protocol drop down list.

Figure 1 Send File

Step 6 Click <Send> and the following window appears.

Figure 2 Xmodem File Send

Step 7 After downloading completes, the following information appears:

Loading ........................................................done
Software Upgrading via Ethernet Interface (FTP/TFTP)

Using TFTP Through an Ethernet Interface

1) Introduction to TFTP

The Trivial File Transfer Protocol (TFTP) employs UDP to provide unreliable data transfer service.

2) Upgrade procedure

Step1 Connect an Ethernet interface of the switch to the PC where the program files are located, and connect the console port of the switch to the same PC.

Step2 Run the TFTP server program on the PC, and put the program files into a file directory.

Caution

4210 series switches are not shipped with the TFTP server program.

Step3 Run the terminal emulation program on the PC, and start the switch, to access the Boot menu.

Step4 Enter 1 in the Boot menu, and press <Enter> to enter the following menu.

Please set application file download protocol parameter:
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return
Enter your choice(0-3):1

Step5 Enter 1 to use TFTP, and press <Enter>. The following information appears:

Please modify your TFTP protocol parameter:
Load File name
Switch IP address
Server IP address

Step6 Input correct information and press <Enter>. The following information appears:

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

Step7 Enter Y to start downloading the files. Enter N to return to the Boot menu. Take entering Y as an example. Enter Y and press <Enter>, the system begins downloading programs. After downloading completes, the system starts writing the programs to the flash. Upon completion of this operation, the screen displays the following information to indicate that the downloading is completed:

Loading ........................................................done
Writing to flash................................................done!
Using FTP Through an Ethernet Interface

1) Introduction to FTP

The 4210 can serve as an FTP server or client. In the following example, the 4210 serves as an FTP client.

2) Upgrade procedure

**Step1** Connect an Ethernet interface of the 4800G to the PC where the program files are located, and connect the console port of the switch to the same PC.

**Step2** Run the FTP server program on the PC, and put the program files into a file directory.

**Step3** Run the terminal emulation program on the PC, and start the switch to access the Boot menu.

**Step4** Enter 1 in the Boot menu and press <Enter> to access the following menu.

Please set application file download protocol parameter:

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

Enter your choice(0-3):2

**Step5** Enter 2 to select FTP and press <Enter>. The following information appears:

Please modify your FTP protocol parameter:

Load File name
Switch IP address
Server IP address
FTP User Name
FTP User Password

**Step6** Input correct information and press <Enter>. The following information appears:

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

**Step7** Enter Y to start downloading the files. Enter N to return to the Boot menu. Take the first case as an example. Enter Y and press <Enter>, and the system begins downloading programs. After downloading completes, the system starts writing the programs into the flash. Upon completion of this operation, the screen displays the following information to indicate that the downloading is completed:

Loading ........................................................done
Writing to flash................................................done!

Please input the file attribute (main/backup/none): main

Appendix

Modified password setup and display for password/key-related security features.
For security purposes, all passwords and keys, including those configured in plaintext, are stored in encrypted form.

### Details of Modified CLI Commands in V3.01.15

#### key (HWTACACS scheme view)

**Old syntax**

```
key { accounting | authentication | authorization } string
```

**New syntax**

```
key { accounting | authentication | authorization } [ cipher | simple ] string
```

**View**

HWTACACS scheme view

**Parameters**

- **accounting**: Sets the key for secure HWTACACS accounting communication.
- **authentication**: Sets the key for secure HWTACACS authentication communication.
- **authorization**: Sets the key for secure HWTACACS authorization communication.
- **cipher**: Sets a ciphertext key.
- **simple**: Sets a plaintext key.

**string**: Specifies the key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 117 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string.

**Change description**

Before modification: The **cipher** and **simple** keywords are not supported. The key for securing HWTACACS authentication, authorization, or accounting communication must be a plaintext string of 1 to 16 characters.

After modification: You can set a key in encrypted form or plaintext form to secure HWTACACS authentication, authorization, or accounting communication.

#### key (RADIUS scheme view)

**Old syntax**

```
key { accounting | authentication } string
```

**Note**
New syntax

    key { accounting | authentication } [ cipher | simple ] string

View

RADIUS scheme view

Parameters

    accounting: Sets the key for secure RADIUS accounting communication.
    authentication: Sets the key for secure RADIUS authentication/authorization communication.
    cipher: Sets a ciphertext key.
    simple: Sets a plaintext key.

    string: Specifies the key string. This argument is case sensitive. If simple is specified, it must be a string of 1 to 16 characters. If cipher is specified, it must be a ciphertext string of 1 to 53 characters. If neither cipher nor simple is specified, you set a plaintext key string.

Change description

Before modification: The cipher and simple keywords are not supported. The key for securing RADIUS authentication/authorization or accounting communication must be a plaintext string of 1 to 16 characters.

After modification: You can set a key in encrypted form or plaintext form to secure RADIUS authentication/authorization or accounting communication.

local-server nas-ip

Old syntax

    local-server nas-ip ip-address key password

New syntax

    local-server nas-ip ip-address key [ cipher | simple ] password

View

System view

Parameters

    nas-ip ip-address: Specifies the IP address of the network access server through which users can access the local RADIUS authentication/authorization server. The IP address must be in dotted decimal notation.
key [ cipher | simple ] password: Sets the key to share between the local RADIUS authentication/authorization server and the network access server.

- **cipher**: Sets a ciphertext key.
- **simple**: Sets a plaintext key.
- **password**: Specifies the key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string.

**Change description**

Before modification: The **cipher** and **simple** keywords are not supported. The key to share between the local RADIUS authentication/authorization server and the network access server must be a plaintext string of 1 to 16 characters.

After modification: You can set a key in encrypted form or plaintext form to share between the local RADIUS authentication/authorization server and the network access server.

**mac-authentication authmode usernameasmacaddress**

**Old syntax**

```
mac-authentication authmode usernameasmacaddress [ usernameformat { with-hyphen | without-hyphen } { lowercase | uppercase } ] fixedpassword password
```

**New syntax**

```
mac-authentication authmode usernameasmacaddress [ usernameformat { with-hyphen | without-hyphen } { lowercase | uppercase } ] fixedpassword [ cipher | simple ] password
```

**View**

System view

**Parameters**

- **usernameformat**: Specifies the username and password input format for MAC-based accounts.
- **with-hyphen**: Uses the hyphenated MAC address of a user, such as 00-05-e0-1c-02-e3, as the username and password for MAC authentication of the user.
- **without-hyphen**: Uses the unhyphenated MAC address of a user, such as 0005e01c02e3, as the username and password for MAC authentication of the user.
- **lowercase**: Enters letters of the MAC address in lower case.
- **uppercase**: Enters letters of the MAC address in upper case.
- **fixedpassword [ simple | cipher ] password**: Uses a fixed password, instead of user MAC addresses, for MAC authentication users.
  - **cipher**: Sets a ciphertext password.
  - **simple**: Sets a plaintext password.
password: Specifies the password string. This argument is case sensitive. If simple is specified, it must be a string of 1 to 63 characters. If cipher is specified, it must be a ciphertext string of 1 to 117 characters. If neither cipher nor simple is specified, you set a plaintext password.

Change description

Before modification: The cipher and simple keywords are not supported. The password you enter must be a plaintext string.

After modification: You can enter a password in encrypted form or plaintext form.

mac-authentication authpassword

Old syntax

mac-authentication authpassword password

New syntax

mac-authentication authpassword [ cipher | simple ] password

View

System view

Parameters

[ cipher | simple ] password: Sets the password of the shared account for MAC authentication users.

- cipher: Sets a ciphertext password.
- simple: Sets a plaintext password.
- password: Specifies the password string. This argument is case sensitive. If simple is specified, it must be a string of 1 to 63 characters. If cipher is specified, it must be a ciphertext string of 1 to 117 characters. If neither cipher nor simple is specified, you set a plaintext password.

Change description

Before modification: The cipher and simple keywords are not supported. The password you enter must be a plaintext string.

After modification: You can enter a password in encrypted form or plaintext form.

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
View

System view

Parameters

\texttt{keyid}: Specifies a key ID in the range of 10 to 4294967295.

\texttt{cipher}: Sets a ciphertext key.

\texttt{simple}: Sets a plaintext key.

\texttt{value}: Specifies the key string. This argument is case sensitive. If \texttt{simple} is specified, it must be a string of 1 to 32 characters. If \texttt{cipher} is specified, it must be a ciphertext string of 1 to 73 characters. If neither \texttt{cipher} nor \texttt{simple} is specified, you set a plaintext key string.

Change description

Before modification: The \texttt{cipher} and \texttt{simple} keywords are not supported. The key you enter must be a plaintext string of 1 to 32 characters.

After modification: You can enter a key in encrypted form or plaintext form.

\texttt{password (Remote-ping test group view )}

Old syntax

\texttt{password password}

New syntax

\texttt{password [ cipher | simple ] password}

View

Remote-ping test group view

Parameters

\texttt{cipher}: Sets a ciphertext FTP password.

\texttt{simple}: Sets a plaintext FTP password.

\texttt{password}: Specifies the password string. This argument is case sensitive. If \texttt{simple} is specified, it must be a string of 1 to 32 characters. If \texttt{cipher} is specified, it must be a ciphertext string of 1 to 73 characters. If neither \texttt{cipher} nor \texttt{simple} is specified, you set a plaintext password string.

Change description

Before modification: The \texttt{cipher} and \texttt{simple} keywords are not supported. The FTP password must be a plaintext string of 1 to 32 characters.

After modification: You can set an FTP password in encrypted form or plaintext form.
password (local user view)

Syntax

```
password [ { cipher | simple } password ]
```

View

Local user view

Parameters

- **cipher**: Sets a ciphertext password.
- **simple**: Sets a plaintext password.

`password`: Specifies the password string. This argument is case sensitive.

- If `simple` is specified, it is a plaintext string of 1 to 63 characters.
- If `cipher` is specified, it is a string of 1 to 117 characters. If you specify a password of 1 to 63 characters and the system can decrypt the password, the system considers that you have specified a ciphertext password. If you specify a password of 1 to 63 characters but the system cannot decrypt the password, the system considers that you have specified a plaintext password.

A password comprising 64 to 117 characters is always considered a ciphertext password.

Change description

Before modification: If `cipher` is specified, you can set an 88-character password or a password of 1 to 63 characters.

After modification: If `cipher` is specified, you can set a password of 1 to 117 characters.

primary accounting (RADIUS scheme view)

Old syntax

```
primary accounting { ip-address | ipv6 ipv6-address } [ port-number ] [ key string ]
```

New syntax

```
primary accounting { ip-address | ipv6 ipv6-address } [ port-number ] [ key [ cipher | simple ] string ]
```

View

RADIUS scheme view

Parameters

- **ip-address**: Specifies the IPv4 address of the primary RADIUS accounting server.
- **ipv6 ipv6-address**: Specifies the IPv6 address of the primary RADIUS accounting server.
port-number: Specifies the service port number of the primary RADIUS accounting server, a UDP port number in the range of 1 to 65535.

key [ cipher | simple ] string: Sets the key for secure communication with the primary RADIUS accounting server.

- cipher: Sets a ciphertext key.
- simple: Sets a plaintext key.
- string: Specifies the key string. This argument is case sensitive. If simple is specified, it must be a string of 1 to 16 characters. If cipher is specified, it must be a ciphertext string of 1 to 53 characters. If neither cipher nor simple is specified, you set a plaintext key string.

Change description

Before modification: The cipher and simple keywords are not supported. The key for securing communication with the primary RADIUS accounting server must be a plaintext string of 1 to 16 characters.

After modification: You can set a key in encrypted form or plaintext form to secure communication with the primary RADIUS accounting server.

primary authentication (RADIUS scheme view)

Old syntax

```
primary authentication { ip-address | ipv6 ipv6-address } [ port-number ] [ key string ]
```

New syntax

```
primary authentication { ip-address | ipv6 ipv6-address } [ port-number ] [ key [ cipher | simple ] string ]
```

View

RADIUS scheme view

Parameters

ip-address: Specifies the IPv4 address of the primary RADIUS authentication/authorization server.

ipv6 ipv6-address: Specifies the IPv6 address of the primary RADIUS authentication/authorization server.

port-number: Specifies the service port number of the primary RADIUS authentication/authorization server, a UDP port number in the range of 1 to 65535.

key [ cipher | simple ] string: Sets the key for secure communication with the primary RADIUS authentication/authorization server.

- cipher: Sets a ciphertext key.
- simple: Sets a plaintext key.
• **string**: Specifies the key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string.

**Change description**

Before modification: The **cipher** and **simple** keywords are not supported. The key for securing communication with the primary RADIUS authentication/authorization server must be a plaintext string of 1 to 16 characters.

After modification: You can set a key in encrypted form or plaintext form to secure communication with the primary RADIUS authentication/authorization server.

**secondary accounting (RADIUS scheme view)**

**Old syntax**

```
secondary accounting { ip-address | ipv6 ipv6-address } [ port-number ] [ key string ]
```

**New syntax**

```
secondary accounting { ip-address | ipv6 ipv6-address } [ port-number ] [ key [ cipher | simple ] string ]
```

**View**

RADIUS scheme view

**Parameters**

- **ip-address**: Specifies the IPv4 address of the secondary RADIUS accounting server.
- **ipv6 ipv6-address**: Specifies the IPv6 address of the secondary RADIUS accounting server.
- **port-number**: Specifies the service port number of the secondary RADIUS accounting server, a UDP port number in the range of 1 to 65535.
- **key [ cipher | simple ] string**: Sets the key for secure communication with the primary RADIUS accounting server.
  - **cipher**: Sets a ciphertext key.
  - **simple**: Sets a plaintext key.
  - **string**: Specifies the key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string.

**Change description**

Before modification: The **cipher** and **simple** keywords are not supported. The key for securing communication with the secondary RADIUS accounting server must be a plaintext string of 1 to 16 characters.
After modification: You can set a key in encrypted form or plaintext form to secure communication with the secondary RADIUS accounting server.

**secondary authentication (RADIUS scheme view)**

**Old syntax**

```plaintext
secondary authentication { ip-address | ipv6 ipv6-address } [ port-number ] [ key string ]
```

**New syntax**

```plaintext
secondary authentication { ip-address | ipv6 ipv6-address } [ port-number ] [ key [ cipher | simple ] string ]
```

**Parameters**

- `ip-address`: Specifies the IPv4 address of the secondary RADIUS authentication/authorization server.
- `ipv6 ipv6-address`: Specifies the IPv6 address of the secondary RADIUS authentication/authorization server.
- `port-number`: Specifies the service port number of the secondary RADIUS authentication/authorization server, a UDP port number in the range of 1 to 65535.
- `key [ cipher | simple ] string`: Sets the key for secure communication with the secondary RADIUS authentication/authorization server.
  - `cipher`: Sets a ciphertext key.
  - `simple`: Sets a plaintext key.
  - `string`: Specifies the key string. This argument is case sensitive. If `simple` is specified, it must be a string of 1 to 16 characters. If `cipher` is specified, it must be a ciphertext string of 1 to 53 characters. If neither `cipher` nor `simple` is specified, you set a plaintext key string.

**Change description**

Before modification: The `cipher` and `simple` keywords are not supported. The key for securing communication with the secondary RADIUS authentication/authorization server must be a plaintext string of 1 to 16 characters.

After modification: You can set a key in encrypted form or plaintext form to secure communication with the secondary RADIUS authentication/authorization server.

**set authentication password**

**Syntax**

```plaintext
set authentication password { simple | cipher } password
```
View

User interface view

Parameters

**cipher**: Sets a ciphertext password.

**simple**: Sets a plaintext password.

**key**: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a plaintext string of 1 to 16 characters. If **cipher** is specified, it can be a plaintext string of 1 to 16 characters or a ciphertext string of 17 to 53 characters.

Change description

Before modification: When you specify the **cipher** keyword, you can enter a string of 1 to 16 characters or a string of 24 characters as the password.

After modification: When you specify the **cipher** keyword, you can enter a string of 1 to 53 characters as the password.

```
snmp-agent usm-user v3
```

**Syntax**

```
snmp-agent usm-user v3 user-name group-name [ [ cipher ] authentication-mode { md5 | sha } auth-password [ privacy-mode { aes128 | des56 } priv-password ] ] [ acl acl-number ]
```

View

System view

Parameters

**user-name**: Specifies a username, a case-sensitive string of 1 to 32 characters.

**group-name**: Specifies a group name, a case-sensitive string of 1 to 32 characters.

**cipher**: Specifies that **auth-password** and **priv-password** are encrypted keys, which can be calculated to a hexadecimal string by using the **snmp-agent calculate-password** command. If this keyword is not specified, **auth-password** and **priv-password** are plaintext keys.

**authentication-mode**: Specifies an authentication algorithm. MD5 is faster but less secure than SHA. For more information about these algorithms, see Security Configuration Guide.

- **md5**: Specifies the MD5 authentication algorithm.
- **sha**: Specifies the SHA-1 authentication algorithm.

**auth-password**: Specifies a case-sensitive plaintext or encrypted authentication key. A plaintext key is a string of 1 to 64 visible characters. If the **cipher** keyword is specified, the encrypted authentication key length requirements differ by authentication algorithm and key string format, as shown in Table 9.
### Table 9 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>

**privacy-mode**: Specifies an encryption algorithm for privacy. The three encryption algorithms AES, 3DES, and DES are in descending order of security. Higher security means more complex implementation mechanism and lower speed. DES is enough to meet general requirements.

- **des56**: Specifies the DES algorithm.
- **aes128**: Specifies the AES algorithm.

**priv-password**: Specifies a case-sensitive plaintext or encrypted privacy key. A plaintext key is a string of 1 to 64 characters. If the **cipher** keyword is specified, the encrypted privacy key length requirements differ by authentication algorithm and key string format, as shown in Table 10.

### Table 10 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>AES128 or DES-56</td>
<td>32 characters</td>
<td>53 characters</td>
</tr>
<tr>
<td>SHA</td>
<td>AES128 or DES-56</td>
<td>40 characters</td>
<td>53 characters</td>
</tr>
</tbody>
</table>

**acl acl-number**: Specifies a basic ACL to filter NMSs by source IPv4 address. The **acl-number** argument represents a basic ACL number in the range of 2000 to 2999. Only the NMSs with the IPv4 addresses permitted in the ACL can use the specified username to access the SNMP agent.

**local**: Represents a local SNMP entity user.

**engineid engineid-string**: Specifies an SNMP engine ID as a hexadecimal string. The **engineid-string** argument must comprise an even number of hexadecimal characters, in the range of 10 to 64. All-zero and all-F strings are invalid.

### Change description

**Before modification**: Only authentication and privacy keys in hexadecimal format are supported.

**After modification**: Both hexadecimal and non-hexadecimal format authentication and privacy keys are supported.

- For encrypted authentication key length requirements, see Table 9.
- For encrypted privacy key length requirements, see Table 10.

### super password

**Syntax**

```
super password [ level user-level ] { cipher | simple } password
```

**Views**

System view
Parameters

- **level user-level**: Specifies a user privilege level in the range of 1 to 3. The default is 3.
- **cipher**: Sets a ciphertext password.
- **simple**: Sets a plaintext password.
- **key**: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a plaintext string of 1 to 16 characters. If **cipher** is specified, it can be a plaintext string of 1 to 16 characters or a ciphertext string of 17 to 53 characters.

Change description

Before modification: When you specify the **cipher** keyword, you can enter a string of 1 to 16 characters or a string of 24 characters as the password.

After modification: When you specify the **cipher** keyword, you can enter a string of 1 to 53 characters as the password.

Details of Added CLI Commands in V3.01.13

dot1x mandatory-domain

Syntax

```
  dot1x mandatory-domain domain-name
  undo dot1x mandatory-domain
```

View

- Ethernet Interface view

Parameters

- **domain-name**: ISP domain name, a case-insensitive string of 1 to 128 characters.

Description

Use the **dot1x mandatory-domain** command to specify the mandatory authentication domain for users accessing the port.

Use the **undo dot1x mandatory-domain** command to remove the mandatory authentication domain.

By default, no mandatory authentication domain is specified.

Note that:

- When authenticating an 802.1X user trying to access the port, the system selects an authentication domain in the following order: the mandatory domain, the ISP domain specified in the username, and the default ISP domain.
- The specified mandatory authentication domain must exist.
Examples

# Configure the mandatory authentication domain my-domain for 802.1X users on Ethernet 1/0/1.
<Sysname> system-view
[Sysname] interface ethernet 1/0/1
[Sysname-Ethernet1/0/1] dot1x mandatory-domain my-domain

accounting lan-access

Syntax

accounting lan-access { local | none | radius-scheme radius-scheme-name [ local | none ] }
undo accounting lan-access

View

ISP domain view

Parameters

local: Performs local accounting. It is not used for charging purposes, but for collecting statistics and limiting the number of local user connections.

none: Does not perform any accounting.

radius-scheme radius-scheme-name: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description

Use the accounting lan-access command to configure the accounting method for LAN access users.

Use the undo accounting lan-access command to restore the default.

By default, the default accounting method that the accounting command prescribes is used for LAN access users.

Note that the RADIUS scheme specified for the current ISP domain must have been configured.

Related commands: accounting, radius scheme.

Examples

# Configure the default ISP domain system to use the local accounting method for LAN access users.
<Sysname> system-view
[Sysname] domain system
[Sysname-system] accounting lan-access local

# Configure ISP domain test to use RADIUS accounting scheme rd for LAN access users and use local accounting as the backup.
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting lan-access radius-scheme rd local

accounting login

Syntax

```
accounting login { hwtacacs-scheme hwtacacs-scheme-name [ local ] | local | none | radius-scheme radius-scheme-name [ local ] }
```

undo accounting login

View

ISP domain view

Parameters

- **hwtacacs-scheme hwtacacs-scheme-name**: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.
- **local**: Performs local accounting. It is not used for charging purposes, but for collecting statistics and limiting the number of local user connections.
- **none**: Does not perform any accounting.
- **radius-scheme radius-scheme-name**: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description

Use the **accounting login** command to configure the accounting method for login users.

Use the **undo accounting login** command to restore the default.

By default, the default accounting method is used for login users.

Note that the RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.

Related commands: **accounting**, **hwtacacs scheme**, **radius scheme**.

Examples

```
# Configure the default ISP domain system to use the local accounting method for login users.
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting login local

# Configure ISP domain test to use RADIUS accounting scheme rd for login users and use local accounting as the backup.
<Sysname> system-view
[Sysname] domain test
```
authentication lan-access

Syntax

```
authentication lan-access { local | none | radius-scheme radius-scheme-name [ local | none ] }
undo authentication lan-access
```

View

ISP domain view

Parameters

- **local**: Performs local authentication.
- **none**: Does not perform any authentication.
- **radius-scheme radius-scheme-name**: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description

Use the `authentication lan-access` command to configure the authentication method for LAN access users.

Use the `undo authentication lan-access` command to restore the default.

By default, the default authentication method is used for LAN access users.

Note that the RADIUS scheme specified for the current ISP domain must have been configured.

Related commands: `authentication`, `radius scheme`.

Examples

```
# Configure the default ISP domain `system` to use local authentication for LAN access users.
<Sysname> system-view
<Sysname> domain system
<Sysname-isp-system> authentication lan-access local

# Configure ISP domain `test` to use RADIUS authentication scheme `rd` for LAN access users and use local authentication as the backup.
<Sysname> system-view
<Sysname> domain test
<Sysname-isp-test> authentication lan-access radius-scheme rd local
```
**authentication login**

**Syntax**

```plaintext
authentication login { hwtacacs-scheme hwtacacs-scheme-name [ local ] | local | none | radius-scheme radius-scheme-name [ local ] }
```

```plaintext
undo authentication login
```

**View**

ISP domain view

**Parameters**

- **hwtacacs-scheme hwtacacs-scheme-name**: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.
- **local**: Performs local authentication.
- **none**: Does not perform any authentication.
- **radius-scheme radius-scheme-name**: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

**Description**

Use the `authentication login` command to configure the authentication method for login users.

Use the `undo authentication login` command to restore the default.

By default, the default authentication method is used for login users.

Note that the RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.

Related commands: `authentication`, `hwtacacs scheme`, `radius scheme`.

**Examples**

```
# Configure the default ISP domain system to use local authentication for login users.
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication login local

# Configure ISP domain test to use RADIUS authentication scheme rd for login users and use local authentication as the backup.
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication login radius-scheme rd local
```
authorization login

Syntax

```plaintext
authorization login { hwtacacs-scheme hwtacacs-scheme-name [ local ] [ local | none ] }
undo authorization login
```

View

ISP domain view

Parameters

- **hwtacacs-scheme hwtacacs-scheme-name**: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.
- **local**: Performs local authorization.
- **none**: Does not perform any authorization. In this case, an authenticated user is automatically authorized with the default rights.

Description

Use the `authorization login` command to configure the authorization method for login users.

Use the `undo authorization login` command to restore the default.

By default, the default authorization method is used for login users.

Note that the HWTACACS scheme specified for the current ISP domain must have been configured.

Related commands: `authorization`, `hwtacacs scheme`, `radius scheme`.

Examples

```
# Configure the default ISP domain system to use local authorization for login users.
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization login local

# Configure ISP domain test to use HWTACACS authorization scheme hwt for login users and use local authorization as the backup.
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization login hwtacacs-scheme hwt local
```

scheme lan-access

Syntax

```plaintext
scheme lan-access { local | none | radius-scheme radius-scheme-name [ local | none ] }
```

December 20, 2012
undo scheme lan-access

View

ISP domain view

Parameters

radius-scheme-name: Name of a RADIUS scheme, a string of up to 32 characters.
local: Specifies to use local authentication.
none: Specifies not to perform authentication.

Description

Use the scheme lan-access command to configure a combined AAA scheme for LAN users.

Use the undo scheme lan-access command to restore the default.

By default, the local AAA scheme is used.

Note that:

- When you use the scheme lan-access command to reference a RADIUS scheme in the current ISP domain, the referenced RADIUS scheme must already exist.
- If you use the scheme lan-access radius-scheme radius-scheme-name local command, the local scheme is used as the secondary scheme in case no RADIUS server is available. That is, if the communication between the switch and a RADIUS server is normal, remote authentication is performed; otherwise, local authentication is performed.
- If you execute the scheme lan-access local or scheme lan-access none command to use local or none as the primary scheme, local authentication is performed or no authentication is performed. In this case, no secondary scheme can be specified and therefore no scheme switching will occur.

Related commands: scheme, display domain.

Examples

# Configure ISP domain aabbcc.net to use RADIUS scheme radius1 for LAN users and use local authentication as the backup.

<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] domain aabbcc.net
New Domain added.
[Sysname-isp-aabbcc.net] scheme lan-access radius-scheme radius1 local
scheme login

Syntax

```
scheme login { local | none | radius-scheme radius-scheme-name [ local ] | hwtacacs-scheme hwtacacs-scheme-name [ local ] }
```

```
undo scheme login
```

View

ISP domain view

Parameters

radius-scheme-name: Name of a RADIUS scheme, a string of up to 32 characters.

local: Specifies to use local authentication.

none: Specifies not to perform authentication.

hwtacacs-scheme-name: Name of an HWTACACS scheme, a string of up to 32 characters.

Description

Use the `scheme login` command to configure a combined AAA scheme for login users.

Use the `undo scheme login` command to restore the default.

By default, the local AAA scheme is used.

Note that:

- When you use the `scheme login` command to reference a RADIUS scheme in the current ISP domain, the referenced RADIUS scheme must already exist.
- If you use the `scheme login radius-scheme radius-scheme-name local` command, the local scheme is used as the secondary scheme in case no RADIUS server is available. That is, if the communication between the switch and a RADIUS server is normal, remote authentication is performed; otherwise, local authentication is performed.
- If you execute the `scheme login hwtacacs-scheme hwtacacs-scheme-name local` command, the local scheme is used as the secondary scheme in case no TACACS server is available. That is, if the communication between the switch and a TACACS server is normal, remote authentication is performed; if the TACACS server is not reachable or there is a key error, NAS IP error, or authentication failure, local authentication is performed.
- If you execute the `scheme login local` or `scheme login none` command to use `local` or `none` as the primary scheme, local authentication is performed or no authentication is performed. In this case, no secondary scheme can be specified and therefore no scheme switching will occur.

Related commands: `scheme`.
Examples

# Configure the default ISP domain system to use RADIUS scheme radius1 for login users and use local authentication as the backup.

```plaintext
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] domain system
[Sysname-isp-aabbcc.net] scheme login radius-scheme radius1 local
```

**primary accounting**

**Syntax**

```plaintext
primary accounting { ip-address | ipv6 ipv6-address } [ port-number ] [ key string ]
undo primary accounting
```

**View**

RADIUS scheme view

**Parameters**

- `ip-address`: IP address of the primary accounting server to be used, in dotted decimal notation.
- `ipv6 ipv6-address`: IPv6 address of the primary accounting server.
- `port-number`: UDP port number of the primary accounting server, ranging from 1 to 65535.
- `key string`: Specifies the shared key for exchanging accounting packets with the primary RADIUS accounting server. A shared key is a case-sensitive string of 1 to 16 characters.

**Description**

Use the `primary accounting` command to set the IP address, port number and shared key of the primary RADIUS accounting server to be used by the current scheme.

Use the `undo primary accounting` command to restore the default IP address and port number of the primary RADIUS accounting server, which are 0.0.0.0 and 1813 respectively.

In the system default RADIUS scheme “system”, the default IP address of the primary accounting server is 127.0.0.1 and the default UDP port number is 1646. In a new RADIUS scheme, the default IP address of the primary accounting server is 0.0.0.0 and the default UDP port number is 1813.

Note that:

- You can configure a shared key for the primary accounting server by specifying `key string` in this command. The shared key configured in this command is used in preference. If `key string` is not configured here, the shared key configured in the `key` command in RADIUS scheme view will be used.
- The IP addresses of the primary and secondary accounting servers cannot be the same. Otherwise, the configuration fails.
Related commands: key, radius scheme, state.

Examples

# Set the IP address and UDP port number of the primary accounting server for RADIUS scheme radius1 to 10.110.1.2 and 1813 respectively.

<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
New Radius scheme
[Sysname-radius-radius1] primary accounting 10.110.1.2 1813

# Specify the IP address of the primary accounting server for RADIUS scheme radius1 as 10.110.1.2, the UDP port of the server as 1813, and the shared key of accounting packets as key1.

<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary accounting 10.110.1.2 1813 key1

primary authentication

Syntax

primary authentication { ip-address | ipv6 ipv6-address } [ port-number ] [ key string ]

undo primary authentication

View

RADIUS scheme view

Parameters

ip-address: IP address of the primary authentication/authorization server to be used, in dotted decimal notation.

ipv6 ipv6-address: IPv6 address of the primary authentication/authorization server.

port-number: UDP port number of the primary authentication/authorization server, ranging from 1 to 65535.

key string: Specifies the shared key for exchanging authentication and authorization packets with the primary RADIUS authentication/authorization server. A shared key is a case-sensitive string of 1 to 16 characters.

Description

Use the primary authentication command to set the IP address, port number and shared key of the primary RADIUS authentication/authorization server used by the current RADIUS scheme.

Use the undo primary authentication command to restore the default IP address and port number of the primary RADIUS authentication/authorization server, which are 0.0.0.0 and 1812 respectively.
In the system default RADIUS scheme “system”, the default IP address of the primary authentication/authorization server is 127.0.0.1 and the default UDP port number is 1645. In a new RADIUS scheme, the default IP address of the primary authentication/authorization server is 0.0.0.0 and the default UDP port number is 1812.

Note that:

- After creating a new RADIUS scheme, you should configure the IP address and UDP port number of each RADIUS server you want to use in this scheme. These RADIUS servers fall into two types: authentication/authorization, and accounting. For each kind of server, you can configure two servers in a RADIUS scheme: primary and secondary servers.
- In an actual network environment, you can make RADIUS server-related configuration as required. But you should configure at least one authentication/authorization server and one accounting server, and at the same time, you should keep the RADIUS server port settings on the switch consistent with those on the RADIUS servers.
- You can configure a shared key for the primary authentication/authorization server by specifying `key string` in this command. The shared key configured in this command is used in preference. If `key string` is not configured here, the shared key configured in the `key` command in RADIUS scheme view will be used.
- The IP addresses of the primary and secondary authentication/authorization servers cannot be the same. Otherwise, the configuration fails.

Related commands: `key`, `radius scheme`, `state`.

**Examples**

```bash
# Set the IP address and UDP port number of the primary authentication/authorization server for RADIUS scheme radius1 to 10.110.1.1 and 1812 respectively.
<Sysname> system-view
System View: return to User View with Ctrl+Z.
<Sysname] radius scheme radius1
New Radius scheme
[Sysname-radius-radius1] primary authentication 10.110.1.1 1812

# Specify the IPv6 address of the primary authentication/authorization server for RADIUS scheme radius1 as 1:1::2:3 and the UDP port of the server as 1812.
<Sysname> system-view
<Sysname] radius scheme radius1
[Sysname-radius-radius1] primary authentication ipv6 1:1::2:3 1812
```

**secondary accounting**

**Syntax**

```bash
secondary accounting { ip-address | ipv6 ipv6-address } [ port-number ] [ key string ]

undo secondary accounting
```
View

RADIUS scheme view

Parameters

ip-address: IP address of the secondary accounting server to be used, in dotted decimal notation.

ipv6 ipv6-address: IPv6 address of the secondary accounting server.

port-number: UDP port number of the secondary accounting server, ranging from 1 to 65535.

key string: Specifies the shared key for exchanging accounting packets with the secondary RADIUS accounting server. A shared key is a case-sensitive string of 1 to 16 characters.

Description

Use the secondary accounting command to set the IP address, port number and shared key of the secondary RADIUS accounting server to be used by the current scheme.

Use the undo secondary accounting command to restore the default IP address and port number of the secondary RADIUS accounting server, which are 0.0.0.0 and 1813 respectively.

Note that:

- Up to 16 secondary accounting servers are supported in a RADIUS scheme.
- You can configure a shared key for the secondary accounting server by specifying key string in this command. The shared key configured in this command is used in preference. If key string is not configured here, the shared key configured in the key command in RADIUS scheme view will be used.
- The IP addresses of the primary and secondary accounting servers cannot be the same. Otherwise, the configuration fails.

Related commands: key, radius scheme, state.

Examples

# Set the IP address and UDP port number of the secondary accounting server for RADIUS scheme radius1 to 10.110.1.1 and 1813 respectively.

<Sysname> system-view
System View: return to User View with Ctrl+Z.

[Sysname] radius scheme radius1
New Radius scheme

[Sysname-radius-radius1] secondary accounting 10.110.1.1 1813

secondary authentication

Syntax

secondary authentication { ip-address | ipv6 ipv6-address } [ port-number ] [ key string ]

undo secondary authentication
View

RADIUS scheme view

Parameters

*ip-address*: IP address of the secondary authentication/authorization server to be used, in dotted decimal notation.

*ipv6 ipv6-address*: IPv6 address of the secondary authentication/authorization server.

*port-number*: UDP port number of the secondary authentication/authorization server, ranging from 1 to 65535.

*key* *string*: Specifies the shared key for exchanging authentication/authorization packets with the secondary RADIUS authentication/authorization server. A shared key is a case-sensitive string of 1 to 16 characters.

Description

Use the `secondary authentication` command to set the IP address, port number and shared key of the secondary RADIUS authentication/authorization server to be used by the current scheme.

Use the `undo secondary authentication` command to restore the default IP address and port number of the secondary RADIUS authentication/authorization server, which is 0.0.0.0 and 1812 respectively.

Note that:

- Up to 16 secondary authentication/authorization servers are supported in a RADIUS scheme.
- You can configure a shared key for the secondary authentication/authorization server by specifying `key string` in this command. The shared key configured in this command is used in preference. If `key string` is not configured here, the shared key configured in the `key` command in RADIUS scheme view will be used.
- The IP addresses of the primary and secondary authentication/authorization servers cannot be the same. Otherwise, the configuration fails.

Related commands: `key`, `radius scheme`, `state`.

Examples

```
# Set the IP address and UDP port number of the secondary authentication/authorization server for RADIUS scheme radius1 to 10.110.1.2 and 1812 respectively.
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
New Radius scheme
[Sysname-radius-radius1] secondary authentication 10.110.1.2 1812
```
state primary

Syntax

state primary { accounting | authentication } { block | active }

View

RADIUS scheme view

Parameters

primary: Specifies that the server to be set is a primary RADIUS server.
accounting: Specifies that the server to be set is a RADIUS accounting server.
authentication: Specifies that the server to be set is a RADIUS authentication/authorization server.
block: Sets the status of the specified RADIUS server to block (that is, the down state).
active: Sets the status of the specified RADIUS server to active (that is, the normal working state).

Description

Use the state primary command to set the status of a primary RADIUS server.

By default, all RADIUS servers in any customized RADIUS scheme are in the block state; the primary RADIUS servers in the default RADIUS scheme "system" are in the active state.

For the primary and secondary servers (authentication/authorization servers, or accounting servers) in a RADIUS scheme, note that:

- When the switch fails to communicate with the primary server due to some server trouble, the switch will turn to the secondary server and exchange messages with the secondary server.
- After the primary server remains in the block state for a set time (set by the timer quiet command), the switch will try to communicate with the primary server again when it receives a RADIUS request. If it finds that the primary server has recovered, the switch immediately restores the communication with the primary server instead of communicating with the secondary server, and at the same time restores the status of the primary server to active while keeping the status of the secondary server unchanged.
- When both primary and secondary servers are in the active or block state, the switch sends messages only to the primary server.

Related commands: radius scheme, primary authentication, secondary authentication, primary accounting, secondary accounting.

Examples

# Set the status of the secondary authentication server in RADIUS scheme radius1 to active.

<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
New Radius scheme

[Sysname-radius-radius1] state secondary authentication active

**state secondary**

**Syntax**

```
state secondary { accounting | authentication } { ip-address | ipv6 ipv6-address } { active | block }
```

**View**

RADIUS scheme view

**Parameters**

- **secondary**: Sets the status of the secondary RADIUS server.
- **accounting**: Sets the status of the RADIUS accounting server.
- **authentication**: Sets the status of the RADIUS authentication/authorization server.
- **ip-address**: IP address of the secondary RADIUS server.
- **ipv6 ipv6-address**: IPv6 address of the secondary RADIUS server.
- **active**: Sets the status of the RADIUS server to **active**, namely the normal operation state.
- **block**: Sets the status of the RADIUS server to **block**.

**Description**

Use the **state secondary** command to set the status of the secondary RADIUS server.

By default, in the default RADIUS scheme **system**, the primary RADIUS server is in **active** state and the secondary RADIUS server is in **block** state; in other RADIUS schemes, all servers are in **block** state.

**Examples**

```bash
# Set the status of the secondary accounting server with IPv6 address 1:1::2:5 to block.
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
New Radius scheme
[Sysname-radius-radius1] state secondary accounting ipv6 1:1::2:5 block
```
cut connection

Syntax

```
cut connection { all | access-type { dot1x | mac-authentication } | domain isp-name | interface
interface-type interface-number | ip ip-address | ipv6 ipv6-address | mac mac-address | radius-
scheme radius-scheme-name | vlan vlan-id | ucibindex ucib-index | user-name user-name }
```

View

System view

Parameters

all: Cuts down all user connections.

access-type { dot1x | mac-authentication }: Cuts down user connections of a specified access type. dot1x is used to cut down all 802.1x user connections, and mac-authentication is used to cut down all MAC authentication user connections.

domain isp-name: Cuts down all user connections in a specified ISP domain. Here, isp-name is the name of an ISP domain, a string of up to 128 characters. You can only specify an existing ISP domain.

interface interface-type interface-number: Cuts down all user connections under a specified port. Here, interface-type is a port type and interface-number is a port number.

ip ip-address: Cuts down all user connections with a specified IP address.

ipv6 ipv6-address: Cuts down all user connections with a specified IPv6 address.

mac mac-address: Cuts down the user connection with a specified MAC address. Here, mac-address is in H-H-H format.

radius-scheme radius-scheme-name: Cuts down all user connections using a specified RADIUS scheme. Here, radius-scheme-name is a string of up to 32 characters.

vlan vlan-id: Cuts down all user connections of a specified VLAN. Here, vlan-id ranges from 1 to 4094.

ucibindex ucib-index: Cuts down the user connection with a specified connection index. Here, ucib-index ranges from 0 to 1047.

user-name user-name: Cuts down the connection of a specified user. Here, user-name is a string of up to 184 characters.

Description

Use the cut connection command to forcibly cut down one user connection, one type of user connections, or all user connections.

This command cannot cut down the connections of Telnet and FTP users.

Related commands: display connection.
Examples

# Cut down all user connections under the ISP domain aabbcc.net.
<Sysname> system-view
System View: return to User View with Ctrl+Z.
<Sysname> cut connection domain aabbcc.net

display connection

Syntax

display connection [ access-type { dot1x | mac-authentication } | domain isp-name | interface interface-type interface-number | ip ip-address | ipv6 ipv6-address | mac mac-address | radius-scheme radius-scheme-name | hwtacacs-scheme hwtacacs-scheme-name | vlan vlan-id | ucibindex ucib-index | user-name user-name ]

View

Any view

Parameters

access-type { dot1x | mac-authentication }: Displays user connections of a specified access type. Here, dot1x is used to display all 802.1x user connections, and mac-authentication is used to display all MAC authentication user connections.

domain isp-name: Displays all user connections under specified ISP domain. Here, isp-name is the name of an ISP domain, a string of up to 128 characters. You can only specify an existing ISP domain.

interface interface-type interface-number: Displays all user connections on a specified port.

ip ip-address: Displays all user connections with a specified IP address.

ipv6 ipv6-address: Displays all user connections with a specified IPv6 address.

mac mac-address: Displays the user connection with a specified MAC address. Here, mac-address is in hexadecimal format (in the form of H-H-H).

radius-scheme radius-scheme-name: Displays all user connections using a specified RADIUS scheme. Here, radius-scheme-name is a string of up to 32 characters.

hwtacacs-scheme hwtacacs-scheme-name: Displays all user connections using a specified RADIUS scheme. Here, hwtacacs-scheme-name is a string of up to 32 characters.

vlan vlan-id: Displays all user connections of a specified VLAN. Here, vlan-id ranges from 1 to 4094.

ucibindex ucib-index: Displays the user connection with a specified connection index. Here, ucib-index ranges from 0 to 1047.

user-name user-name: Displays the connection of a specified user. Here, user-name is a character string in the format of pure-username@domain-name. The pure-username cannot be longer than 55
characters, the domain-name cannot be longer than 24 characters, and the entire user-name cannot be longer than 184 characters.

**Description**

Use the `display connection` command to display information about specified or all user connections.

If you execute this command without specifying any parameter, all user connections will be displayed.

This command cannot display information about the connections of FTP users.

Related commands: `cut connection`.

**Examples**

```plaintext
# Display information about all user connections.
<Sysname> display connection
------------------unit 1------------------------
Index=40 , Username=user1@domain1
MAC=000f-3d80-4ce5  , IP=0.0.0.0
  On Unit 1: Total 1 connections matched, 1 listed.

# Display information about the user connection with index 0.
[Sysname] display connection ucibindex 0
Index=0   , Username=user1@system
MAC=000f-3d80-4ce5   , IP=192.168.0.3
  Access=8021X   ,Auth=CHAP   ,Port=Ether   ,Port NO=0x10003001
  Initial VLAN=1, Authorization VLAN=1
  ACL Group=Disable
  CAR=Disable
  Priority=Disable
  Start=2000-04-03 02:51:53 ,Current=2000-04-03 02:52:22 ,Online=00h00m29s
  On Unit 1:Total 1 connections matched, 1 listed.
  Total 1 connections matched, 1 listed.

Here, Port NO=0x10003001 means (by the binary bits):

| Table 11 Description of the Port NO field |
|------------------|------------------|------------------|------------------|------------------|------------------|
| 31 to 28 bit  | 27 to 24 bit  | 23 to 20 bit  | 19 to 12 bit  | 11 to 0 bit  | VLAN ID |
| UNIT ID  | Slot number  | Sub-slot number  | Port number  | VLAN ID  |
```

**nas-ip**

**Syntax**

```
nas-ip { ip-address | ipv6 ipv6-address }
undo nas-ip
```
View

RADIUS scheme view

Parameters

`ip-address`: Source IP address for RADIUS messages, an IP address of this device. This address can neither be the all 0's address nor be a Class-D address.

`ipv6 ipv6-address`: Specifies an IPv6 address. It must be an address of the device and must be a unicast address that is neither a loopback one nor a link-local one.

Description

Use the `nas-ip` command to set the source IP address of outgoing RADIUS messages.

Use the `undo nas-ip` command to remove the source IP address setting.

By default, the IP address of the outbound interface is used as the source IP address of RADIUS messages.

Note

The `nas-ip` command in RADIUS scheme view has the same function as the `radius nas-ip` command in system view; and the configuration in RADIUS scheme view takes precedence over that in system view.

You can set the source IP address of outgoing RADIUS messages to avoid messages returned from RADIUS server from being unable to reach their destination due to physical interface trouble. It is recommended to use a Loopback interface address as the source IP address.

Related commands: `display radius scheme`, `radius nas-ip`.

Examples

```
# Set source IP address 10.1.1.1 for outgoing RADIUS messages in RADIUS scheme radius1.
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
New Radius scheme
[Sysname-radius-radius1] nas-ip 10.1.1.1

# Set the IPv6 address for the device to use as the source address of the RADIUS packets to 1:1::2:2.
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] radius scheme radius1
```
radius nas-ip

Syntax

    radius nas-ip { ip-address | ipv6 ipv6-address }

    undo radius nas-ip

View

    System view

Parameters

    ip-address: Source IP address to be set, an IP address of this device. This address can neither be the all 0's address nor be a Class-D address.
    ipv6 ipv6-address: Specifies an IPv6 address. It must be an address of the device and must be a unicast address that is neither a loopback one nor a link-local one.

Description

    Use the radius nas-ip command to set the source IP address of outgoing RADIUS messages.
    Use the undo radius nas-ip command to restore the default setting.
    By default, no source IP address is set, and the IP address of corresponding outbound interface is used as the source IP address of RADIUS messages.

Note

    The nas-ip command in RADIUS scheme view has the same function as the radius nas-ip command in system view; and the configuration in RADIUS scheme view takes precedence over that in system view.

    Note that:
    - You can set the source IP address of outgoing RADIUS messages to avoid messages returned from RADIUS server from being unable to reach their destination due to physical interface trouble. It is recommended to use a Loopback interface address as the source IP address.
    - You can set only one source IP address by using this command. When you re-execute this command again, the newly set source IP address will overwrite the old one.
Related commands: \texttt{nas-ip}.

\textbf{Examples}

\begin{verbatim}
# Set source address 129.10.10.1 for outgoing RADIUS messages.
<Sysname> system-view
System View: return to User View with Ctrl+Z.
<Sysname> radius nas-ip 129.10.10.1

# Set the IPv6 address for the device to use as the source address of the RADIUS packets to 1:1::2:2.
<Sysname> system-view
<Sysname> radius nas-ip ipv6 1:1::2:2
\end{verbatim}

\textbf{port-security timer autolearn}

\textbf{Syntax}

\begin{verbatim}
port-security timer autolearn \textit{age}
undo port-security timer autolearn
\end{verbatim}

\textbf{View}

System view

\textbf{Parameters}

\textit{age}: Aging time of the security MAC address entries, in the range 1 to 30240 minutes.

\textbf{Description}

Use the \texttt{port-security timer autolearn} command to configure the aging time for the security MAC address entries that are learned by the port automatically.

Use the \texttt{undo port-security timer autolearn} command to restore the default.

By default, the aging time is 0, that is, the security MAC address entries are not aged.

\begin{verbatim}

\begin{itemize}
  \item \texttt{Note}
\end{itemize}

After you execute the \texttt{port-security timer autolearn} command, you can display security MAC address entries by the \texttt{display mac-address security} command. Though the aging time field displayed has a value of "NOAGED", the aging of security MAC address entries is enabled already.
\end{verbatim}


Examples

# Set the security mode to autolearn, the maximum number of MAC address entries allowed on the port to 4, and the aging time for the learned security MAC address entries to 10 minutes.

<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] port-security timer autolearn 10
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] port-security max-mac-count 4
[Sysname-Ethernet1/0/1] port-security port-mode autolearn