



Switch 5500G V3.03.02p18 Release Notes

Keywords: resolved problems, software upgrading

Abstract: *This release notes describes the **Switch 5500G V3.03.02p18** release with respect to hardware and software compatibility, released features and functions, resolved problems, software upgrading, and related documentation.*

Acronyms:

Abbreviations	Full spelling
ACL	Access Control List
CLI	Command line interface
DHCP	Dynamic Host Configuration Protocol
FTP	File Transfer Protocol
GARP	Generic Attribute Registration Protocol
GVRP	GARP VLAN Registration Protocol
HGMP	Huawei Group Management Protocol
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocol
LACP	Link Aggregation Control Protocol
MIB	Management Information Base
MSTP	Multiple Spanning Tree Protocol
NDP	Neighbor Discovery Protocol
NTP	Net Time Protocol
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RMON	Remote monitoring
RSTP	Rapid Spanning Tree Protocol
SNMP	Simple Network Management Protocol
SP	Strict priority
SSH	Secure Shell



Abbreviations	Full spelling
STP	Spanning Tree Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
3ND	3Com network director

Table of Contents

Version Information.....	6
Version Number	6
Version History.....	6
Hardware and Software Compatibility Matrix.....	7
Restrictions and Cautions	8
Feature List	9
Hardware Features	9
Software Features.....	10
Version Updates	14
Feature Updates	14
Command Line Updates	18
MIB Updates	38
Configuration Changes	40
V3.03.02p18 Operation Changes.....	40
V3.03.02p16 Operation Changes.....	40
V3.03.02p15 Operation Changes.....	41
V3.03.02p14 Operation Changes.....	41
V3.03.02p13 Operation Changes.....	41
V3.03.02p12 Operation Changes.....	41
V3.03.02p11 Operation Changes.....	41
V3.03.02p07 Operation Changes.....	41
V3.03.02p05 Operation Changes.....	42
V3.03.02p04 Operation Changes.....	42
V3.03.02p03 Operation Changes.....	42
V3.03.02p01 Operation Changes.....	43
V3.03.02 Operation Changes.....	44
V3.03.01p05 Operation Changes.....	44
V3.03.01p03 Operation Changes.....	44
V3.03.01p01 Operation Changes.....	45
V3.03.00 Operation Changes.....	45
Open Problems and Workarounds	46
List of Resolved Problems	48
Resolved Problems in V3.03.02p18.....	48
Resolved Problems in V3.03.02p16.....	48
Resolved Problems in V3.03.02p15.....	49
Resolved Problems in V3.03.02p14.....	50
Resolved Problems in V3.03.02p13.....	51
Resolved Problems in V3.03.02p12.....	52
Resolved Problems in V3.03.02p11.....	52

Resolved Problems in V3.03.02p07.....	56
Resolved Problems in V3.03.02p05.....	61
Resolved Problems in V3.03.02p04.....	62
Resolved Problems in V3.03.02p03.....	64
Resolved Problems in V3.03.02p01.....	67
Resolved Problems in V3.03.02.....	72
Resolved Problems in V3.03.01p05.....	72
Resolved Problems in V3.03.01p04.....	75
Resolved Problems in V3.03.01p03.....	77
Resolved Problems in V3.03.01p01.....	82
Resolved Problems in V3.03.00.....	87
Related Documentation.....	87
Software Upgrading.....	88
Remote Upgrading through CLI	88
Boot Menu	89
Software Upgrading via Console Port (Xmodem Protocol).....	90
Software Upgrading via Ethernet Interface (FTP/TFTP).....	92
Software Upgrading via TFTP	92
Software Upgrading via FTP	93

List of Tables

Table 1 Version history 6

Table 2 Compatibility matrix..... 7

Table 3 Hardware features 9

Table 4 Software features..... 10

Table 5 Feature updates..... 14

Table 6 Command line updates..... 18

Table 7 MIB updates..... 38

Version Information

Version Number

Version Information: 3Com OS V3.03.02s168p18

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

Version History

Table 1 Version history

Version number	Last version	Release date	Remarks
V3.03.02s168p18	V3.03.02s168p16	2011-06-21	None
V3.03.02s168p16	V3.03.02s168p15	2011-03-14	None
V3.03.02s168p15	V3.03.02s168p14	2010-12-16	None
V3.03.02s168p14	V3.03.02s168p13	2010-10-21	None
V3.03.02s168p13	V3.03.02s168p12	2010-09-13	None
V3.03.02s168p12	V3.03.02s168p11	2010-07-25	None
V3.03.02s168p11	V3.03.02s168p07	2010-06-21	None
V3.03.02s168p07	V3.03.02s56p05 V3.03.02s168p05	2010-01-26	From the version, only release the APP of 168-bit encryption for SSH.
V3.03.02s56p05	V3.03.02s56p04	2009-10-23	None
V3.03.02s168p05	V3.03.02s168p04		
V3.03.02s56p04	V3.03.02s56p03	2009-08-19	None
V3.03.02s168p04	V3.03.02s168p03		
V3.03.02s56fp04	V3.03.02s56fp02	2009-08-19	None
V3.03.02s168fp04	V3.03.02s168fp02		
V3.03.02s56p03	V3.03.02s56p01	2009-06-18	None
V3.03.02s168p03	V3.03.02s168p01		
V3.03.02s56fp02	V3.03.02s56f	2009-04-28	None
V3.03.02s168fp02	V3.03.02s168f		
V3.03.02s56p01	V3.03.02s56	2009-03-13	None
V3.03.02s168p01	V3.03.02s168		
V3.03.02s56	V3.03.01s56p05	2008-10-31	New features released
V3.03.02s168	V3.03.01s168p05		
V3.03.02s56f	None	2008-11-05	First release, supporting OSM module.
V3.03.02s168f			
V3.03.01s56p05	V3.03.01s56p04	2008-07-18	None
V3.03.01s168p05	V3.03.01s168p04		

Version number	Last version	Release date	Remarks
V3.03.01s56p04	V3.03.00s56p03	2008-05-27	None
V3.03.01s168p04	V3.03.00s168p03		
V3.03.01s56p03	V3.03.00s56p01	2008-03-28	None
V3.03.01s168p03	V3.03.00s168p01		
V3.03.01s56p01	V3.03.00s56	2008-01-25	None
V3.03.01s168p01	V3.03.00s168		
V3.03.00s56	None	2007-08-25	First release of V3.03.xx
V3.03.00s168			

Hardware and Software Compatibility Matrix

Table 2 Compatibility matrix

Item	Specifications
Product family	Switch 5500G series
Hardware platform	24-Port-EI 48-Port-EI 24-Port-PWR 48-Port-PWR 24-Port-FX
Minimum memory requirements	128 MB
Minimum flash requirements	16 MB
Boot ROM version	V5.05 for the main board; V240 for the expansion board
Host software	s4c03_03_02s168p18.app
iMC version	iMC PLAT 5.0 SP1-E0101 + P05 iMC UAM 5.0 SP1-E0101 + P03 iMC EAD 5.0 SP1-E0101 + P03
iNode version	iNode PC 5.0-E0103
Web version	s4i06_05
Remarks	s4c03_03_02s168p18.app is the 168-bit SSH encryption program.

**Caution**

- V3.03.00 is the first release of V3.03.xx series. Some new features are added on the basis of V3.02.xx. Refer to Feature Updates for details.
 - V3.02.xx is an enhanced version and is backward and forward compatible.
-

Sample: Display version information.

```
<5500G-EI> display version
```

```
3Com Corporation
```

```
Switch 5500G-EI 52-Port Software Version 3Com OS V3.xx.xx
```

---- Note①

```
Copyright(c) 2004-2011 3Com Corporation and its licensors, All rights reserved.
```

```
Switch 5500G-EI uptime is 0 week, 0 day, 0 hour, 22 minutes
```

```
Switch 5500G-EI PWR 48-Port with 1 MIPS Processor
```

```
128M      bytes SDRAM
```

```
16384K    bytes Flash Memory
```

```
Config Register points to FLASH
```

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

```
CPLD Version is 002
```

```
Bootrom Version is x.xx
```

---- Note②

```
[Subslot 0] 48 FE + 4 GE Hardware Version is 00.00.00
```

Restrictions and Cautions

When configuring the S5500G, be sure that you are aware of these restrictions and cautions:

- 1) For storm suppression, use the pps mode because the ratio mode is not suitable for long frames.
- 2) If an interface goes up and down frequently during receiving route update packets, garbage routes cannot be removed.
- 3) On a stacking switch, not all ports are capable of line-speed forwarding.
- 4) The default anti-attack function may be affected if the default queue scheduling configuration is changed. Leave the default queue-scheduling configuration unchanged if there is no special requirement
- 5) IGMP snooping is not supported on the 10G expansion board.
- 6) Silicon behaviour: Giant packets and CRC error packets cannot be counted accurately on the 10G expansion board.
- 7) Silicon behaviour: IP packets with the Options field cannot be forwarded
- 8) The flow control function can process received pause frames, but cannot send out pause frames.
- 9) Using the **display mac-address** command can display MAC addresses on the main control board but cannot display MAC addresses on the expansion board and the slave device.

- 10) When the 5500G-EI acts as an SSH server, the SFTP server on it only supports the PSFTP client of the third-party software named putty.
- 11) Ensure that the device is power-on when performing write operations to the flash such as executing the **save** command.
- 12) When user-defined ACLs are used, 4 bytes (inner VLAN tag length) need to be added when calculating the offset of packets, because the chip treats all packets as double tagged.
- 13) BGP does not support equal-cost multi-path (ECMP).
- 14) Don't upgrade the boot ROM of the expansion card before the version higher than 220 is released.
- 15) Limitation of port mirroring: The packets sent by CPU cannot be mirrored on the egress port.
- 16) When you mirror packets sent by ports on an expansion board, the packets from a port on the front panel to the expansion board cannot be mirrored if the monitor port is not on the expansion board.
- 17) Do not use VLAN mapping together with voice VLAN, 802.1X, MAC authentication, port security, or configuration of maximum MAC addresses that can be learned.
- 18) A nonexistent destination VLAN can be configured in mac-address-mapping, and thus the corresponding MAC replication in the VLAN can be done.
- 19) Link-aggregate ports don't support ARP inspection and IP source guard features.
- 20) DHCP snooping can't work together with selective QinQ.
- 21) If you need to configure both mac-address-mapping and link-aggregation on the same port, configure mac-address-mapping first, and then configure link-aggregation. If you need to remove them, remove link-aggregation configuration first. When lots of MAC addresses need to be mapped, don't perform shutdown and undo shutdown operations frequently.
- 22) The destination MAC address of smartlink packets is 01-0f-e2-00-00-04.
- 23) After upgrading the software of a NTP-configured stacking device from a version between V3.03.00 and V3.03.00p03 to V3.03.02 or later, you need to remove the existing NTP configuration and reconfigure it.

Feature List

Hardware Features

Table 3 Hardware features

Category	Description
Dimensions (H × W × D)	43.6mm × 440mm × 260mm (1.72 × 17.32 × 10.24 in.) (devices without PWR) 43.6mm × 440mm × 420mm (1.72 × 17.32 × 16.54 in.) (devices with PWR)
Weight (full configuration)	≤7.5kg (16.53 lb.) (24-port devices) ≤8kg (17.64 lb.) (48-port devices)
Input voltage	AC: Rated Voltage range: 100 VAC to 240 VAC (50Hz to 60Hz) Max Voltage range: 90 VAC to 264 VAC (50Hz to 60Hz)

Category	Description
	DC: Rated voltage range: –60 VDC to –48 VDC Max voltage range: –72 VDC to –36 VDC
Maximum consumption power	S5624P: 170 W S5648P: 230 W S5624P-PWR: 540 W S5648P-PWR: 600 W S5624F: 170 W
Operating temperature	0°C to 45°C (32°F to 113°F)
Operating humidity	10% to 90%

Software Features

Table 4 Software features

Features	Description
XRN stack	
Port auto-negotiation	Supports both speed and duplex mode auto-negotiation
MAC address table	Address learning Supports up to 16 K MAC addresses including up to 256 static MAC addresses
Jumbo Frame	Supports a maximum of 9 K bytes
STP/RSTP/MSTP	Supports STP and complies with IEEE 802.1D/802.1s
Flow control	Supports IEEE 802.3x flow control mode (full-duplex) Supports back-pressure based flow control (half-duplex)
Link aggregation	Supports up to 8 aggregation groups, and up to 8 FE ports or 4 GE per group Supports link aggregation across devices
VLAN	Supports: Up to 4 K IEEE 802.1Q-compliant VLANs; Port-based VLANs; port-based VLAN trunk; Inter-VLAN routing; VLAN batch configuration; VLAN batch display
Unicast, multicast and broadcast suppression	Supports bandwidth ratio- and rate-based suppression modes on ports.

Features	Description
802.1X authentication	The main purpose of IEEE 802.1X is to implement authentication for wireless LAN users, but its application in IEEE 802 LANs provides a method of authenticating LAN users.
Centralized MAC address authentication	Centralized MAC address authentication is triggered by data packets. In this authentication, the MAC addresses of packets are used as both user names and passwords. Upon receiving the first packet from a user, the switch retrieves the source MAC address from the packet, adds the address to both user name and password fields in a RADIUS packet, and sends the RADIUS packet (authentication packet) to a RADIUS server. The remaining procedure is similar to 802.1X. If authentication succeeds, the source MAC address is added to the MAC address table on the switch, and the user is permitted to access the network.
Port internal/external loopback test	The port internal loopback test detects the connectivity between switch chips and PHY chips. The port external loopback test detects the connectivity between PHY chips and network interfaces with the help of the self-loop header. The two tests used together can determine whether a fault is a switch fault or a link fault.
Voice VLAN	The voice VLAN feature adds ports into voice VLANs by identifying the source MAC addresses of packets. It automatically assigns higher priority for voice traffic to ensure voice quality. This feature supports two application modes: manual and automatic.
DHCP relay	Through a DHCP relay agent, DHCP clients in a subnet can communicate with a DHCP server in another subnet to obtain valid IP addresses. In this way, DHCP clients in different subnets can share one DHCP server. This method saves costs and helps implement centralized management.
Network protocols	TCP/IP protocol suite; secondary IP address configuration; ARP (including gratuitous ARP); DHCP relay agent;
IP address forwarding table	Supports up to 8 K IP address forwarding entries
IP routing	Supports static routing, RIP, OSPF, RIP ECMP, BGP
Multicast	Supports IGMP, PIM-DM and PIM-SM
Reliability	Supports VRRP
QoS	Supports: Bandwidth management Priority configuration based on VLAN, port, IEEE 801.1P, ToS/Diffserv, and CoS Up to 8 sending queues per port Traffic classification QoS profile Port mirroring Priority marking for protocol packets sent by CPU
IGMP snooping	IGMP snooping is a multicast constraining mechanism that runs on Layer 2 devices to manage and control multicast groups.
Password recovery	Recovers Boot ROM and APP passwords

Features	Description
NTP	NTP, built on TCP/IP, is used to distribute accurate time information on a network.
Web network management	
Diagnostics and alarm output	Records and reports network faults for troubleshooting.
Fast startup	In fast startup mode, a switch can complete a startup process within 60 seconds by skipping the power-on self test (POST) and directly running the APP program. You can set the startup mode to fast or normal in the boot ROM menu.
PoE update	Supports global PoE software update
PoE profile	Supported
Software upload and upgrade	Supports software upload and upgrade through the XMODEM protocol, FTP or TFTP. The device supports the FTP server, FTP client and TFTP client.
Hot patch	Fix system errors without rebooting the device or interrupting network operation
System configuration and management	Configuration methods supported: CLI, console port, telnet; Features and functions supported: SNMP, remote monitoring (RMON) 1/2/3/9 group MIBs, system logging, hierarchical alarming.
Network maintenance	Filtering, output and collection of alarm/debug information; Diagnostic tools: Ping, Tracert; Remote maintenance through Telnet and other ways
TACACS+	An enhanced version of TACACS protocol, which cannot work together with XRN.
HGMP	A cluster management protocol
LLDP	Operate on the data link layer to exchange device information between directly connected devices
GVRP	
QinQ	Supports double-tag feature
DHCP snooping	
ARP detection and IP check	DHCP snooping security features
Unauthorized DHCP server detection	The DHCP relay agent has this feature added to detect unauthorized DHCP servers.
Multicast source check	With the multicast-source-deny command, you can prevent a port from being a multicast source port to stop users from sending multicast data.
Unknown multicast drop	With this feature enabled in a VLAN, unknown multicast packets in the VLAN are discarded to save network bandwidth.

Features	Description
IP-MAC-port binding	After the IP address and MAC address of a host are bound to a port, packets of the host can pass the port, while those of other hosts not bound to the port cannot. Other ports are not affected by this configuration.
VCT	Virtual cable test
DLDP	Device Link Detection Protocol
Traps sending when ARP/MAC address table is full	When the ARP/MAC address table is full, a trap is sent.
IGMP snooping querier	IGMP querier at layer2
IGMP snooping group policy	Supports filtering unnecessary IGMP packets such as report packets
Guest VLAN	
FTP disconnection	Disconnects FTP connections through CLI
Port security	Port security features
MSDP	Multicast Source Discovery Protocol, which cannot work together with XRN
DHCP server	The device can act as a DHCP server.
Protocol based VLAN	802.1v, which supports IPV4 /IPX/appleTalk
Mac based VLAN	Assign hosts to a VLAN based on their MAC addresses
IGMP group policy	Supports filtering unnecessary IGMP packets
Port mirroring	Includes remote port mirroring and local mirroring. Remote port mirroring supports port mirroring across devices through VLAN channel.
Smart link	Achieve active/standby link redundancy backup and fast convergence
Storm control	Control traffic received on an Ethernet port
IPv6 management	Supports IPv6 applications: Ping, Traceroute, TFTP and Telnet
EAD quick deployment	Easing the work of EAD client deployment
Web authentication	Free users from installing any special authentication client software

Version Updates

Feature Updates

Table 5 Feature updates

Version Number	Item		Description
V3.03.02p18	Hardware updates	feature	None
	Software updates	feature	None
V3.03.02p16	Hardware updates	feature	None
	Software updates	feature	None
V3.03.02p15	Hardware updates	feature	None
	Software updates	feature	None
V3.03.02p14	Hardware updates	feature	None
	Software updates	feature	None
V3.03.02p13	Hardware updates	feature	None
	Software updates	feature	None
V3.03.02p12	Hardware updates	feature	None
	Software updates	feature	None
V3.03.02p11	Hardware updates	feature	None
	Software updates	feature	None
V3.03.02p07	Hardware updates	feature	None
	Software updates	feature	New features: 1) 802.1X Unicast Trigger Function 2) Mandatory 802.1X authentication domain 3) Multiple secondary RADIUS servers 4) AAA servers per user type
V3.03.02p05	Hardware	feature	None

Version Number	Item		Description
	updates		
	Software updates	feature	None
V3.03.02p04	Hardware updates	feature	None
	Software updates	feature	<p>New features:</p> <p>1) System-guard transparent feature</p> <p>With this function, you can configure the switch not to deliver OSPF, PIM, RIP, or VRRP multicast packets to the CPU while the corresponding protocol is not enabled on the switch.</p> <p>2) Mac-address max-mac-count log</p> <p>3) OSPF supports Appendix E</p> <p>4) LACP MAD</p>
V3.03.02p03	Hardware updates	feature	None
	Software updates	feature	<p>1) Restart accounting when the reauthentication user name changes.</p> <p>2) Private LLDP MIB</p> <p>3) CPU-protection feature</p> <p>4) Command-alias feature</p> <p>5) Loopback detection trap</p> <p>6) IPV6 ACL feature</p> <p>7) When a device acquires an IP address by DHCP, it adds a default route to its routing table with gateway IP as next hop.</p>
V3.03.02p01	Hardware updates	feature	None
	Software updates	feature	<p>New features:</p> <p>1) HTTPS</p> <p>2) Auto VLAN</p> <p>3) Support of RADIUS for line-rate</p> <p>4) Attribute ignore feature</p> <p>This feature can configure for RADIUS to ignore the authentication attribute in the packet of RADIUS Authentication Accept packet.</p>
V3.03.02	Hardware updates	feature	None
	Software updates	feature	<p>New features:</p> <p>1) SSHv1</p> <p>2) MAC-based VLAN</p> <p>3) Port auto-power-down</p>

Version Number	Item		Description
			4) Hot patch 5) LLDP Please refer to the Operation and Command Manuals.
V3.03.01p04	Hardware updates	feature	None
	Software updates	feature	New Features: 1) Transparent transmission of IGMP protocol packets 2) Separation of local ARP proxy and ARP proxy through CLI 3) RSA, DSA negotiation order self-selection 4) Multicast prune delay configuration
V3.03.01p03	Hardware updates	feature	None
	Software updates	feature	New Features: Support for RFC4188 and RFC2674
V3.03.01p02	Hardware updates	feature	None
	Software updates	feature	None
V3.03.01p01	Hardware updates	feature	None
	Software updates	feature	New features: ARP source MAC consistency check: The feature checks both the source MAC address and sender MAC address of an ARP packet. If they are identical, the switch refreshes the corresponding ARP entry according to the packet. If not, the switch will not refresh the ARP entry.
V3.03.00	Hardware updates	feature	None
	Software updates	feature	The following features are added to V3.03.00 on the basis of V3.02.xx. 1) DHCP snooping security features, including ARP detection and IP check 2) ARP proxy and local ARP proxy 3) VLAN mapping 4) Selective QINQ 5) VLAN ACL 6) IGMP snooping non-flooding

Version Number	Item	Description
		<ul style="list-style-type: none"> 7) FTP banner 8) HTTP banner 9) Telnet copyright 10) Port speed auto-negotiation configurable 11) Port link delay (Link state change delay) 12) Manual addition of a host to a multicast group 13) Smart link 14) BPDU tunnel enhancement 15) Router port manual designation 16) Storm control 17) Layer-2 ACL (acl number 4000) support for inner-VLAN range based match criteria configuration. 18) Traffic-redirect action, which can untag and redirect packets to the master port of a link aggregation group (by default, no untag operation is performed). 19) IPv6 management 20) DHCP snooping support for processing DHCP NAK and decline packets 21) Enhanced SFP 22) Local authentication application upon HWTACACS authentication failures 23) XRN auto-stacking 24) Port isolation across stacking devices 25) EAP authentication for telnet users 26) Port security and/or mode 27) Support connecting to the Cisco OSPF P2MP non-broadcast interface 28) RIP support for offset field modification of specific subnets 29) SNMP support for cipher password copy 30) IGMPv3 snooping 31) Support for long domain names 32) SNMP mask configuration in MIB view 33) MAC authentication support for guest VLAN 34) Remote-ping test enhancement 35) DLDP recover 36) DHCP option 82 string function

Version Number	Item	Description
		37) HWTACACS support for super authentication 38) HGMP topology management and trace-MAC 39) EAD quick deployment 40) Web authentication 41) Web support for cluster configuration 42) Implementation of OSPF NSSA changes defined in RFC3101

Command Line Updates

Table 6 Command line updates

Version Number	Item	Description
V3.03.02p18	New Commands	None
	Removed Commands	None
	Modified Commands	None
V3.03.02p16	New Commands	<p>Add new keyword of noshut to command 'arp rate-limit enable'. The full descriptions of the command are as follow:</p> <p>Syntax</p> <p>arp rate-limit enable [noshut] undo arp rate-limit enable</p> <p>View</p> <p>Ethernet port view</p> <p>Parameters</p> <p>noshut: Does not shut down the port.</p> <p>Description</p> <p>Use the arp rate-limit enable command to enable ARP packet rate limit on the port.</p> <p>Use the undo arp rate-limit enable command to disable ARP packet rate limit on the port.</p> <p>By default, ARP packet rate limit is disabled, and ARP packet rate is not limited on a port.</p> <p>Without the noshut keyword, this command enables the switch to shut down the port when the maximum rate is reached.</p> <p>With the noshut keyword, this command enables the switch to discard incoming ARP packets received on the</p>

Version Number	Item	Description
		port when the maximum rate is reached.
	Removed Commands	None
	Modified Commands	None
V3.03.02p15	New Commands	None
	Removed Commands	None
	Modified Commands	None
V3.03.02p14	New Commands	None
	Removed Commands	None
	Modified Commands	None
V3.03.02p13	New Commands	None
	Removed Commands	None
	Modified Commands	None
V3.03.02p12	New Commands	None
	Removed Commands	None
	Modified Commands	None
V3.03.02p11	New Commands	None
	Removed Commands	None
	Modified Commands	mac-authentication timer offline-detect Refer to <i>3Com Switch 5500G Family Command Reference(V03.03.02)</i> for detail.
V3.03.02p07	New Commands	Refer to <i>3Com Switch 5500G Family Command Reference(V03.03.02)</i> for details of the following new features: 1) 802.1X Unicast Trigger Function 2) Mandatory 802.1X authentication domain 3) Multiple secondary RADIUS servers 4) AAA servers per user type
	Removed Commands	None
	Modified Commands	None
V3.03.02p05	New Commands	None
	Removed Commands	None
	Modified Commands	None
V3.03.02p04	New Commands	Command 1: Syntax system-guard transparent { ospf pim rip vrrp }


Version Number	Item	Description
		<p>undo system-guard transparent { ospf pim rip vrrp }</p> <p>View</p> <p>System view</p> <p>Parameters</p> <p>ospf: Specifies control of OSPF multicast packets, whose destination IP addresses are 224.0.0.5 or 224.0.0.6.</p> <p>pim: Specifies control of PIM multicast packets, whose destination IP addresses is 224.0.0.13.</p> <p>rip: Specifies control of RIP multicast packets, whose destination IP addresses is 224.0.0.9.</p> <p>vrrp: Specifies control of VRRP multicast packets, whose destination IP addresses is 224.0.0.18.</p> <p>Description</p> <p>Use the system-guard transparent command to configure the system-guard transparent function for the specified protocol. Then, upon receiving a multicast packet of the specified protocol, the switch will only broadcast the packet within the corresponding VLAN, but not deliver the packet to the CPU for processing.</p> <p>Use the undo system-guard transparent command to disable the function for the specified protocol. Then, upon receiving a multicast packet of the specified protocol, the switch will not only broadcast the packet within the corresponding VLAN but also deliver the packet to the CPU for processing.</p> <p>By default, the system-guard transparent function is disabled on the switch.</p> <p>Note that: If OSPF, PIM, RIP, or VRRP is enabled on the switch, do not enable the system-guard transparent function for the protocol. For example, if RIP is enabled on the switch, do not configure the system-guard transparent rip command. Otherwise, RIP cannot function normally.</p> <p>Examples</p> <p># Configure the system-guard transparent function for VRRP, so that the switch does not deliver VRRP multicast packets to the</p>

Version Number	Item	Description
		<p>CPU for processing.</p> <pre><sysname> system-view</pre> <p>System View: return to User View with Ctrl+Z.</p> <pre>[sysname] system-guard transparent vrrp</pre> <p>Caution: When enabling VRRP, undo this command. Otherwise, VRRP can't work correctly.</p>
	Removed Commands	None
	Modified Commands	None
V3.03.02p03	New Commands	Please refer to the manuals of new features provided along with current version.
	Removed Commands	None
	Modified Commands	Please refer to the manuals of new features for IPv6 ACL command.
V3.03.02p01	New Commands	<p>Command 1:</p> <p>icmp acl-priority</p> <p>Syntax</p> <pre>icmp acl-priority undo icmp acl-priority</pre> <p>View</p> <p>System view</p> <p>Default Level</p> <p>3: Management Level</p> <p>Parameters</p> <p><i>None</i></p> <p>Description</p> <p>Use the icmp acl-priority command to restore the system-defined ACLs for ICMP attack guard.</p> <p>Use the undo icmp acl-priority command to cancel the system-defined ACLs for ICMP attack guard.</p> <p>By default, the system keeps the system-defined ACLs for ICMP attack guard.</p> <p>In a secure network, you can cancel the system-defined ACLs for ICMP attack guard, and thus increase the available ACL resources for setting user-defined security policies.</p> <p>With the system-defined ACLs for ICMP</p>


Version Number	Item	Description
		<p>attack guard canceled, the ICMP attacks in the network may affect the device's processing for normal packets. Therefore, before canceling the system-defined ACLs for ICMP attack guard, check ICMP attack vulnerabilities in the network to make sure that the network can operate properly after you cancel the system-defined ACLs for ICMP attack guard.</p> <p>Examples</p> <p># Cancel the system-defined ACLs for ICMP attack guard.</p> <pre><Sysname> system-view [Sysname] undo icmp acl-priority</pre> <p>Command 2:</p> <p>Syntax</p> <p>mirroring stp-collaboration</p> <p>undo mirroring stp-collaboration</p> <p>View</p> <p>System view</p> <p>Default Level</p> <p>3: Management Level</p> <p>Parameters</p> <p><i>None</i></p> <p>Description</p> <p>Use the mirroring stp-collaboration command to enable port mirroring – STP collaboration.</p> <p>Use the undo mirroring stp-collaboration command to disable port mirroring – STP collaboration.</p> <p>By default, port mirroring – STP collaboration is not enabled.</p> <p>With this function enabled, the device determines whether to enable port mirroring on a port by monitoring the STP status of the port:</p> <ul style="list-style-type: none"> • The device automatically disables port mirroring on a port in Discarding state; • The device enables port mirroring on the port when the port restores to Forwarding state. <p>In this way, port mirroring is utilized more</p>


Version Number	Item	Description
		<p>efficiently.</p> <p>Examples</p> <pre># Enable port mirroring – STP collaboration. <Sysname> system-view [Sysname] mirroring stp-collaboration</pre> <p>Command 3:</p> <p>Syntax:</p> <pre>attribute-ignore { standard vendor vendor-id } type type-value undo attribute-ignore { all standard vendor vendor-id }</pre> <p>View:</p> <p>RADIUS view</p> <p>Description:</p> <p>"attribute-ignore vendor vendor-id type type-value" is used to add a new configuration to ignore all the private attribute that is given Vendor ID, Type.</p> <p>"attribute-ignore standard type type-value" is used to add a new configuration to ignore all the standard attribute that is given Type.</p> <p>"undo attribute-ignore all" is used to undo all the ignore configuration of the RADIUS attribute.</p> <p>"undo attribute-ignore standard" is used to undo the ignore configuration of the RADIUS standard attribute</p> <p>"undo attribute-ignore vendor vendor-id" is used to undo the ignore configuration of the given Vendor ID private attribute.</p> <p>One RADIUS, standard attribute can configure one attribute-ignore command at most; identical Vendor ID can configure one attribute-ignore command at most. One RADIUS, at most configure 3 attribute-ignore commands.</p> <p>Example:</p> <pre>#configure RADIUS "system" ignore 81 type standard attribute [Switch]radius scheme system [Switch-radius-system]attribute-</pre>

Version Number	Item	Description
		<p>ignore standard type 81</p> <p>#configure RADIUS "system" ignore 22 type H3C private attribute (Vendor ID=25506):</p> <pre>[Switch-radius-system]attribute- ignore vendor 25506 type 22</pre> <p>#delete RADIUS "system" ignore standard attribute configuration:</p> <pre>[Switch-radius-system]undo attribute- ignore standard</pre> <p>#delete RADIUS "system" ignore H3C private attribute configuration:</p> <pre>[Switch-radius-system]undo attribute- ignore vendor 2011</pre> <p>#delete RADIUS "system" all the ignore attribute configuration:</p> <pre>[Switch-radius-system]undo attribute- ignore all</pre>
	Removed commands	None
	Modified Commands	None
V3.03.02	New Commands	Please refer to the Operation Manual and Command Manual.
	Removed commands	Please refer to the Operation Manual and Command Manual.
	Modified Commands	Please refer to the Operation Manual and Command Manual.
V3.03.01p05	New Commands	None
	Removed commands	None
	Modified Commands	None
V3.03.01p04	New Commands	<p>Command 1:</p> <p>Syntax</p> <p>igmp transparent enable</p> <p>undo igmp transparent enable</p> <p>View</p> <p>Ethernet port view</p> <p>Parameters</p> <p>None</p> <p>Description</p> <p>Use the igmp transparent enable command to enable transparent IGMP message transmission on the port.</p>

Version Number	Item	Description
		<p>Use the undo igmp transparent enable command to disable transparent IGMP message transmission on the port.</p> <p>By default, transparent IGMP message transmission is disabled on a port.</p> <p>For a VLAN-VPN-disabled port, the switch can transmit an IGMP message received on the port within the VLAN that the IGMP message belongs to normally. For the switch to transparently transmit an IGMP message received on a VLAN-VPN port in the outer VLAN, however, you must enable transparent IGMP message transmission on the port.</p> <hr/> <p> Caution</p> <ul style="list-style-type: none"> • If your switch is required to process the IGMP messages received on a VLAN-VPN port (for example, because IGMP or IGMP snooping is enabled on the port), you must disable transparent IGMP message transmission on the port so that the switch can process the IGMP messages normally. • Do not enable transparent IGMP message transmission on a port without VLAN-VPN enabled. <hr/> <p>Examples</p> <pre># Enable transparent IGMP message transmission on port GigabitEthernet 1/0/1. <Sysname> system-view System View: return to User View with Ctrl+Z. [Sysname] interface GigabitEthernet 1/0/1 [Sysname-GigabitEthernet1/0/1] igmp transparent enable</pre> <p>Command 2:</p> <p>Syntax</p> <p>local-proxy-arp enable undo local-proxy-arp enable</p> <p>View</p> <p>VLAN interface view</p>

Version Number	Item	Description
		<p>Parameters</p> <p>None</p> <p>Description</p> <p>Use the local-proxy-arp enable command to enable local proxy ARP on the VLAN interface.</p> <p>Use the undo local-proxy-arp enable command to disable local proxy ARP on the VLAN interface.</p> <p>By default, local proxy ARP is disabled on the VLAN interfaces of a switch.</p> <p>Examples</p> <p># Enable local proxy ARP on VLAN-interface 2.</p> <pre><Sysname> system-view [Sysname] interface vlan-interface 2 [Sysname-Vlan-interface2] local-proxy-arp enable</pre> <p>Command 3:</p> <p>Syntax</p> <p>prune delay <i>interval</i></p> <p>undo prune delay</p> <p>View</p> <p>PIM view</p> <p>Parameters</p> <p><i>interval</i>: Specifies the prune delay interval in seconds, in the rage of 1 to 128.</p> <p>Description</p> <p>Use the prune delay command to configure the PIM prune delay interval.</p> <p>Use the undo prune delay command to restore the default PIM prune delay interval.</p> <p>By default, the PIM prune delay interval is 5 seconds.</p> <p>Upon receiving a prune message from a downstream node, the upstream node does not take a prune action immediately; instead, it maintains the forwarding state of the interface to the downstream. If the</p>

Version Number	Item	Description
		<p>upstream node receives a prune override message from the downstream node within the prune delay interval, it cancels the prune action; otherwise, it prunes the interface to the downstream when the prune delay times out.</p> <hr/> <p> Note</p> <p>The PIM prune delay function is applicable only to PIM-SM networks, but not to PIM-DM networks.</p> <hr/> <p>Examples</p> <p># Set the PIM prune delay interval to 75 seconds.</p> <pre><Sysname> system-view System View: return to User View with Ctrl+Z. [Sysname] pim [Sysname-pim] prune delay 75</pre>
	Removed commands	None
	Modified Commands	None
V3.03.01p03	New Commands	<p>Command:</p> <p>Syntax</p> <pre>loopback-detection shutdown enable undo loopback-detection shutdown enable</pre> <p>View</p> <p>Ethernet port view</p> <p>Parameter</p> <p>None</p> <p>Description</p> <p>Use the loopback-detection shutdown enable command to enable the loopback port auto-shutdown function.</p> <p>Use the undo loopback-detection shutdown enable command to disable the function.</p> <p>The loopback port auto-shutdown function works in conjunction with the loopback detection function (refer to loopback-detection enable). If a loop is found at a port:</p> <ul style="list-style-type: none"> • With the function enabled on the port,

Version Number	Item	Description
		<p>the system will shut down the port, and send log messages to the terminal. After the loop is removed, you need to use the undo shutdown command to bring up the port.</p> <ul style="list-style-type: none"> With the function disabled on the port, the system will only send log messages to the terminal, and the port is still in the normal forwarding state. <p>By default, the loopback port auto-shutdown function is enabled on ports if the device boots with the default configuration file (config.def); if the device boots with null configuration, this function is disabled.</p> <p>Related command: loopback-detection enable; loopback-detection control enable.</p> <hr/> <p> Note</p> <p>You cannot enable both the loopback port control function (with the loopback-detection control enable command) and the loopback port auto-shutdown function on a port. If you do so, the function configured later will take effect.</p> <hr/> <p>Example</p> <p># Enable the loopback port auto-shutdown function on port GigabitEthernet 1/0/1.</p> <pre><Sysname> system-view System View: return to User View with Ctrl+Z. [Sysname] loopback-detection enable [Sysname] interface gigabitethernet 1/0/1 [Sysname-GigabitEthernet1/0/1] loopback-detection shutdown enable</pre>
	Removed commands	None
	Modified Commands	None
V3.03.01p01	New Commands	<p>Command:</p> <p>Syntax</p> <p>arp anti-attack valid-check enable</p> <p>undo arp anti-attack valid-check enable</p> <p>View</p> <p>System view</p> <p>Parameters</p>

Version Number	Item	Description
		<p>None</p> <p>Description</p> <p>Use the arp anti-attack valid-check enable command to enable ARP source MAC address consistency check.</p> <p>Use the undo arp anti-attack valid-check enable command to disable this function.</p> <p>By default, ARP source MAC address consistency check is disabled.</p> <p>Examples</p> <p># Enable ARP source MAC address consistency check.</p> <pre><Sysname> system-view [Sysname] arp anti-attack valid-check enable</pre>
	Removed commands	None
	Modified Commands	None
V3.03.00	New Commands	Please refer to the documents provided by 3Com.
	Removed commands	<p>Command 1:</p> <p>Syntax</p> <p>multicast load-sharing enable { global-hash local-hash }</p> <p>undo multicast load-sharing enable</p> <p>Reason</p> <p>After modification, multicast load-sharing is enabled by default.</p> <p>Command 2:</p> <p>Syntax</p> <p>display workpath</p> <p>Reason</p> <p>This is a debugging command.</p> <p>Command 3:</p> <p>Syntax:</p> <p>spt-switch-threshold infinity [group-policy acl-number [order order-value]]</p> <p>undo spt-switch-threshold [group-policy acl-number]</p>


Version Number	Item	Description
		<p>View</p> <p>PIM view</p> <p>Reason</p> <p>The switch chip does not support multicast speed calculation.</p> <p>Command 4:</p> <p>Syntax</p> <p>language-mode { english chinese }</p> <p>View</p> <p>user view</p> <p>Reason</p> <p>Chinese language mode is not needed.</p>
	Modified Commands	<p>Command 1:</p> <p>Syntax:</p> <pre>rule [rule-id] { deny permit } [[type protocol-type protocol-mask lsap lsap- code lsap-wildcard] format-type cos cos source { source-mac-addr source-mac- mask vlan-id }* dest dest-mac-addr dest- mac-mask c-tag-vlan c-tag-vlan-begin [to c-tag-vlan-end] time-range time-name]*</pre> <p>undo rule rule-id</p> <p>View:</p> <p>Layer 2 ACL view</p> <p>Parameters:</p> <p><i>c-tag-vlan-begin, c-tag-vlan-end</i>: VLAN ID, in the range of 1 to 4094.</p> <p>This keyword and argument combination is usually used in cooperation with the QinQ function. For information about QinQ, refer to <i>VLAN-VPN Operation</i>.</p> <p>Description:</p> <p>Use this command to define an ACL rule for matching the inner VLAN range of QINQ.</p>


Version Number	Item	Description
		<p>Command 2:</p> <p>Syntax</p> <pre> traffic-redirect inbound <i>acl-rule</i> { cpu { interface <i>interface-type</i> <i>interface-number</i> / link-aggregation-group <i>agg-id</i> } [untagged] }</pre> <p>undo traffic-redirect inbound <i>acl-rule</i></p> <p>View</p> <p>Ethernet port view</p> <p>Parameters</p> <p>link-aggregation-group <i>agg-id</i>: Specifies the aggregation group the traffic is to be redirected to. The <i>agg-id</i> argument is the ID of an aggregation group, in the range 1 to 464.</p> <p>untagged: Specifies to remove the outer VLAN tag of a packet after the packet is redirected to a port or an aggregation group.</p> <p>Command 3:</p> <p>Syntax</p> <pre> traffic-limit inbound { link-group <i>acl-number</i> [rule <i>rule-id</i>] ip-group <i>acl-number</i> rule [<i>rule-id</i>] link-group <i>acl-number</i> rule [<i>rule-id</i>] user-group <i>acl-number</i> [rule <i>rule-id</i>] } [union-effect] <i>target-rate</i> [burst-bucket <i>burst-bucket-size</i>] [exceed <i>action</i>]</pre> <p>undo traffic-limit inbound { link-group <i>acl-number</i> [rule <i>rule-id</i>] } ip-group <i>acl-number</i> [rule <i>rule-id</i>] link-group <i>acl-number</i> rule [<i>rule-id</i>] user-group <i>acl-number</i> [rule <i>rule-id</i>] }</p> <p>View</p> <p>Ethernet port view</p> <p>Parameters</p> <p>union-effect: Specifies that all the ACL rules, including those identified by the <i>acl-rule</i> argument in this command and those applied previously, are valid. If this keyword is not specified, traffic policing issues both the rate limiting action and the permit action at the same time, that is, traffic</p>

Version Number	Item	Description
		<p>policing permits the conforming traffic to pass through. If this keyword is specified, traffic policing issues only the rate limiting action but not the permit action. In this case, if a packet matches both an ACL rule specified in the traffic-limit command and another previously applied ACL rule with the deny keyword specified, the packet will be dropped.</p> <p>burst-bucket <i>burst-bucket-size</i>: Specifies the maximum burst traffic size (in KB) allowed. The following are the value ranges for the <i>burst-bucket-size</i> argument:</p> <ul style="list-style-type: none"> • GigabitEthernet port: 4 to 512 • 10-GigabitEthernet port: 4 to 8192 <p>The <i>burst-bucket-size</i> argument must be an integer power of 2. If the burst size is not specified, it is 512 KB by default.</p> <p>Command 4:</p> <p>Syntax</p> <p>line-rate outbound <i>target-rate</i> [burst-bucket <i>burst-bucket-size</i>]</p> <p>undo line-rate outbound</p> <p>View</p> <p>Ethernet port view</p> <p>Parameters</p> <p>burst-bucket <i>burst-bucket-size</i>: Specifies the maximum burst traffic size (in KB). This is the buffer size provided for burst traffic while traffic is being forwarding or received at the rate of <i>target-rate</i>. The following are the value ranges for the <i>burst-bucket-size</i> argument:</p> <ul style="list-style-type: none"> • GigabitEthernet port: 4 to 512 • 10 GigabitEthernet port: 4 to 8192 <p>The <i>burst-bucket-size</i> argument must be an integer power of 2. If it is not specified, 64 KB applies by default.</p> <p>Command 5:</p> <p>Syntax</p> <p>display vlan [<i>vlan-id1</i> [to <i>vlan-id2</i>]] all dynamic static]</p> <p>View</p> <p>Any view</p>

Version Number	Item	Description
		<p>Parameters</p> <p><i>vlan-id1</i>: Specifies the ID of a VLAN of which information is to be displayed, in the range of 1 to 4094.</p> <p>to <i>vlan-id2</i>: In conjunction with <i>vlan-id1</i>, define a VLAN range to display information about all existing VLANs in the range. The <i>vlan-id2</i> argument takes a value in the range of 1 to 4094, and must not be less than that of <i>vlan-id1</i>.</p> <p>all: Displays information about all the VLANs.</p> <p>dynamic: Displays the number of dynamic VLANs and the ID of each dynamic VLAN. Dynamic VLANs refer to VLANs that are generated through GVRP or those distributed by a RADIUS server.</p> <p>static: Displays the number of static VLANs and the ID of each static VLAN. Static VLANs refer to VLANs manually created.</p> <p>Description</p> <p>Use the display vlan command to display information about VLANs. The output shows the ID, type, VLAN interface state and member ports of a VLAN.</p> <p>If no keyword or argument is specified, the command displays the number of existing VLANs in the system and the ID of each VLAN.</p> <p>Command 6:</p> <p>Syntax</p> <pre>reset vrrp statistics [interface vlan- interface vlan-id [vrid virtual-router-id]]</pre> <p>View</p> <p>User view</p> <p>Parameters</p> <p>vlan-interface <i>vlan-id</i>: Specifies a VLAN interface by its ID. <i>vlan-id</i> is the ID of a VLAN interface.</p> <p>vrid <i>virtual-router-id</i>: Specifies a VRRP group. <i>virtual-router-id</i> is the VRRP group ID, ranging from 1 to 255.</p>

Version Number	Item	Description
		<p>Description</p> <p>Use the reset vrrp statistics command to clear the VRRP statistics information.</p> <p>When you execute this command,</p> <ul style="list-style-type: none"> • If neither a VLAN interface nor a VRRP group is specified, the statistics information about all the VRRP groups on the switch is cleared. • If only a VLAN interface is specified, the statistics information about all the VRRP groups on the specified VLAN interface is cleared. • If both a VLAN interface and a VRRP group are specified, the statistics information about the specified VRRP group on the specified VLAN interface is cleared. <p>Command 7:</p> <p>Syntax</p> <pre> vrrp vrid virtual-router-id authentication-mode authentication-type authentication-key undo vrrp vrid virtual-router-id authentication-mode </pre> <p>View</p> <p>VLAN interface view</p> <p>Parameters</p> <p><i>virtual-router-id</i>: VRRP group ID, ranging from 1 to 255.</p> <p><i>authentication-type</i>: Authentication type, which can be:</p> <ul style="list-style-type: none"> • simple: Indicates to perform simple text authentication. • md5: Indicates to perform the authentication by using MD5 algorithm. <p><i>authentication-key</i>: Authentication key, which can be:</p> <ul style="list-style-type: none"> • When the authentication type is simple, the authentication key is in plain text and can contain one to eight characters. • When the authentication type is md5, the authentication key can be a string of one to eight characters in plain text, such as 1234567, or a 24-character MD5 encrypted string, such as <code>_(TT8FJY\5SQ=^Q`MAF4<1!!.</code>

Version Number	Item	Description
		<p>Description</p> <p>Use the vrrp vrid authentication-mode command to specify the authentication type and the authentication key for a VRRP group to receive and send VRRP packets.</p> <p>Use the undo vrrp vrid authentication-mode command to restore the default.</p> <p>By default, no VRRP authentication is configured.</p> <hr/> <p> Note</p> <ul style="list-style-type: none"> • The authentication key is case sensitive. • Before configuring VRRP authentication on a VLAN interface, you need to create a VRRP group and configure the virtual IP address of it on the VLAN interface. • This command sets the authentication type and authentication key for all the VRRP groups on an interface. This is determined by the protocol, which defines that all the VRRP groups on an interface share the same authentication type and authentication key. Besides, all the members joining the same VRRP group should also share the same authentication type and authentication key. <hr/> <p>Examples</p> <p># Set the authentication type of VRRP group 1 on VLAN-interface 2 to simple and the authentication key for it to aabbcc.</p> <pre><Sysname> system-view System View: return to User View with Ctrl+Z. [Sysname] interface Vlan-interface 2 [Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1 [Sysname-Vlan-interface2] vrrp vrid 1 authentication-mode simple aabbcc</pre> <p>Command 8:</p> <p>Syntax</p> <p>vrrp vrid <i>virtual-router-id</i> track interface vlan-interface <i>vlan-id</i> [reduced <i>value-reduced</i>]</p> <p>undo vrrp vrid <i>virtual-router-id</i> track interface vlan-interface <i>vlan-id</i></p>

Version Number	Item	Description
		<p>View</p> <p>VLAN interface view</p> <p>Parameters</p> <p><i>virtual-router-id</i>: VRRP group ID, ranging from 1 to 255.</p> <p><i>vlan-id</i>: A VLAN interface ID to be tracked.</p> <p><i>value-reduced</i>: Value by which the priority decreases. This argument ranges from 1 to 255 and defaults to 10.</p> <p>Description</p> <p>Use the vrpp vrid track interface command to set a VLAN interface to be tracked.</p> <p>Use the undo vrpp vrid track interface command to disable a VLAN interface from being tracked.</p> <p>The VLAN interface tracking function extends the use of the backup function. With this function enabled on a switch, the backup function can take effect not only when the VLAN interface where a VRRP group resides fails, but also when some other VLAN interfaces on the switch fail. You can utilize the VLAN interface tracking function by specifying monitored VLAN interfaces.</p> <p>When the tracked VLAN interface on the master of a VRRP group is down, the priority of the master decreases by the value set by the <i>value-reduced</i> argument, allowing a switch with the highest priority in the VRRP group becomes the master.</p> <hr/> <p> Note</p> <ul style="list-style-type: none"> • If an IP address owner exists in a VRRP group, do not configure the interface tracking function on the IP address owner. If configured, the function cannot take effect. • A VRRP group can track up to eight VLAN interfaces simultaneously. <hr/> <p>Examples</p> <p># On VLAN-interface 2, configure to track VLAN-interface 1 and configure the priority of the master of VRRP group 1 (on VLAN-</p>

Version Number	Item	Description
		<p>interface 2) to decrease by 50 when VLAN-interface 1 goes down.</p> <pre><Sysname> system-view System View: return to User View with Ctrl+Z. [Sysname] interface Vlan-interface 2 [Sysname-Vlan-interface2] vrrp vrid 1 track interface vlan-interface 1 reduced 50</pre> <p>Command 9:</p> <p>Syntax</p> <p>display ntdp single-device mac-address <i>mac-address</i></p> <p>View</p> <p>Any view</p> <p>Parameters</p> <p><i>mac-address</i>: MAC address of the device whose detailed information is to be displayed.</p> <p>Description</p> <p>Use the display ntdp single-device mac-address command to display the detailed information, which is collected through NTDP protocol packets, about a single device. The information displayed by the command is similar to that displayed by the display cluster members command. However, if you want to display information about a device that is enabled with only NTDP and is not in any cluster, you have to use the display ntdp single-device mac-address command.</p> <p>Command 10:</p> <p>Syntax</p> <p>display ntdp device-list [verbose]</p> <p>View</p> <p>Any view</p> <p>Parameters</p> <p>verbose: Displays the detailed information of devices in a cluster.</p>

Version Number	Item	Description
		Description Use the display ntdp device-list command to display the cluster device information collected by NTDP.

MIB Updates

Table 7 MIB updates

Version number	Item	MIB file	Module	Description
V3.03.02p18	New	None	None	None
	Modified	None	None	None
V3.03.02p16	New	None	None	None
	Modified	None	None	None
V3.03.02p15	New	None	None	None
	Modified	None	None	None
V3.03.02p14	New	None	None	None
	Modified	None	None	None
V3.03.02p13	New	None	None	None
	Modified	None	None	None
V3.03.02p12	New	None	None	None
	Modified	None	None	None
V3.03.02p11	New	None	None	None
	Modified	None	None	None
V3.03.02p07	New	None	None	None
	Modified	None	None	None
V3.03.02p05	New	None	None	None
	Modified	None	None	None
V3.03.02p04	New	None	None	None
	Modified	None	None	None

Version number	Item	MIB file	Module	Description
V3.03.02p03	New	1) H3C-VOICE-VLAN-MIB 2) H3C-LLDP-EXT-MIB	1) VOICE VLAN 2) LLDP	1) Add node h3cVoiceVlanPortLegacy and h3cVoiceVlanPortQoSTrus in h3cvoiceVlanPortTable to control 'voice VLAN legacy' and 'voice VLAN QOS trust'. 2) Adding the following private MIB: (1) h3cLldpAdminStatus: Enable/Disable LLDP in global; (2) h3cLldpComplianceCDPStatus: LLDP supports CDP in global; (3) h3cLldpPortConfigTable:LLDP port configure table; (4) h3cLldpPortConfigPortNum: LLDP port number; (5) h3cLldpPortConfigCDPComplianceStatus: LLDP supports CDP in port
	Modified	None	None	None
V3.03.02p01	New	None	None	None

Version number	Item	MIB file	Module	Description
	Modified	dot1x_tree.c a3com_domain_tree.c	(1) dot1xPaePortInitialize (2) h3cDomainVlanAssignMode	<p>(1)</p> <p>This node did not function in the past. After being modified, its function is as follows:</p> <ul style="list-style-type: none"> Setting this attribute to TRUE causes the port to cut all its 802.1x users. The attribute value restores to FALSE once cutting operation is completed. Setting this attribute to FALSE has no effect. This attribute always returns FALSE when it is read. <p>(2)</p> <p>The VLAN assignment mode. The mode should be the same as the mode of the corresponding server.</p> <ul style="list-style-type: none"> 1 (integer) - Integer VLAN assignment mode. 2 (string) - String VLAN assignment mode. 3 (vlanlist) - VLAN-List VLAN assignment mode. <p>The default value is integer.</p> <p>The third mode is used to support the auto-vlan feature, which is supported beginning with the new software version.</p>

Configuration Changes

V3.03.02p18 Operation Changes

None.

V3.03.02p16 Operation Changes

None.

V3.03.02p15 Operation Changes

- 1) DHCP Snooping supports forwarding BOOTP packet.

V3.03.02p14 Operation Changes

None.

V3.03.02p13 Operation Changes

None.

V3.03.02p12 Operation Changes

None.

V3.03.02p11 Operation Changes

- 1) The Changes of syslog records WEB user's name

In early version: The syslog records only the user's name after a WEB user log in, such as:

```
%Apr  7 09:10:24:698 2010 switch WEB/5/USER:- 1 -web login succeed
%Apr  7 09:10:47:961 2010 switch WEB/5/USER:- 1 -web logout
```

In current version: The syslog records both the user's name and the user's IP address after a WEB user log in, such as:

```
%Apr  7 09:20:34:698 2010 switch WEB/5/USER:- 1 -web (1.1.1.1) login succeed
%Apr  7 09:20:37:961 2010 switch WEB/5/USER:- 1 -web (1.1.1.1) logout
```

- 2) The Changes of LLDP function

In early version:LLDP packets are forwarded to other ports if LLDP function is disabled globally.

In current version:LLDP packets aren't forwarded if LLDP function is disabled globally.

- 3) The change of the bootp reply packet's length

In early version:

Switch serves as DHCP relay. If the packet received by the device whose length less than 300 bytes, the device does not add padding automatically to make packet length to 300 bytes.

In current version:

Switch serves as DHCP relay. If the packet received by the device whose length less than 300 bytes, the device add padding automatically to make packet length to 300 bytes.

V3.03.02p07 Operation Changes

- 1) Dot1x free-ip and stack aren't mutually exclusive any longer.
- 2) The change to DHCP server, DHCP snooping and DHCP Relay

In early version:

DHCP server, DHCP snooping and DHCP Relay can not be enabled at the same time; otherwise PC can't get IP address successfully.

In current version:

DHCP server, DHCP snooping and DHCP Relay can be enabled at the same time. PC can get IP address successfully from switch, and of three functions can record its item.

V3.03.02p05 Operation Changes

- 1) The change to the operation of 'mac-address aging destination-hit enable' command

In early version:

Executing this command, only destination-hit function is enabled.

In current version:

Executing this command, the mac-address synchronization function will also be enabled besides the destination-hit function.

V3.03.02p04 Operation Changes

- 1) The change to the Syslog

In early version:

Specific syslog messages will be sent to log server from every unit in a stack.

In current version:

Specific syslog messages will be sent to log server only from the master unit in a stack.

V3.03.02p03 Operation Changes

- 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.

V3.03.02p01 Operation Changes

- 1) DHCP Snooping and DHCP Relay are not mutually exclusive any longer.
- 2) Change to optical module recognition

Modify the way the switch deals with the module EEPROM checksum. The checksum error module changes from not recognizing information to debugging information.

- 3) Correlative product or ARP forwarding restriction

Before modification:

With the ARP forwarding restriction function enabled, when receiving an ARP request packet, the switch forwards the ARP request packet through the trusted ports only; with the ARP forwarding restriction function disabled, the switch forwards ARP request packets through all ports in the VLAN except the source port.

With the ARP forwarding restriction function enabled, when receiving an ARP response packet, the switch forwards the ARP response packet according to the MAC addresses in the packet, or through trusted ports if the MAC address table does not contain the destination MAC address. With ARP forwarding restriction disabled, the switch forwards the received ARP response packet through all ports in the VLAN except the source port.

After modification:

With the ARP forwarding restriction function enabled, when an ARP request packet is received from a trusted port, the switch forwards the ARP request packet through all ports in the VLAN except the source port; when receiving the ARP request packet from an untrusted port, the switch forwards the ARP request packet through the trusted ports only. With ARP forwarding restriction disabled, the switch forwards the received ARP request packet through all ports in the VLAN except the source port.

When receiving an ARP response packet from a trusted port, the switch forwards the ARP response packet according to the MAC addresses in the packet, or through all ports in the VLAN except the source port if the MAC address table does not contain the destination MAC address; when receiving an ARP response packet from an untrusted port, the switch forwards the ARP response packet according to the process described above, that is: with the ARP forwarding restriction enabled, the ARP response packet is forwarded according to the MAC address in the packet, or through trusted ports if the MAC address table does not contain the destination MAC address; with ARP forwarding restriction disabled, the ARP response packet is forwarded through all ports in the VLAN except the source port.

V3.03.02 Operation Changes

- 1) Change to the maximum number of VLAN interfaces

The maximum number of VLAN interfaces is changed from 64 to 128

- 2) The change to the default stp pathcost standard

In early version:

By default, the IEEE 802.1t standard is used to calculate the default path costs of ports.

In current version:

By default, the legacy standard is used to calculate the default path costs of ports.

V3.03.01p05 Operation Changes

- 1) Change to the maximum number of static routes

The maximum number of static routes is changed from 256 to 1024.

V3.03.01p03 Operation Changes

- 1) **dot1x timer tx-period** command modification

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 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.

- 2) Change to loopback-detection function

A new option "shutdown" is added to loopback-detection function. After loopback-detection shutdown is enabled, if a loopback occurs at a port, the port will be shutdown. Then, you can bring up the port with the **undo shutdown** command. If a port is shut down by loopback-detection, the state of the port is displayed as "LOOPBACK DETECTION DOWN" with the **display interface** command, and displayed as "LPD DOWN" with the **display brief interface** command.

Note:

- Loopback-detection shutdown is different from the **shutdown** command in that: If a port is shutdown by loopback-detection, you cannot see the **shutdown** command by running the **display this** command on that port.
- Loopback-detection shutdown function is mutually exclusive with loopback-detection control function.

V3.03.01p01 Operation Changes

- 1) Change to 802.1X function

Before modification:

After an 802.1X client passes 802.1X authentication,

- a) If the client's IP address is manually changed, the switch disconnects the client.
- b) If the client changes its IP address by using DHCP and the switch is not enabled with DHCP snooping, the switch disconnects the client.
- c) If the client changes its IP address by using DHCP and the switch has DHCP snooping enabled, the switch does not disconnect the client.

After modification:

The switch will not disconnect the client when one of the above mentioned situations occurs.

V3.03.00 Operation Changes

After modification:

- 1) Info-center related configuration is placed at the end part of the configuration file.
- 2) The **vlan-vpn enable** command is exclusive with stack configuration only, and can coexist with other protocols such as STP/GVRP.
- 3) The device is compatible with line feed characters "\r\n" and "\n", so that it can exchange files with the TFTP server running on the UNIX system.
- 4) The ping operation performance is improved, but consequently the real time performance of displaying port statistics is reduced, that is, a delay occurs when you view port statistics.
- 5) You can perform port mirroring and mirroring group configuration through the web interface.
- 6) The device forwards unknown EAP packets rather than discards them.
- 7) The default DLDP interval is changed from 10s to 5s, and the interval range is changed from 5s-100s to 1s-100s. Two devices with different DLDP interval settings cannot communicate with each other using DLDP.
- 8) The protocol number of DLDP is changed from 0800 to 8809. When V3.03.00 or a later version works with V3.02.04 or an earlier version, when the DLDP port STP status is discarding, DLDP cannot function normally.
- 9) The sequence of matching web files is changed from main, backup, default to default, main, backup.
- 10) The maximum number of secondary IP addresses for an interface is changed from 4 to 6.
- 11) The combo ports support physical shutdown. Using the **shutdown** command on an active combo port makes the port down physically rather than switch the combo status from active to inactive. Only the undo shutdown operation is used to switch the status.

- 12) The device no longer sends PortMstiStateDiscarding trap and log packets when a port goes down.

Open Problems and Workarounds

OLSD27415

- First found-in version: V3.02.00
- Description: Execute the **undo ndp enable** command on a stacking device, save the configuration, and reboot the device. Then, the **undo ndp enable** configuration is lost.
- Workaround: None

OLSD26983

- First found-in version: V3.02.00
- Description: When many MAC-authentication users try to login, the following situation may occur: the user connection number is zero, but the user access number is nonzero, and the access users cannot be deleted.
- Workaround: None

OLSD28479

- First found-in version: V3.02.00
- Description: Configure a static multicast MAC address. Display the number of static multicast MAC addresses with the **display mac-address static count** command. The newly configured multicast MAC address is not counted.
- Workaround: None

OLSD28238

- First found-in version: V3.02.00
- Description: When you use the **ip route-static** command to configure a static route, you are allowed to select a loopback interface as the next hop.
- Workaround: None

OLSD28646

- First found-in version: V3.02.00
- Description: Two switches form a stack in a complex network. Enable OSPF, PIM SM, and VRRP on the two devices. Inject a lot of broadcast and multicast packets to make CPU usage very high. Errors may occur to the expansion board, and the expansion board may reboot.
- Workaround: None

OLSD28365

- First found-in version: V3.02.00
- Description: The device is attacked by broadcast packets, and thus cannot telnet to the server.
- Workaround: Configure an ACL to increase the priority of telnet packets.

OLSD28340

- First found-in version: V3.02.00
- Description: A stack is designated as the administrator in a cluster. It connects to a cluster member switch through a slave device in the stack. If the member switch works in passive FTP mode, the FTP cluster will fail to get packets.
- Workaround:

(1) Change the FTP operating mode of the cluster member switch to port mode.

(2) Connect the cluster member switch to the XRN master device.

LSOD02394

- First found-in version: V3.03.01p01
- Description: Enable cluster on a stacking device. Use large packets to ping another device through a slave unit from the stacking device. The ping operation may fail.
- Workaround: None

LSOD02873

- First found-in version: V3.03.01p01
- Description: Configure a link-aggregation group across units in a stack that has STP enabled, and inject heavy traffic into aggregate ports. Change the physical link state of stack ports frequently for a long time. The stack may break.
- Workaround: None.

LSOD07900

- First found-in version: V3.03.01p05
- Description: Configure NTP service related commands, such as **ntp-service unicast-server**, on a stacking device running a software version between V3.02.04p06 and V3.03.01p04. Save the configuration, upgrade the software to version V3.03.01p05, and then reboot the device. If the master device after reboot is different from the one before reboot, the NTP function will fail.
- Workaround: After reboot, delete and re-configure NTP service related commands.

LSOD07892

- First found-in version: V3.03.01p05
- Description: Two PCs are connected to a stacking device and try to login through SFTP and SSH respectively. When the correct SFTP username is input and the device is waiting for the password from one PC, an SSH login operation performed from the other PC will fail the SFTP function and the SSH login will fail too, and vice versa.
- Workaround: In this case, a new login operation can be performed only after the previous login succeeds.

List of Resolved Problems

Resolved Problems in V3.03.02p18

ZDD04119/ZDD04171

- First Found-in Version: V3.03.02p16
- Condition: Device with LLDP running, such as IP Phone, is connected to switch. The switch receives LLDP packets from the IP Phone and sets up LLDP neighbor information entry. And the chassisID of the neighbor information is net address.
- Description: The chassisID in the LLDP information displayed on the switch is not correct.

LSOD10389

- First Found-in Version: V3.03.02p16
- Condition: With AAA local authentication and the blacklisting action of lock or lock-time configured (by the password-control login-attempt command), a Telnet, FTP, or SSH user who failed to login after the specified number of consecutive attempts uses the correct password to log in.
- Description: The user logged in, so the blacklist function did not work.

LSOD10395/LSOD10396

- First Found-in Version: V3.03.02p16
- Condition: Switch serves as DHCP relay, it receives DHCP discover packet, the bootp flag of which is 0x0001.
- Description: The switch drops DHCP packet, and DHCP client can not get IP address.

Resolved Problems in V3.03.02p16

LSOD10340

- First Found-in Version: V3.03.02p15
- Condition: Configure dot1x function, and the dot1x authentication-method is EAP. In one second, the dot1x client sends two EAPOL-start packets to trigger an authentication.
- Description: The dot1x authentication failed.

LSOD10272/LSOD10301

- First Found-in Version: V3.03.02p15
- Condition: With stack and link aggregation over units, the master port from one device has configured 'port trunk permit vlan all', the slave port from other device has configured 'port trunk permit vlan 1'.
- Description: The slave port is not selected. Configure 'port trunk permit vlan all' under this port is invalid.

LSOD10303/LSOD10306

- First Found-in Version: V3.03.02p15

- Condition: Enable DHCP relay with valid configuration. Make the relay receive DHCP inform packet from client.
- Description: DHCP inform packet will be relayed to DHCP server, but the sources IP of the relayed inform packet will be not DHCP relay's input interface.

LSOD10299/LSOD10302

- First Found-in Version: V3.03.02p15
- Condition: Enable DHCP relay with valid configuration and system server group 1 is referred by VLAN interface, and DHCP client successfully apply IP address. Create another server group 0 and then delete it in system mode.
- Description: After irrelevant server group 0 being created and deleted, DHCP client can not get IP address.

LSOD10298

- First Found-in Version: V3.03.02p13
- Condition: Execute command 'display transceiver interface <port number>' to show the information of a XENPAK module, which is in the slot of 10GE expansion card.
- Description: The system prompts 'Error: The transceiver is absent. '.

Resolved Problems in V3.03.02p15

LSOD10082/LSOD10232

- First Found-in Version: V3.03.02p14
- Condition: When STP is disabled, 'loopback internal' test is executed on port A. At the same time, port B receives an STP packet. Port A and port B are in the same VLAN.
- Description: STP packet is sent back from port B.

LSOD10247/LSOD10274

- First Found-in Version: V3.03.02p14
- Condition: Use the command 'port-security trap dot1xlogon', 'port-security trap dot1xlogoff' or 'port-security trap dot1xlogfailure' to open the trap of dot1x, and the dot1x authentication-method is EAP, a user logs in successfully, and change the username when doing re-authentication.
- Description: Although the re-authentication is successful, the username in the trap dose not change.

ZDD03292/ZDD03331

- First Found-in Version: V3.03.02p14
- Condition: Configure the switch as DHCP client, and there is no END option in ACK packet from DHCP server.
- Description: The switch can not get IP address.

LSOD10189/LSOD10187

- First Found-in Version: V3.03.02p14
- Condition: Plug in BIDI fiber module.

- Description: The fiber module type is different between log information and the information displayed by command 'display transceiver interface'.

LSOD10163

- First Found-in Version: V3.03.02p14
- Condition: In stack, configure 10GE link-aggregation across unit, member port A is trunk type, save the configuration and reboot the stack.
- Description: Port A changed from trunk type to access type.

LSOD10207

- First Found-in Version: V3.03.02p14
- Condition: Configure the device through Web. Select 'Port > MAC Address [Add]' from the navigation tree to add MAC address to a port of specified VLAN.
- Description: Cannot choose a port of specified VLAN to add MAC address.

LSOD10180

- First Found-in Version: V3.03.02p14
- Condition: When the first octet of the MAC address of the client or the gateway is not 0x00(such as 30-00-00-00-00-01).
- Description: The EAD-Quick-Deploy feature doesn't work.

Resolved Problems in V3.03.02p14

LSOD10079

- First Found-in Version: V3.03.02p13
- Condition: There are telnet users on device, executing 'display users all' command.
- Description: The IP address is reduplicated in the result. For example (the italic part is unwanted):

```
<sysname>display users all
```

	UI	Delay	Type	Ipaddress	Username	Userlevel
F 0	AUX 0	00:01:09				3
F 1	AUX 1	00:00:00				3
2	AUX 2					
3	AUX 3					
4	AUX 4					
5	AUX 5					
6	AUX 6					
7	AUX 7					
+ 18.118.118.458	VTY 0	00:00:13	TEL	18.118.118.45		3
+ 18.118.118.1119	VTY 1	00:00:03	TEL	18.118.118.111		3
10	VTY 2					
11	VTY 3					
12	VTY 4					
+	:	User-interface is active.				
F	:	User-interface is active and work in async mode.				

LSOD10176

- First Found-in Version: V3.03.01p01
- Condition: After two or more vlan-interfaces are configured, expansion card is pulled out and inserted again. Packets with subnet-directed broadcast IP are received by the expansion card, and the destination subnet is local.
- Description: IP forward-broadcast doesn't work. If the device is rebooted with required configuration, this problem also occurs. However, it doesn't always happen when a stack is rebooted.

LSOD10166

- First Found-in Version: V3.03.02p07
- Condition: In stack system, configure 'mac-address max-mac-count X' on several ports; send a lot of ARP packets with unknown source MAC to port A of slave device.
- Description: The CPU usage of device is up to 100%.

LSOD10077

- First Found-in Version: V3.03.02p11
- Condition: In a fabric, both master and slave were attacked by telnet log on packets.
- Description: The ACL resources will leak on master and slave.

LSOD09951

- First Found-in Version: V3.03.02p04
- Condition: Devices are in a fabric and dot1x is enabled. Radius server is connected to the fabric through an expansion module with 10GE port. Reboot the fabric.
- Description: There is a little possibility that user connected to the units without expansion module may fail to be authenticated.

Resolved Problems in V3.03.02p13**LSOD10155**

- First Found-in Version: V3.03.02p11
- Condition: Log in to a device through the console port and set it to full startup mode in Boot Menu.
- Description: There are garbled characters displayed on the user terminal.

LSOD10050

- First Found-in Version: V3.03.02p11
- Condition: Configure 'pki certificate access-control-policy', then add and remove related certificate attribute access control rule.
- Description: Every operation will lead to 1056 bytes memory leak.

LSOD10083

- First Found-in Version: V3.03.02p12
- Condition: Switch serves as DHCP snooping, and it receives bootp packets or abnormal DHCP packets without option 53.
- Description: Switch reboots abnormally.

LSOD10090

- First Found-in Version: V3.03.02p11
- Condition: Configure several VRRP backup groups. Execute command 'display vrrp interface vlan vlanid' or 'display vrrp interface vlan vlanid vrid vridnumber'.
- Description: Every operation of display will lead to 32 bytes memory leak.

Resolved Problems in V3.03.02p12**LSOD10016**

- First Found-in Version: V3.03.02p11
- Condition: Switch serve as DHCP snooping, and it receives DHCP ACK packets with source UDP port 4011.
- Description: DHCP snooping can not transmit those DHCP ACK packets.

LSOD10023

- First Found-in Version: V3.03.02p07
- Condition: Switch serves as DHCP relay and DHCP snooping, PC gets IP address through switch and renews its IP address.
- Description: When PC renew its IP address, DHCP snooping can not refresh its item.

LSOD10029

- First Found-in Version: V3.03.02p07
- Condition: Using DC power
- Description: There is 'Power 1: Get Temperature failed' while executing command 'display environment'.

LSOD10030

- First Found-in Version: V3.03.02p11
- Condition: Insert an expansion card into the device.
- Description: About 180KB memory leaks on main board.

Resolved Problems in V3.03.02p11**LSOD09957**

- First Found-in Version: V3.03.02p05
- Condition: Configure VLAN-interface A and B on the device. Configure IP address of B as NAS-IP address of the RADIUS scheme. Do dot.1X authentication with RADIUS server.
- Description: NAS-IP address in RADIUS Authentication-Request packet sent to server is IP address of A, not B.

LSOD09962

- First Found-in Version: V3.03.02p07
- Condition: Configure supp-timeout period to X seconds with 'dot1x timer supp-timeout' command. Configure retry times to Y seconds with 'dot1x retry' command. The result X multiplied by Y is

larger than 80. Configure 'dot1x authentication-method eap'. Do dot1X authentication. The dot1X client doesn't response to EAP challenge packet.

- Description: When authentication fails, the device doesn't send failure packet.

ZDD02999

- First Found-in Version: V3.03.02p07
- 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.

LSOD09929

- First Found-in Version: V3.03.01p01
- Condition: Firstly create at least two VLAN interfaces and they are all up, secondly configure a loopback interface, finally delete the earliest VLAN interface.
- Description: The loopback interface can't ping successfully.

LSOD09894

- First Found-in Version: V3.03.02p07
- Condition: CPU is busy and there is a lot of trap information in a moment.
- Description: device reboots abnormally.

LSOD09928

- First Found-in Version: V3.03.02p07
- 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.

LSOD09920

- First Found-in Version: V3.03.02p07
- 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.

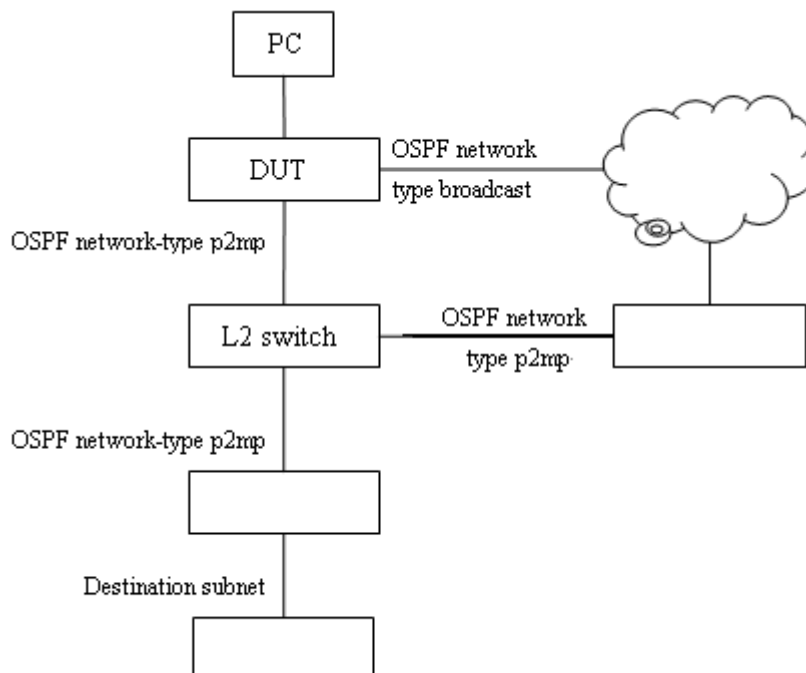
LSOD09911

- First Found-in Version: V3.03.02p07
- Condition: The switch is enabled with DHCP snooping. The PXE client obtains an IP address through the switch, and downloads the bootstrap program and boot menu through the switch.
- Description: The PXE client can obtain an IP address successfully, but it fails to download the bootstrap program and boot menu.

LSOD09808

- First found-in version: V3.03.01
- Condition: n the following network, OSPF is enabled on a device, and 'ospf network-type p2mp' is configured on some interfaces. Some 32-bit host routes are learnt on the P2MP interfaces. There are two or more non-ECMP routes for a specified destination sub-network and the route via

P2MP interface is preferred. The next-hop of the preferred route has a 32-bit host route. If the P2MP interface breaks, the route switches to a broadcast interface. After a while, the P2MP link restores.



- Description: After the P2MP link restores, both routing table and fib table restore normal. However, the data flow doesn't always switch back to the P2MP interface.

LSOD09745

- First Found-in Version: V3.03.02p04
- Condition: In a stack, dot1x is not enabled globally, but enabled on several ports.
- Description: Attempt to execute 'dot1x' globally times out and fails.

LSOD09830

- First Found-in Version: V3.03.02p05
- Condition: The client application does dot1x authentication with TTLS certification.
- Description: By chance, the device reboots abnormally for dead loop.

LSOD09815

- First Found-in Version: V3.03.01
- Condition: In PIM SM protocol, the device receives a assert message from the incoming interface, while the PIM routing entry's RPF neighbor is NULL.
- Description: The device reboots abnormally.

LSOD09837

- First Found-in Version: V3.03.02p07
- Condition: Switch serves as DHCP relay, two PCs get IP address through two different relay interfaces.
- Description: In the offer packets that switch sent to PC, the source IP address in IP header is incorrect.

ZDD02827

- First Found-in Version: V3.03.02p07
- Condition: Switch serves as DHCP relay and it receives a bootp packet without magic cookie.
- Description: The switch regards the packet as wrong one and drops it.

LSOD09809

- First Found-in Version: V3.03.02p07
- Condition: The configuration file of each switch in a stack includes 'abr-summary' command. Reboot each switch independently in order to constitute the stack. The master originated the LSA that came from the 'abr-summary' command.
- Description: The slave will be rebooted repeatedly and can not join the stack.

LSOD09746

- First Found-in Version: V3.03.02p07
- Condition: DHCP-snooping is enabled on a stack. Reboot the stack, and the starting processes of the devices are finished at different time.
- Description: After the stack is reestablished, the DHCP clients on slave devices probably can't get IP addresses.

LSOD09762

- First Found-in Version: V3.03.02p07
- Condition: Set the combo fiber port to down using 'shutdown' command.
- Description: Use command 'undo shutdown' to enable the combo copper port, but the port can not link up.

LSOD09829

- First Found-in Version: V3.03.02p01
- Condition: Enable mac-authentication and set the offline-detect timer to be smaller 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.

LSOD09811

- First Found-in Version: V3.03.02p07
- 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.

LSOD09797

- First Found-in Version: V3.02.02p01
- Condition: The BPDU-tunnel function for protocol A is enabled on a device.

- Description: The source MAC address (named as MAC_X) of packets which belongs to protocol A may be learned incorrectly, therefore packets whose destination MAC address is MAC_X can't be forwarded normally.

LSOD09619

- First Found-in Version: V3.03.02p07
- Condition: The network device acted as SSH server, and received specific SSH attack packets.
- Description: The device will be rebooted abnormally.

LSOD09678

- First Found-in Version: V3.03.02p03
- 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.

LSOD09700

- First Found-in Version: V3.03.02p07
- Condition: Enable DHCP server and DHCP snooping on switch. The pool lease of DHCP server is set less than one minute, and lots of users get IP address from switch.
- Description: The memory exhausted on switch.

LSOD09722

- First Found-in Version: V3.03.02p07
- Condition: In 'radius scheme A' view, configure 'primary authentication' command with IPv4 address, 'secondary authentication' command with IPv6 address.
- Description: If primary authentication server does not response, the switch tries to do authentication with secondary server, but the authentication fails.

Resolved Problems in V3.03.02p07

LSOD09499

- First Found-in Version: V3.03.02p05
- Condition: When 802.1X authentication and mac-authentication are both enabled on the port, the user first pass the mac-authentication and success get IP address by DHCP, then do 802.1X authentication success and get IP address by DHCP again.
- Description: Sometimes the IP address shown by the command "display connection" is in reverse order.

LSOD09555

- First Found-in Version: V3.03.02p05
- 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: V3.03.02p03
- 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.

LSOD09598

- First Found-in Version: V3.03.02p05
- Condition: Configure 'accounting optional'. And 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.

LSOD09554

- First Found-in Version: V3.03.02p05
- Condition: The switch enables DHCP snooping and the up-link port of the switch is configured as the trust port of DHCP snooping. The DHCP server and the user's PC are connected to the up-link port of the switch.
- Description: DHCP snooping record the user item on trust port.

LSOD09324

- First Found-in Version: V3.03.02p05
- Condition: Configure IPv6 ACL rule including COS or VID by WEB or command line.
- Description: The rule is configured successfully by WEB, but unsuccessfully by command line.

LSOD09537

- First Found-in Version: V3.03.02p05
- Condition: 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.

LSOD09483

- First Found-in Version: V3.03.02p05
- Condition: Test the IPV6 communication between a device and a stack that has an aggregation group across different units.
- Description: The stack device can not communicate with other device.

LSOD09498

- First Found-in Version: V3.03.02p05
- 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.

LSOD09533

- First Found-in Version: V3.03.02p05
- Condition: The last two combo ports of the device are link-up. Reboot the device.
- Description: During booting, the last two combo ports status change from down to up twice.

LSOD09434

- First Found-in Version: V3.03.02p05
- 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: V3.03.02p05
- 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.

LSOD09406

- First Found-in Version: V3.03.02p03
- Condition: There are many switches serve as DHCP snooping in network. PC applies for IP address through DHCP snooping and finally get a conflict one.
- Description: The DHCP Decline packets broadcast in network for a while.

LSOD09332

- First Found-in Version: V3.03.02p03
- Condition: Configure DHCP rate limit on port, and display the configuration.
- Description: The switch shows the default configuration.

LSOD09048

- First Found-in Version: V3.03.02p03
- Condition: Configure the ipv6 ACL that include destination IP address and source IP address in sequence.
- Description: The source IP address includes part of the destination IP address in the current information.

LSOD09369

- First Found-in Version: V3.03.02p04
- Condition: An OSPF route has N (N>1) next hops, IP_A is old next hop, whose cost is Cost_A, IP_B is current next hop, whose cost is Cost_B, Cost_B<Cost_A.
- Description: The next hop of the route can not be refreshed.

LSOD09439

- First Found-in Version: V3.03.01
- 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: V3.03.01p05
- Condition: Connect device to HUAWEI S2300 and running LLDP.
- Description: The device can not find S2300 as LLDP neighbor.

LSOD09295

- First Found-in Version: V3.03.02p03
- Condition: Dot1x is enabled on a device. Ping the device with IPv6 address from an unauthenticated PC.
- Description: The device makes a response to the ping request.

LSOD09478

- First Found-in Version: V3.03.02p05
- Condition: Switch serves as DHCP snooping, and PC get IP address through DHCP snooping.
- Description: Switch will drop those packets without option 51 for it checks the option51 of DHCP ACK packet.

LSOD09333

- First Found-in Version: V3.03.02p05
- Condition: On stack, enter RADIUS scheme view, set the status of a secondary accounting server to block. Then display the status of RADIUS server with 'display radius scheme' command.
- Description: The status of primary authentication server, secondary authentication server on slave units is unexpectedly changed to block.

LSOD09263

- First Found-in Version: V3.03.02p04
- 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. '.

LSOD09123

- First Found-in Version: V3.03.02p05
- 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 log-on, although the password configuration of local-user A is null or it is not consistent with remote server.

LSOD09283

- First Found-in Version: V3.03.02p04
- 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: V3.03.02p05
- 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.

LSOD09273

- First Found-in Version: V3.03.02p04
- Condition: Remove the ACL which is applied with 'packet-filter' command globally.
- Description: The information prompted is incorrect: 'Error : Acl 4003 has been applied by packet-filter action on port ? can not be deleted or changed!' The correct information should be: 'Error : Acl 4003 has been applied by packet-filter action on global, can not be deleted or changed!'

LSOD09278

- First Found-in Version: V3.03.02p04
- 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: V3.03.02p04
- 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.

LSOD09322

- First Found-in Version: V3.03.02p04
- Condition: Binding static item in DHCP interface pool, save this configuration and reboot switch.
- Description: The configuration of static binding item is lost.

LSOD09052

- First Found-in Version: V3.03.02p04
- 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.

LSOD09717/LSOD09709

- First Found-in Version: V3.03.02p05

- Condition: Configuring 'authentication-mode scheme command-authorization' on the user interface, a user telnet the switch and logging 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.

LSOD09572/LSOD09605

- First Found-in Version: V3.03.02p05
- Condition: Configuring the switch as a DHCP server, an IP phone connecting the switch and getting voice VLAN ID and IP address from the switch.
- Description: The IP phone can not get voice VLAN ID and IP address successfully within 25 seconds.

LSOD09630/LSOD09653

- First Found-in Version: V3.03.02p05
- Condition: The device on which STP is enabled by default, receiving STP TC BPDU.
- Description: Dynamic MACs on stp-edged ports and stp-disabled ports will be deleted also.

Resolved Problems in V3.03.02p05

LSOD09096

- First Found-in Version: V3.03.02p03
- Condition: Connect PC to port A of a slave device in stack. After reboot the slave device, the port A enters guest-VLAN.
- Description: Display interface information on the master of stack. It is shown that the port A is not in the guest-VLAN.

LSOD09204

- First Found-in Version: V3.03.02p03
- 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-withoui). 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: V3.03.02p03
- 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.'

LSOD09156

- First Found-in Version: V3.03.02p04
- Condition: In stack, do 802.1X authentication with iMC server. User A log-in, then user B log-in from another device of the fabric with the same user-name of A.
- Description: The iMC server forces user A to log-out.

LSOD08866

- First Found-in Version: V3.03.02p03
- Condition: Walk the entAliasMappingIdentifier node.
- Description: The multiple entities of walk result have the same index which causes the failure in synchronizing device data through SNMP network management.

LSOD09143

- First Found-in Version: V3.03.02p03
- 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.

LSOD09176

- First Found-in Version: V3.03.02p03
- Condition: Enable voice VLAN legacy and connect an IP phone to switch.
- Description: The switch may ignore CDP packets from IP phone, and voice VLAN will not work.

ZDD02426

- First Found-in Version: V3.03.02p04
- Condition: The device has an 8-SFP expansion module where several optical modules including 100M SFP are plugged. Reboot it from CLI.
- Description: There is remote possibility that all optical modules on the expansion module can't be identified.

Resolved Problems in V3.03.02p04

LSOD09059

- First Found-in Version: V3.03.00
- 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.

ZDD02152

- First Found-in Version: V3.03.02p03
- Condition: Switch work as Telnet client or server. Input non-english character after login.
- Description: Possible unexpected logout.

LSOD08964

- First Found-in Version: V3.03.02p03
- Condition: Enable DHCP snooping and DHCP snooping option 82 on switch with replacing strategy.
- Description: Switch can not replace OPTION 82 of DHCP discover packet correctly.

LSOD09106

- First Found-in Version: V3.03.02p03
- Condition: EAD fast deployment is enabled on the port connecting the switch to a client, and no VLAN-interface is created for the VLAN where the port resides. The client sends repetitive HTTP requests or out-of-sequence HTTP packets when it is unauthenticated and accesses the network.
- Description: A memory leak occurs.

LSOD09080

- First Found-in Version: V3.03.02p03
- Condition: Access MIB node "hwNDPPortStatus" on a stack.
- Description: Each slave unit leaks 9K-byte memories every time. No memory leakage occurs on master unit.

LSOD08774

- First Found-in Version: V3.03.02p01
- Condition: Do EAD authentication with iMC server.
- Description: The user goes off-line soon after passing the security checking.

LSOD09095

- First Found-in Version: V3.03.01p07
- Condition: Enable 802.1x 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 802.1x 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.

LSOD09097

- First Found-in Version: V3.03.02p03
- Condition: The device has been configured user ACL remark VLAN ID, and user VLAN ID is configured as multicast VLAN ID. The device receives IGMP report message from the host.
- Description: The device can not transmit IGMP report message to upstream device periodically, so as to multicast stream to be interrupted.

LSOD09102

- First Found-in Version: V3.03.00
- Condition: Set up an extended IP ACL with number 3000, and add a rule with protocol key. Such as "rule 0 permit ip", in which "ip" means IP protocol. View the configuration file by "more" command after saving configuration, or display the current configuration.
- Description: The protocol key of the rule in the configuration becomes capital, and it will be lowercase in current version. For example, former version shows up "rule 0 permit IP" and current version shows "rule 0 permit ip". There is no any effect for function.

LSOD09100

- First Found-in Version: V3.03.02p03

- Condition: Net management software, which is using SNMP, is connected to the slave device in a stack.
- Description: Execute setting operation; the operation can be succeeding, but the device cannot send SNMP response to the net management software.

LSOD09045

- First Found-in Version: V3.03.02
- Condition: A large amount of security MAC addresses are learnt in a stack.
- Description: Several MAC address can not be aged after aging timer is reached.

LSOD08988

- First Found-in Version: V3.03.02p03
- Condition: One user with privilege level 0 login the web management interface.
- Description: WEB can not show the page of "Help".

Resolved Problems in V3.03.02p03

LSOD08968

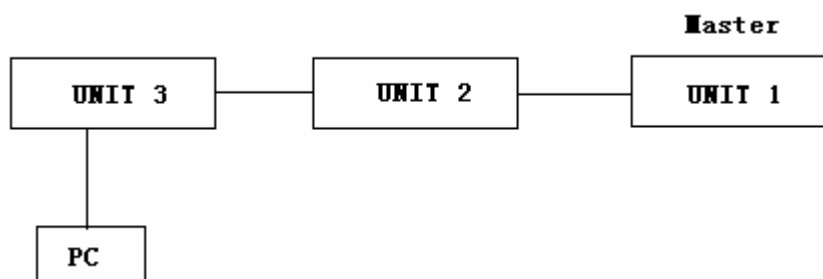
- First Found-in Version: V3.03.02p01
- Condition: Enable mac-authentication and set the offline-detect timer to be larger than one half of mac-address aging timer on the switch. And connect a PC to the switch to do mac-authentication, but the traffic sent from the PC is very small, such as only sending 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.

LSOD08964

- First Found-in Version: V3.03.02p01
- Condition: A switch serves as DHCP SNOOPING, and enable DHCP SNOOPING OPTION 82 function with replace strategy on the switch.
- Description: The switch can not replace the OPTION 82 of DHCP discover packet correctly.

LSOD06917

- First Found-in Version: V3.03.02p01
- Condition: In the following network, the monitor port is on the master device (UNIT 1). After rebooting fabric with saved configuration, configure the ports of UNIT 3 as the source mirroring port and the monitor port.



- Description: The fabric can't ping the PC connected to the mirroring port successfully.

LSOD08776

- First Found-in Version: V3.03.02p01
- Condition: Execute "ip host" command and the "hostname" parameter includes "-" character.
- Description: The command fails and the message of "Invalid host name format!" is prompted.

LSOD08895

- First Found-in Version: V3.03.01p05
- Condition: DHCP relay and MSTP are enabled on a device. The device is connected to a DHCP server through VLAN A on a port on the expansion card, and connected to a DHCP client through VLAN B on another port, and VLAN B i
- Description: DHCP relay function becomes invalid.

LSOD08757

- First Found-in Version: V3.03.02p01
- Condition: Enable NDP on a fabric system and many NDP adjacent devices attached to the same port of the device.
- Description: When getting the NDP neighbor information through SNMP, the usage of CPU of the device is high.

LSOD08789

- First Found-in Version: V3.03.01p05
- Condition: The device with a dual-10GE expansion module has learned many dynamic routes and received various exceptional packets.
- Description: There is little probability that the expansion module restarts by itself and output logs as below:

```
%Mar 6 05:38:50:138 2009 sysname IFNET
%Mar 6 05:39:17:540 2009 sysname IFNET
```

LSOD08892

- First Found-in Version: V3.03.02p01
- Condition: The devices are in a fabric. Lots of VLAN and some MSTP instances are configured. Execute the command "active region-configuration".
- Description: There is little probability that the command fails and the device outputs the following information:

```
Command synchronization failed, please try later...
```

LSOD08905

- First Found-in Version: V3.03.02p01
- Condition: Execute command "display memory" in a stack composed of multiple devices. Press "Ctrl+C" before the display process completes.
- Description: A memory leak of 1K bytes occurs.

LSOD08907

- First Found-in Version: V3.03.02p01
- Condition: Access a device repeatedly by SSH with public key authentication.
- Description: An exception may occur on the device at little probability.

LSOD08729

- First Found-in Version: V3.03.02p01
- Condition: Set port-security as "and" mode in device. Some users do MAC and dot1x authentication on several ports at the same time.
- Description: The dynamic "auto vlan" is added to some port's configuration.

LSOD08843

- First Found-in Version: V3.03.02p01
- Condition: Set port-mirroring function on web.
- Description: The CPU usage of device is up to 100%, and the information of port-mirroring can't be normally displayed at web view.

LSOD08788

- First Found-in Version: V3.03.02p01
- Condition: The 802.1x server is CAMS or IMC, the device enable DHCP snooping or DHCP relay, the 802.1x client which is on-line requests ip address frequently.
- Description: The device send accounting update packet to server frequently, which lead the 802.1x client off-line.

LSOD08808

- First Found-in Version: V3.03.02p01
- Condition: The IP address of a WEB server is the same as that of the vlan-interface of a device.
- Description: After user login through web-authentication, the user's layer-2 traffic can't be forwarded normally.

LSOD08874

- First Found-in Version: V3.03.02p01
- Condition: When congestion happens on a port, enable burst mode function.
- Description: All packets can't be forwarded on the port.

LSOD08878

- First Found-in Version: V3.03.01p05
- Condition: Lots of mac-authentication users are online and run for a long time.
- Description: Check the user information by the command of "display mac-authentication interface xxx", some users are not online, but their MAC addresses exist when checking the MAC address table by "display mac-address".

Resolved Problems in V3.03.02p01

LSOD08570

- First found-in version: V3.03.02
- Condition: Enable the port security feature on a stack, and set the intrusion mode to **blockmac**. After one port (for example, port A) learns some blocked MAC addresses, remove the device to which port A belongs from the stack.
- Description: Such blocked MAC addresses on the other devices of the stack can not be removed.

LSOD08631

- First found-in version: V3.03.02
- Condition: Enable 802.1X and debugging for RADIUS packets. Lots of users log on and then log off.
- Description: The device reboots.

LSOD08734

- First found-in version: V3.03.02
- Condition: Enable STP and loopback detection in both interface view and system view. A loop occurs on the port.
- Description: The loop on the port can not be detected.

LSOD08575

- First found-in version: V3.03.02
- Condition: When **non-flooding** is enabled, the device acts as the NTP client in the multicast mode to synchronize timekeeping.
- Description: The timekeeping of the device can not be synchronized.

LSOD08721

- First found-in version: V3.03.02
- Condition: The device is enabled with DHCP Snooping, quick EAD deployment, and ARP detection. Additionally, its port connected to a PC is configured with IP check. Use the **shutdown** command to shut down the port connected to the PC and configure the **am user-bind** command to bind the IP and MAC addresses of the PC to the switch. Then use the **undo shutdown** command to bring up the port and cancel the binding.
- Description: The PC can not access the gateway after it gets an IP address.

LSOD08656

- First found-in version: V3.03.02
- Condition: Configure the **multicast static-group** command on a device configured with multicast VLAN.
- Description: When deleting the **multicast static-group** configuration, you cannot delete the IGMP snooping group.

LSOD08702

- First found-in version: V3.03.02

- Condition: Execute the **display interface** command.
- Description: The values of the "Last 300 seconds input" field and the "Last 300 seconds output" field are always zero.

LSOD08667

- First found-in version: V3.03.02
- Condition: Use the **display transceiver xxx** command to check the Copper SFP information.
- Description: The device does not support displaying Copper SFP information.

LSOD08674

- First found-in version: V3.03.02
- Condition: In a stack, there is **global am user-bind** in the rebooting configuration file. After rebooting, the minimum Unit ID is not that of the master. Configure **global am user-bind** again and then delete all the **global am user-bind** from the slave units.
- Description: The device displays the checksum different from that of unit 1 when you save the configuration.

LSOD08665

- First found-in version: V3.03.02
- Condition: In a stack, enable port security in autolearn mode and aging mode on ports. After the security MAC is learnt, disable the port security feature when the security MAC is aging.
- Description: The device reboots.

LSOD08713

- First found-in version: V3.03.02
- Condition: Display the voice VLAN information of an LLDP neighbor.
- Description: The COS value and DSCP value of the voice VLAN are incorrect.

LSOD08716

- First found-in version: V3.03.02
- Condition: Configure the **lldp compliance CDP** command on a switch to communicate with a Cisco device through Cisco CDP version 1.
- Description: The duplex mode of the LLDP neighbor displayed is incorrect.

LSOD08678

- First found-in version: V3.03.02
- Condition: Reboot the master device of a stack.
- Description: Failed to discover LLDP neighbors on an STP port in Discarding state.

LSOD08717

- First found-in version: V3.03.02
- Condition: Enable the IP check function, the IP check static binding function, and the MFF user port function on the same port of a switch.
- Description: The switch reboots abnormally.

LSOD08726

- First found-in version: V3.03.02
- Condition: There are several units in a stack. Reboot the master device of the stack.
- Description: The VRRP function becomes abnormal.

LSOD08679

- First found-in version: V3.03.02
- Condition: Units A, B, and C are in the same stack. An 802.1x user logs in through Port X of unit A, and Port X is assigned to the authorization VLAN (PVID or auto VLAN). Reboot unit B. Then the user in unit A logs off, and port X leaves the authorization VLAN.
- Description: After the user logs off, execute the **display interface** command on units A and B to display information about port X. It is showed that the port is no longer in the authorization VLAN. Execute the **display** command on unit C, and it is showed that the port is still in the authorization VLAN.

LSOD08657

- First found-in version: V3.03.02
- Condition: In a stack device, configure port security in autolearn mode for a port, and set the max-mac-count limit. Let the port learn MAC addresses automatically, and make MAC count of the port reach the limit.
- Description: Try to add one more MAC address to the port using the **mac-address security** command. Although a failure information is showed, the **display mac-address** command shows that the additional MAC address is added actually, making the MAC count of the port exceed the limit.

LSOD08652

- First found-in version: V3.03.02
- Condition: Add a hybrid port to the Guest VLAN of 802.1x, and then use the **undo port hybrid vlan** command to remove the port from the Guest VLAN.
- Description: The **display interface** command shows that the port is still in the Guest VLAN. Actually, the port is not in the VLAN.

LSOD08675

- First found-in version: V3.03.02
- Condition: In a stack, a port in unit A is assigned to the guest VLAN (VLAN x) of port security. Then send packets of verified source MAC addresses to the port continuously.
- Description: After the port is removed from the guest VLAN, PVID of the port changes back to the original VLAN y. Execute the **display mac-address** on unit B, and some dynamic MAC addresses in VLAN y without authentication are displayed.

LSOD08281/LSOD08283

- First found-in version: V3.03.01p05
- Condition: Specify an NTP server (e.g. 1.1.1.2) on the device, without specifying a source interface or source address. The device selects a source address automatically (e.g. 1.1.1.1) to communicate with the specified server. After a while, the device synchronizes its time with the

NTP server. If the topology or the routing table changes, the device cannot communicate with the NTP server through the selected source address.

- Description: When the topology or the routing table changes, the device still uses the old source address (e.g. 1.1.1.1) as the source address of NTP requests. Therefore, NTP responses from the NTP server cannot be delivered correctly to the device, and the device fails to synchronize its time with the NTP server.

LSOD08260/LSOD08278

- First found-in version: V3.03.01p05
- Condition: Run command "update fabric <filename>" on device A, which is in a stack.
- Description: When the command is run, a memory leakage of 256 bytes occurs on device A.

LSOD08334/LSOD08346

- First found-in version: V3.03.01p05
- Condition: Log in to the switch by using the URL address `http://x.x.x.x:23` (x.x.x.x is the device's IP address), and refresh the web page several times.
- Description: The switch reboots abnormally.

LSOD08306/LSOD08308

- First found-in version: V3.03.01p05
- Condition: In a stack, repeatedly execute the following commands: "build XXX", "anagement-vlan synchronization enable" and "undo build" orderly, then save the configuration.
- Description: Saving the configuration fails.

LSOD08377/LSOD08395

- First found-in version: V3.03.01p05
- Condition: Inject heavy traffic with priority 7 to the CPU of a single-10GE expansion card or a dual-10GE expansion card, such as OSPF traffic with destination IP address 224.0.0.5 or 224.0.0.6, RIP traffic with destination IP address 224.0.0.9, PIM traffic with destination IP address 224.0.0.13, VRRP traffic with destination IP address 224.0.0.18, NTDP traffic, HGMP traffic, etc.
- Description: The status of the expansion card becomes abnormal after long-term injection, and the device displays the prompt: "The x board 1 adaptor is removed" (x is equal to unit ID - 1).

LSOD08388/LSOD08412

- First found-in version: V3.02.00p01
- Condition: Configure an IP address for a VLAN interface and a static route repeatedly. The VLAN interface is in up state and its IP address is the same as the next hop of the configured static route. For example:
 - [sysname] ip route-static 10.1.1.0 24 1.1.1.1
 - [sysname-Vlan-interface1] ip address 1.1.1.1 24
- Description: The direct route of the VLAN interface is lost from the FIB table and pinging another IP address in the subnet fails.

LSOD08392/LSOD08431

- First found-in version: V3.03.02

- Condition: After a switch gets an IP address through DHCP successfully, configure a manual link-aggregation group, and then display detailed information about the link-aggregation group.
- Description: The switch reboots abnormally.

LSOD08440/LSOD08445

- First found-in version: V3.03.02
- Condition: Insert an ESFP 100M optical module into a port.
- Description: The transceiver type of the port displayed with the **display transceiver interface** command is UNKNOWN_SFP, which should be 100_BASE_LX_SFP.

LSOD08318/LSOD08473

- First found-in version: V3.03.02
- Condition: The device is enabled with DHCP snooping and quick EAD deployment, and its port connected to a PC is configured with IP check.
- Description: The PC can access the network freely without passing dot1x authentication after it gets an IP address.

LSOD08460/LSOD08482

- First found-in version: V3.03.02
- Condition: The device is enabled with voice VLAN, dot1X (or port-security in userlogin, userloginext, or userloginsecure mode) and DHCP-launch.
- Description: A PC connected to the device fails dot1X authentication and thus cannot access the network.

LSOD08486/LSOD08487

- First found-in version: V3.02.04p01
- Condition: Configure the last two COMBO ports to work in 100M/FULL or 100M/HALF mode, use a straight-through cable to connect them, and then perform an optical-to-electrical change to the COMBO ports.
- Description: The two COMBO ports cannot go up.

LSOD08537/LSOD08540

- First found-in version: V3.03.02
- Condition: Devices form a stack.
- Description: When the stack ports receive invalid packets (length < 64B), there is little probability that commands executed run slowly and some packets are dropped in the stack. And the problem persists.

LSOD08554/LSOD08576

- First found-in version: V3.03.02
- Condition: There are security MAC addresses in the switch. Then walk the dot1qTpFdbStatus node through SNMP.
- Description: The result is incomplete.

Resolved Problems in V3.03.02

LSOD08196

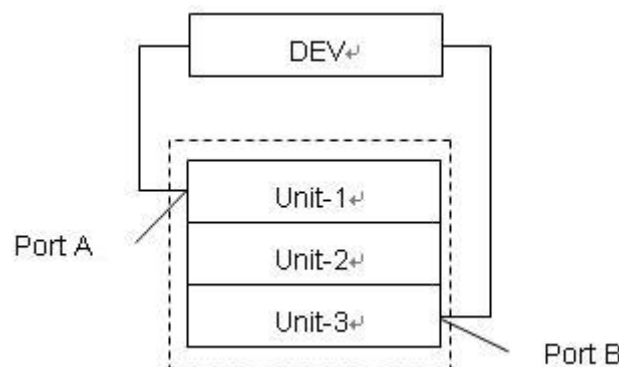
- First found-in version: V3.03.01p05
- Condition: The switch is the first-hop router of a multicast source. A device of another vendor (for instance IP 8800 of NEC) is the RP. The RP cannot create multicast forwarding entries through PIM null-register packets. The multicast forwarding table of the RP is aged out when the link between the first-hop router and RP is interrupted.
- Description: The RP cannot create the multicast forwarding table after the link is recovered.

LSOD08193

- First found-in version: V3.03.01p05
- Condition: Configure password information.
- Description: The password can be displayed in log information, which compromises security.

LSOD06161

- First found-in version: V3.03.00ep01
- Condition: In the network shown below, RSTP is configured, Port A is the root port, and Port B is an alternate port. Save the configuration and reboot Unit-1 and Unit-2 in sequence.



- Description: Temporary loop occurs in the network.

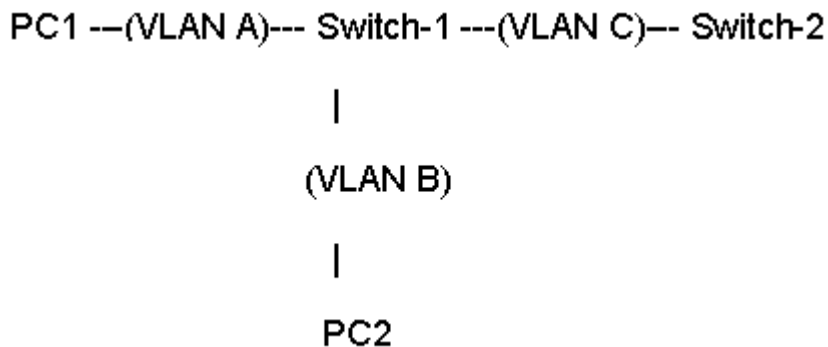
Resolved Problems in V3.03.01p05

LSOD07614

- First found-in version: V3.03.01p04
- Condition: Execute the **display power** command on a stacking device.
- Description: A memory leak of 2048 bytes occurs each time the operation is performed.

LSOD07718

- First found-in version: V3.03.01p04
- Condition: The network is shown below:



PC1 and PC2 communicate with each other at Layer-3 through Switch 1.

Configure a static ARP entry that has no VLAN ID or outbound interface specified for PC2 on Switch 1. After PC1 and PC2 communicate with each other, the egress port and VLAN ID (VLAN B) of the ARP entry are learned.

Then change the network as follows:

Remove VLAN B from Switch 1, configure VLAN B on Switch 2, and move PC2 from Switch 1 to Switch 2.

After that, all PC1, Switch 1, Switch 2 and PC2 communicate with one another at Layer-3.

The new network is shown below:



- Description: The ping operation from PC1 to PC2 fails. To solve the problem, you have to reboot Switch 1.

LSOD07630

- First found-in version: V3.03.01p04
- Condition: Perform EAD authentication on a port. Before authentication, the port's PVID is V1. During authentication, the port is assigned a VLAN ID of V2. V2 and V1 are not in the same MSTP instance.
- Description: EAD security policy authentication fails.

LSOD07571

- First found-in version: V3.03.01p03
- Condition: The switch works together with the CAMS server to implement RADIUS authentication. The CAMS server assigns an SSL VPN group number to the switch.
- Description: RADIUS authentication fails because the switch does not support the SSL VPN group number attribute.

LSOD07629

- First found-in version: V3.03.01p04
- Condition: Log in to the web interface, click Cluster -> Cluster Upgrade to view web version.

- Description: The format of web version is changed from s4ix.x.x-yyyy to s4ixx_yy.

LSOD07676

- First found-in version: V3.03.01p04
- Condition: Configure the **ip address dhcp-alloc** command on a VLAN interface.
- Description: The TTL of the DHCP Discover packet sent on the VLAN interface is 1. Because the DHCP relay agent drops packets with TTL being 1, the DHCP Discover packet can't be forwarded to the DHCP server.

LSOD07686

- First found-in version: V3.03.01p04
- Condition: A port on the expand board receives jumbo frames.
- Description: Jumbo frame statistics are available on that port regardless of whether the **giant-frame statistics enable** command is configured or not.

LSOD07700

- First found-in version: V3.02.04p06
- Condition: Two devices are connected with each other through a port aggregation group, and they are configured as a VRRP group.
- Description: After the VRRP master device is restarted, there is little probability that its VRRP virtual MAC address is learned by the link aggregation group and VRRP does not work normally.

LSOD07595

- First found-in version: V3.02.00p05
- Condition: A device is configured with one or more IP addresses and an expansion card with two 10-Gigabit ports is inserted into the device. The device runs for a long time.
- Description: There is little probability that some serious error occurs to the expansion card. Once the error occurs, the expansion card broadcasts all received packets in corresponding VLANs, and a host connected to the expansion card cannot access the device.

LSOD07119

- First found-in version: V3.03.01p04
- Condition: A stack serves as a DHCP client and gets an IP address from a DHCP server. Delete the IP address pool on the DHCP server.
- Description: After the DHCP client's IP address lease expires, the DHCP client state on the master device is different from that on slave devices in the stack.

LSOD07801

- First found-in version: V3.03.01p04
- Condition: Execute the **snmp-agent trap enable** command on the device. Then, execute the **display snmp-agent trap-list** command
- Description: The traps of the OADP module that is not supported by the device exist in the output information.

LSOD07873

- First found-in version: V3.02.01c04
- Condition: Several devices in a stack that serves as an SSH server are attacked by multiple illegal SSH users at the same time.
- Description: After a period, all VTY resources are used up, and legal SSH users cannot log in.

LSOD07623

- First found-in version: V3.03.01p04
- Condition: NTP is enabled on a stack. Power off the master device to use another device as the new master.
- Description: NTP function becomes invalid.

LSOD07808

- First found-in version: V3.03.01p04
- Condition: Enable DHCP-triggered authentication globally. Enable port security on the port connected to clients and set its security mode to **userlogin-secure-or-mac** or **userlogin-secure-or-mac-ext**.
- Description: DHCP packets cannot trigger authentication.

LSOD07757

- First found-in version: V3.03.01p04
- Condition: Pull out an expansion module of a slave device in a stack, and then insert it within 10 seconds.
- Description: The device outputs a log:

```
%Jun 25 15:28:27:239 2008 SWITCH DRIVER/5/WARN:- 2 -  
Error occurred while processing subcard insertion (code 0x8)
```

Using the **display drv-module all statistic** command, you can find the failure of QACL function from the output:

```
Error occurred 1 times among 2 times subcard insertion since start-up.  
Subcard insertion functions in the latest time failed:  
QACL,
```

As a result, ACL configuration errors occur on the expansion module, and the packets received on this module cannot be processed normally.

Resolved Problems in V3.03.01p04

LSOD07316

- First found-in version: V3.03.01
- Condition: Perform 802.1X authentication with the CAMS server. Before authentication, the port's VLAN ID is V1; after authentication, its VLAN ID is V2.
- Description: The online clients list on the CAMS server shows that the corresponding user's VLAN ID is V1 rather than V2.

LSOD07416/LSOD07422/LSOD07420/LSOD01108

- First found-in version: V3.02.04
- Condition: For an 802.1x authentication port, the dynamically assigned VLAN ID and the previous PVID are not in the same MSTP instance.
- Description: Authentication fails.

LSOD07375

- First found-in version: V3.03.01
- 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: V3.03.01p02
- Condition: Disable and then enable STP periodically on the device to cause frequent network topology changes.
- Description: There is little probability that the device reboots without exception information.

LSOD07124

- First found-in version: V3.03.01p02
- Condition: A stack serves as a DHCP relay agent. A PC gets an IP address through it, and then sends a DHCP inform packet to get extra information.
- Description: The DHCP relay agent does not process the DHCP ACK packet returned from the DHCP server correctly, and thus the PC cannot process the DHCP ACK packet.

LSOD07386

- First found-in version: V3.03.01p01
- Condition: A loopback is detected under a port after loopback-detection shutdown is enabled on the port.
- Description: The device may reboot.

LSOD07313

- First found-in version: V3.03.01
- Condition: Swap an SFP module within 5 seconds.
- Description: Check the SFP information with the **display transceiver** command. The information is not updated.

LSOD07467

- First found-in version: V3.03.01p02
- Condition: Send traffic out port A at a rate higher its maximum rate.
- Description: The dropped packets are not counted.

LSOD07414

- First found-in version: V3.02.00p01

- Condition: Configure ECMP routes on a device that has a 1-port or 2-port 10G expansion module. Reboot the device, or shutdown and then undo shutdown a VLAN interface that is the outbound interface of an ECMP route.
- Description: The ECMP route may become incorrect on the expansion module. As a result, IP packets received on a port of the expansion module and matching the ECMP route cannot be forwarded to the right destination but to the CPU.

LSOD07460

- First found-in version: V3.03.01
- Condition: A stack is established, and the following conditions are met on a stacking unit.
 - (1) The unit ID is not 1.
 - (2) A DHCP server is connected to a port of this unit, which is configured as a DHCP snooping trusted port.
- Description: After the unit is rebooted, a connected DHCP client cannot get an IP address.

LSOD07506

- First found-in version: V3.03.01
- Condition: Insert an SFP module to a port on the front panel of a 5500G-EI SFP 24-port device.
- Description: The number of the port to which the SFP module is inserted is different from that displayed on the SNMP network management server.

Resolved Problems in V3.03.01p03

LSOD07038

- First found-in version: V3.03.01p01
- Condition: The stack serves as a DHCP relay agent. After a PC gets its IP address from a DHCP server through the DHCP relay agent, it sends a DHCP Inform packet to the DHCP server.
- Description: When the PC requests an IP address again, it has to repeat the request operation before it gets an IP address.

LSOD07240

- First found-in version: V3.03.01p01
- Condition: A switch serves as a DHCP relay agent. Send DHCP request packets to the switch continuously and clear DHCP client entries from the switch at the same time.
- Description: The switch reboots or cannot build client temporary entries according to DHCP requests.

LSOD07138

- First found-in version: V3.03.01p01
- Condition: A stack has DHCP snooping enabled. A PC gets an IP address from a DHCP server through the stack.
- Description: Display DHCP client information on Unit X with the **display dhcp-snooping unit X** command. The remaining lease time is always 0.

LSOD07145

- First found-in version: V3.03.01p01
- Condition: An administrator initiates RADIUS authentication. The server assigns two administrative privilege attributes, (Vendorid=43, Type=1) and (Vendorid=2011, Type=29).
- Description: RADIUS authentication fails.

LSOD07184

- First found-in version: V3.03.01p01
- Condition: A stacking device joins a cluster as a cluster member.
- Description: A memory leak of 512 bytes occurs on the slave device per minute.

LSOD07234

- First found-in version: V3.03.01p01
- Condition: Execute the **undo cluster enable** command on a stacking device that also works as a cluster member.
- Description: The cluster configuration of the master device cannot be synchronized to the slave device.

LSOD07128

- First found-in version: V3.03.01p01
- Condition: A stack has STP BPDU protection enabled. An STP edge port on a slave device becomes administratively down after receiving BPDUs.
- Description: Using the **display stp portdown** command cannot view information about the port.

LSOD07143

- First found-in version: V3.03.01p01
- Condition: Port A, which is not a STP edge port, is connected to a terminal. Port A goes up.
- Description: The STP status of port A in MSTI changes from discarding to forwarding directly, without passing the learning state.

LSOD07136

- First found-in version: V3.03.01p01
- Condition: Telnet to a device that is handling huge IUC traffic.
- Description: The telnet user is hung up and the corresponding resources cannot be released.

LSOD07140

- First found-in version: V3.03.01p01
- Condition: Two devices form a stack. Two users telnet to the stack through the master device and the slave device respectively. Execute the **free user-interface vty** command on the console port of the slave device, and use the **display users** command to view the user information on the master device.
- Description: The master device reboots abnormally.

LSOD06680/LSOD07269

- First found-in version: V3.03.01p01

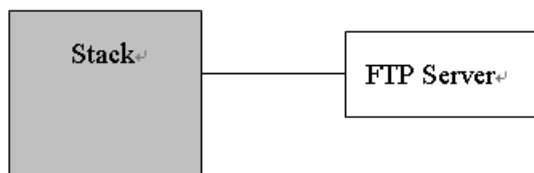
- Condition: The device has the default configuration file 'config.def', but has no startup configuration file specified.
- Description: The device does not use the auto-configuration function after startup, but runs the default configuration file 'config.def'.

ZDD01517

- First found-in version: V3.03.01p01
- Condition: Use the AT&T network management tool to backup the configuration on the device.
- Description: A memory leak of 512K bytes occurs each time a backup operation is performed.

LSOD06530

- First found-in version: V3.03.01p01
- Condition: The network diagram is shown below: The stack acts as an FTP client. Device A in the stack is not directly connected to the FTP server. All devices in the figure are the S5500G series.



- Description: Performing FTP put operations on Device A fails.

LSOD07122

- First found-in version: V3.03.01p01
- Condition: Insert a Finisar SX BCL optical module into the SFP slot of the device.
- Description: The device cannot identify this type of module.

LSOD07191

- First found-in version: V3.03.01p01
- Condition: In any view, run the **display drv-module qacl ?** command to show help information.
- Description: The help information is incorrect.

The incorrect information is,

```
<sysname>display drv-module qacl ?
qacl_configuration  Write data into chip
qacl_resource       Read data from chip
<cr>
```

The correct information should be,

```
<sysname>display drv-module qacl ?
qacl_configuration  QACL configuration
qacl_resource       QACL resource information
<cr>
```

LSOD07195

- First found-in version: V3.03.01p01
- Condition: A slave unit in a stack has an expansion card inserted. Reboot the stack, and ping a PC or another device connected to the slave unit from outside of the stack.

- Description: The ping operation may fail.

LSOD06651

- First found-in version: V3.03.01p01
- Condition: Enable DHCP-triggered authentication on globally. Enable port security on a port and set the port security mode to **userlogin-withoui**.
- Description: DHCP packets received on the port do not trigger 802.1X authentication.

LSOD07030

- First found-in version: V3.03.01p01
- Condition: Configure the **dhcp-snooping trust** command on each unit of a stack, save configuration, and then reboot the stack.
- Description: The trusted ports configuration fails to be synchronized in the stack, and thus the stack cannot forward DHCP packets normally.

LSOD06979

- First found-in version: V3.03.01p01
- Condition: A port of a unit in a stack detects or receives TC BPDUs.
- Description: The ARP entries learned on ports of other units cannot be deleted.

LSOD06977

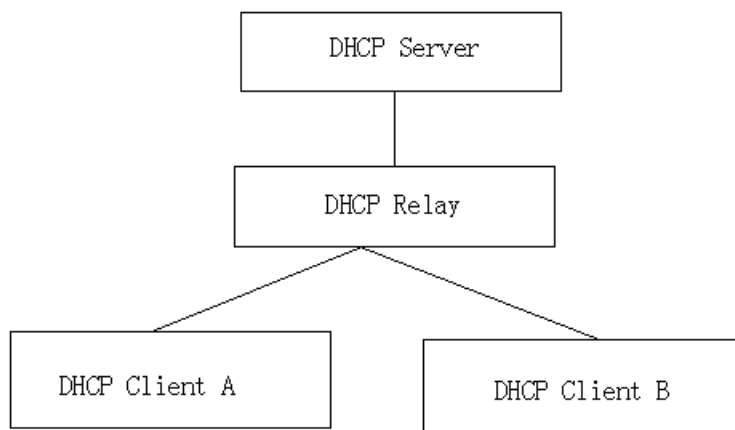
- First found-in version: V3.03.01p01
- Condition: Configure a port aggregation group across a stack. The memory usage on a device is very high (idle memory is only 2M, for example).
- Description: MSTP fails to work and the device reboots.

LSOD06983

- First found-in version: V3.03.01p01
- Condition: Enable DHCP snooping on a stack. The startup time is different on different units. A DHCP client entry is created on the stack.
- Description: Display DHCP client information with the **display dhcp-snooping** command. The lease time of the DHCP client entry is different on different units.

LSOD07046

- First found-in version: V3.03.01p01
- Condition:



The network diagram is as shown above.

Client A obtains IP address IP_A, and then releases the IP address. Then, client B sends a DHCP request containing client ID information, and the DHCP server allocates IP address IP_A to client B.

- Description: Such an operation causes a memory leak of 32 bytes on the DHCP relay agent.

LSOD07047

- First found-in version: V3.03.01p01
- Condition: Insert a SUMITOMO SFP module into a port on the front panel of a 5500G-EI SFP 24-port device; or insert a SUMITOMO SFP module into a port on the expansion card of any device model.
- Description: All the ports on the front panel of the 5500G-EI SFP 24-port device cannot recognize any SFP modules; all the ports on the expansion card cannot recognize any SFP modules.

LSOD06936

- First found-in version: V3.03.01p01
- Condition: No XENPAK optical module is inserted to the TenGigabitEthernet port on a single-port 10 GE expansion card whose version is REV_D.
- Description: The hardware type of the TenGigabitEthernet port is displayed as XPK_UNKNOWN with the **display interface TenGigabitEthernet** command, which should be XPK_NO_CONNECTOR.

LSOD06981

- First found-in version: V3.03.01p01
- Condition: LACP protocol packets received do not conform to the protocol specifications (124 bytes)
- Description: Those packets are discarded because they fail packet length check, and thus aggregation fails.

LSOD06978

- First found-in version: V3.03.01p01
- Condition: In the following network, enable EAD quick deployment on the switch that performs only layer-2 forwarding and connects to the RADIUS server via a layer-3 device.



- Description: EAD quick deployment cannot be implemented.

LSOD07065

- First found-in version: V3.03.01p01
- Condition: Enable DHCP relay agent on the switch, and then inject DHCP request/ACK packets to the switch continuously. Execute the **display dhcp-security** command on the switch.
- Description: The switch reboots abnormally.

TCD00854

- First found-in version: V3.03.01p01
- Condition: Change the mode of port A from “1000 M and full duplex” to “speed auto and duplex auto” when it is in DLDP down status. Disable DLDP on that port and then shutdown it.
- Description: Port A does not send any link-down trap.

LSOD06725

- First found-in version: V3.03.01p01
- Condition: A PD device connects to the switch. Pull in and plug out the PD device to generate a power-down notification trap (pethPsePortOnOffNotification trap).
- Description: The port index in the the pethPsePortOnOffNotification trap is incorrect.

Resolved Problems in V3.03.01p01

LSOD05600

- First found-in version: V3.03.00
- Condition: Enable the **arp restricted-forwarding** command on a stack. A DHCP client and a DHCP server are connected to different stacking units.
- Description: The client cannot ping the server after it gets an IP address.

LSOD05954

- First found-in version: V3.03.00
- Condition: Enable **dhcp-snooping** on a stack, the uplink of which is a link aggregation group. The primary port of the link aggregation group is down. A PC sends a DHCP request with the unicast flag set through the stack.
- Description: The PC cannot get an IP address successfully.

LSOD05565

- First found-in version: V3.03.00
- Condition: Enable **dhcp-snooping** on a stack, the downlink of which is a link-aggregation group across stacking units. The primary port of the link-aggregation group is down.
- Description: A connected PC cannot get an IP address through the stack.

LSOD05630

- First found-in version: V3.03.00
- Condition: **Voice VLAN legacy** is enabled on a device.
- Description: When the CPU usage is high, the device cannot send one CDP packet every second.

LSOD05840

- First found-in version: V3.03.00
- Condition: Certificate re-authentication is enabled on a RADIUS server.
- Description: A user cannot be re-authenticated.

LSOD05513

- First found-in version: V3.03.00
- Condition: Configure a MD5 key longer than 16 bytes on a device and synchronize time with a NTP server through authentication. Then, save the configuration and reboot the device.
- Description: After reboot, the device cannot synchronize time with the NTP server.

LSOD05807

- First found-in version: V3.03.00
- Condition: In cluster view, reboot a member switch with its MAC address.
- Description: The member switch does not reboot.

LSOD06082

- First found-in version: V3.03.00
- Condition: Configure selective QinQ when ACL resources are insufficient.
- Description: The configuration terminal does not respond.

LSOD06122

- First found-in version: V3.03.00
- Condition: Enable DHCP snooping and UDP-helper on a stack. A DHCP client and a DHCP server are connected to different stacking devices, and the MAC address of the DHCP client is configured as a static MAC address on the stack.
- Description: The DHCP client cannot get an IP address.

LSOD06072

- First found-in version: V3.03.00
- Condition: EAD quick deployment is enabled on a device. A user connected to the device and the EAD web server belong to different VLANs.
- Description: If the user tries to access the web interface through a browser before authentication, maybe the user cannot be redirected to the predefined web page.

LSOD05415/LSOD05466

- First found-in version: V3.03.00
- Condition: Enable port isolation in a link-aggregation group.
- Description: Sometimes, the link-aggregation group cannot be isolated from other member ports.

LSOD00851

- First found-in version: V3.03.00
- Condition: A stack serves as a DHCP server. Many DHCP clients request IP addresses while the memory usage of the master device is up to 90%.
- Description: The master unit may reboot due to dead loop.

LSOD02302

- First found-in version: V3.03.00
- Condition: In a stack with a link-aggregation group configured across units, modify the STP cost of the stack to change the STP status of the aggregate link from forwarding to discarding.
- Description: A transient loop appears, causing packet storm.

LSOD02678

- First found-in version: V3.03.00
- Condition: In a network with maximum instances and VLANs configured, and with lots of MAC addresses in the MAC table, change the STP instance status.
- Description: The STP topology oscillates and cannot converge.

LSOD02688

- First found-in version: V3.03.00
- Condition: Voice VLAN and EAD quick deployment are enabled on the same port.
- Description: EAD quick deployment doesn't work.

LSOD02896

- First found-in version: V3.03.00
- Condition: Enable STP on a stacking device, port A of which has learned maximum ARP entries. If port A receives TC packets, the ARP entries learned on it should be deleted.
- Description: Only the ARP entries on the unit where port A resides can be deleted, while the ARP entries corresponding to port A in other units cannot be deleted.

LSOD03647

- First found-in version: V3.03.00
- Condition: Enable MSTP in a stack and configure maximum instances and VLANs. Save the configuration and reboot the stack when a lot of ports in the stack are being used.
- Description: The stack may reboot due to dead loop.

LSOD03483

- First found-in version: V3.03.00
- Description: Use the **mac-address max-mac-count xxx** command to configure the maximum number of MAC addresses that port A can learn. Port A learns MAC addresses when receiving a lot of packets with the source MAC address changed.
- Avoidance: Use the **display mac-address** command to show the learned MAC addresses. It takes relatively a long time before the information can be output.

LSOD06487

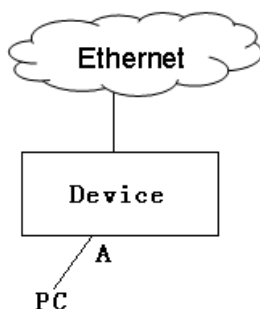
- First found-in version: V3.03.00
- Condition: Run the **ping -t** command to ping a peer device for a long time. The peer does not respond with ICMP responses in time. Thus, "request timeout" occurs.
- Description: When the peer can respond in time, the ping operation still fails. To ping the peer, you have to perform a new ping operation.

LSOD04261

- First found-in version: V3.03.00
- Condition: Multiple devices form a ring topology, and OSPF is enabled in the network. Then, reboot a stacking device in the network.
- Description: OSPF cannot converge quickly and the network breaks for about 30 seconds.

LSOD06207

- First found-in version: V3.03.00
- Condition:



As shown in the above figure, enable 802.1X on port A that 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: V3.03.00
- Condition: Enable 802.1X on the device to perform authentication on a DRCOM client.
- Description: Sometimes, the EAPOL start packet from the client gets no response, and thus authentication fails. Sometimes, after authentication succeeds, the client cannot log out because the EAPOL logoff packet from the client gets no response.

LSOD05492

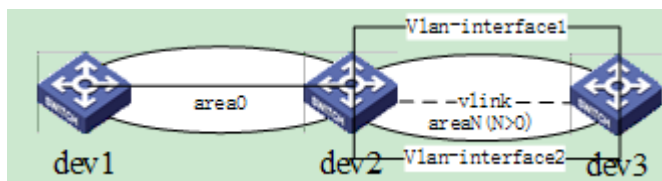
- First found-in version: V3.03.00
- Condition: Set the minimum super user password length to N1. Set super user password "password 1" with a length of N2. Then change the minimum super user password length to N3 ($N3 > N2 > N1$). Log out and then log in.
- Description: Password 1 can still be used to log in.

LSOD06871

- First found-in version: V3.03.00
- Condition: Use the **tftp source-ip** command to set a source IP address for TFTP connections.
- Description: This configuration takes effect for CLI operations, but does not take effect for web interface operations.

LSOD06384

- First found-in version: V3.03.00
- Condition:



- 1) dev1 connects to dev2 through a VLAN interface, which locates in area 0; dev2 connects to dev3 through two VLAN interfaces, which locate in area N (N>0).
 - 2) The routes from dev3 to the loopback address on dev2 are equal-cost routes.
 - 3) Configure vlink peers on dev2 and dev3 to establish two vlink neighbors between dev2 and dev3.
- Description: Use the **display ospf peer brief** command to view the vlink neighbors. The addresses of the neighbors on the local device are not consistent with the peer addresses.

LSOD06754

- First found-in version: V3.03.00
- Condition: Configure a static multicast MAC address on devices in a stack.
- Description: The multicast MAC address has the same collection of local forwarding ports on each device in the stack. For example, unit 1 and unit 2 form the stack. Port num-1 on unit 1 and port num-2 on unit 2 are configured as the forwarding ports of the multicast MAC address. The actual forwarding ports of the multicast MAC address contain four ports: two are num-1 and num-2 ports on unit 1; another two ports are num-1 and num-2 ports on unit 2.

LSOD06672

- First found-in version: V3.03.00
- Condition: A traffic-priority rule that filters packets with specific source MAC addresses is applied to port A. Then configure those MAC addresses as OUI MAC addresses.
- Description: Executing the **copy configuration source port-A destination port-B** command fails. If port-A belongs to a link aggregation group, the traffic-priority rule of port A cannot be synchronized to other port members in the same aggregation group.

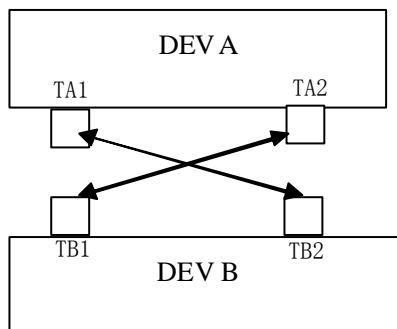
LSOD06822

- First found-in version: V3.03.00
- Condition: Enable DHCP snooping on the switch. Connect a client to the switch through a hub which is working on 10M speed and half duplex mode. Perform DHCP request operations on the client frequently, and shutdown the switch's port that connects to the hub.

- Description: Sometimes, no link-down trap is sent when the port is physically down. And the speed and duplex mode shown by using the **display interface** command is not "Unknown-speed mode, unknown-duplex mode".

LSOD06670

- First found-in version: V3.03.00
- Condition:



Enable STP on DEV A and disable STP on DEV B. Port TA1 and Port TA2 belong to the same aggregation group on DEV A, and Port TB1 and Port TB2 belong to the same aggregation group on DEV B.

- Description: The STP state of port TA1 changes continuously.

LSOD06630

- First found-in version: V3.03.00
- Condition: A 5500G-EI SFP 24-port device connects to another device and then starts up.
- Description: The COMBO port is always up.

LSOD06786

- First found-in version: V3.03.00
- Condition: STP is disabled. Configure port isolation between Port A and Port B on one device. Send STP packets into Port A.
- Description: Port isolation fails, and packets are forwarded through Port B.

LSOD06739

- First found-in version: V3.03.00
- Condition: Dot1X and EAD quick deployment are enabled on the device. Dot1X is enabled on port A. Send a lot of packets with unknown source MAC addresses to port A.
- Description: Memory leaks occur.

Resolved Problems in V3.03.00

It is the first release of V3.03.xx.

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.

The device software can be upgraded through console port, TFTP, and FTP.

Remote Upgrading through CLI

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

```
<Switch> ftp 10.10.110.1
Trying
Press CTRL+K to abort
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.app switch.app
[ftp] get switch.btm switch.btm
[ftp] bye
<Switch> boot bootrom switch.btm
please wait ...
Bootrom is updated!
<Switch> boot boot-loader switch.app
<Switch> display boot-loader
The app to boot at the next time is: flash:/ switch.app
<Switch> reboot
```

After getting the new application file, reboot the device to have the upgraded application take effect.

Note that if you do not have enough Flash space, upgrade the Boot ROM program first, and then FTP the application 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 5500G PWR 28-Port BOOTROM, Version 5.01
*
*****

Copyright (c) 2004-2007 3Com Corporation and its licensors.
Creation date   : Nov 27 2007, 11:54:20
CPU type       : BCM4704
CPU Clock Speed : 200MHz
BUS Clock Speed : 33MHz
Memory Size    : 128MB

Mac Address    : 00e0fc123456
```

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 Boot ROM 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)

Step 1: Enter **6** in the Boot menu and press <Enter> to access the bootRom update menu.

Bootrom update menu:

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

Enter your choice(0-3):

Step 2: 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. Exit

Enter your choice (0-5):

Step 3: 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.

Step 4: 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.

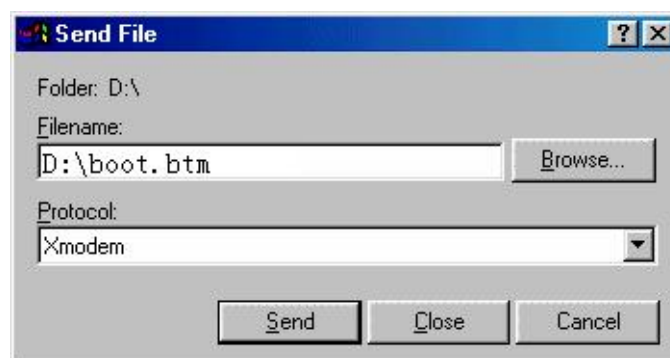


Figure 1 Send File

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

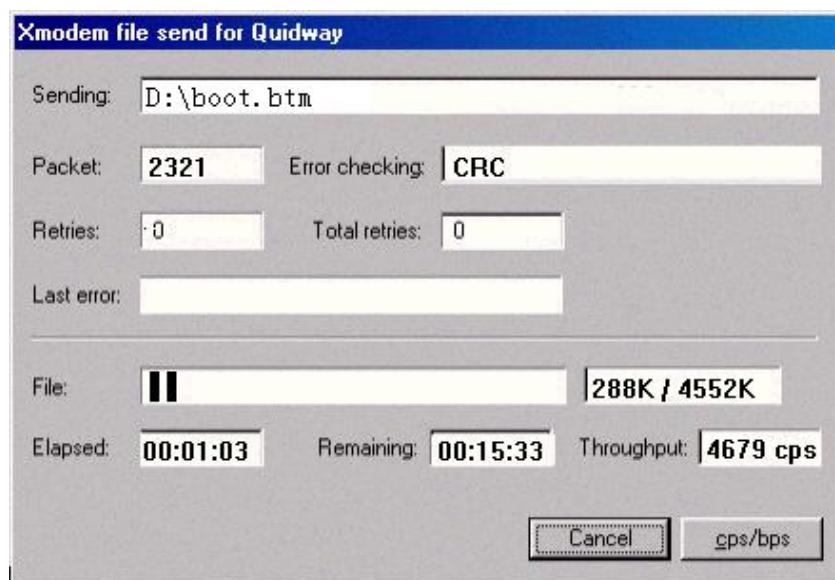


Figure 2 Xmodem File Send

Step 7: After the downloading of the program is completed, the screen will display the following information:

Loading ...CCCCCCCCC done!

Software Upgrading via Ethernet Interface (FTP/TFTP)

Software Upgrading via TFTP

1) Introduction to TFTP

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

2) Upgrade procedure

Step 1: 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.

Step 2: Run the TFTP server program on the PC, and put the program files into a file directory.



Caution

Switch 5500G series are not shipped with TFTP server program.

Step 3: Run the terminal emulation program on the PC, and start the switch, to access the Boot menu.

Step 4: 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 to boot menu

Enter your choice(0-3):1

Step 5: Enter **1** to use TFTP, and press <Enter>. The following information appears:

Load File name

Switch IP address (This address and the server IP address must be on the same network segment)

Server IP address (IP address of the PC where the file is stored)

Step 6: Input correct information and press <Enter>. The following information appears:

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

Step 7: 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:

Loadingdone!

Writing to flash.....done!

Software Upgrading via FTP

1) Introduction to FTP

The 5500G can serve as an FTP server or client. In the following example, it serves as an FTP client.

2) Upgrade procedure

Step 1: 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.

Step 2: Run the FTP server program on the PC, and put the program files into a file directory.

Step 3: Run the terminal emulation program on the PC, and start the switch to access the Boot menu.

Step 4: 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 to boot menu

```
Enter your choice(0-3):2
```

Step 5: 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
```

Step 6: Input correct information and press <Enter>. The following information appears:

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

Step 7: 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!
```