Switch 4500G s3q05_02_00s56(s168)p12 Release Notes

Keywords: Resolved problems, software upgrading

Abstract: *This release notes describes the Switch 4500G s3q05_02_00s56(s168)p12 release with respect to version information, updating, unresolved and solved problems, and software upgrading.*

Acronyms:

Abbreviations	Full spelling
AAA	Authentication, Authorization and Accounting
ARP	Address Resolution Protocol
CMW	Comware
DHCP	Dynamic Host Configuration Protocol
GVRP	GARP VLAN Registration Protocol
IGMP	Internet Group Management Protocol
LACP	Link Aggregation Control Protocol
MIB	Management Information Base
MSTP	Multiple Spanning Tree Protocol
RIP	Routing Information Protocol
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
VLAN	Virtual Local Area Network

Table of Contents

List of Tables

Version Information

Version Number

Version Information: *3Com OS V5.02.00s56(S168)p12*

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

Version History

Table 1 Version history

Version number	Last version	Release Date	Remarks
s3q05_02_00s56(s168)p12	*s3q05_02_00s56(s168)p02*	*2009-09-30*	None
s3q05_02_00s56(s168)p02	*s3q05_02_00s56(s168)p01*	*2009-04-30*	None
s3q05_02_00s56(s168)p01	*s3q05_02_00s56(s168)*	*2009-03-30*	None
s3q05_02_00s56(s168)	*s3q05_01_03s56(s168)*	*2009-02-25*	None
s3q05_01_03s56(s168)	*s3q05_01_02s56(s168)*	*2008-01-30*	None
s3q05_01_02s56(s168)	*s3q05_01_00s56(s168)p01*	*2007-09-24*	None
s3q05_01_00s56(s168)p01	*s3q05_01_00s56(s168)*	*2007-01-30*	None
s3q05_01_00s56(s168)	*None*	*2006-10-18*	None

Hardware and Software Compatibility Matrix

Table 2 Compatibility matrix

Item	Specifications
Product family	*Switch 4500G series*
Hardware platform	*Switch 4500G 24-Port/ 4500G 48-Port /* *Switch 4500G 24-Port PWR/4800G 48-Port PWR* *Switch 4500G 24-Port SFP*
Minimum memory requirements	*128M*
Minimum Flash requirements	*16 MB*
Boot ROM version	*Version 503 (Note: You can view the version number with the display version command in any view. See Note②)*
Host software	*s3q05_02_00s56p12.app* *s3q05_02_00s168p12.app*

Item	Specifications
iMC Version	*iMC PLAT 3.20-R2602 + P06* *iMC UAM 3.60-E6203* *iMC EAD 3.60- E6203* *iMC NTA 3.20-E0601 + P01* *iMC QoSM 3.20-E0603 + P01*
iNode Version	*iNode PC 3.60-E6204*
Remarks	*s3q05_02_00s56p12 provides 56-bit encryption for SSH* *s3q05_02_00s168p12.app provides 168-bit encryption for SSH*

Sample: Display software and boot Rom version information of the 4500G switch.

```
<4500G>dis version
3Com Corporation
3Com Switch 4500G 24-Port Software Version 3Com OS V5.02.00s56p12- Note①
Copyright (c) 2004-2009 3Com Corp. and its licensors. All rights reserved.
3Com Switch 4500G 24-Port uptime is 0 week, 0 day, 0 hour, 5 minutes

3Com Switch 4500G 24-Port with 1 Processor
128M    bytes SDRAM
16384K  bytes Flash Memory

Hardware Version is REV.B
CPLD Version is 006
Bootrom Version is 503                          ------- Note②
[SubSlot 0] 24GE+4SFP Hardware Version is REV.B
[SubSlot 1] 2 CX4 Hardware Version is REV.B
```

Restrictions and Cautions

When configuring the Switch 4500G, be sure that you are aware of these restrictions and cautions:

1) VLAN ACLs cannot take effect on QinQ-enabled ports because of implementation limitations.
2) When the configuration of port isolation conflicts with the redirect action of QoS, the port isolation configuration overrides. For example, assume ports g1/0/1 and g1/0/2 belong to a port isolation group and the QoS policy applied on g1/0/1 contains a traffic behavior to redirect traffic received on g1/0/1 to g1/0/2. When receiving traffic matching the QoS policy, port g1/0/1 will not redirect it to port g1/0/2, because both ports are members of a port isolation group, which prevents them from forwarding traffic to each other.
3) The broadcast/multicast/unknown unicast suppression threshold configured as a percentage of the total bandwidth in port view is accurate only for 64-byte packets. This is because the chip supports only broadcast suppression by PPS, and the system converts the percentage into PPS per 64 bytes. Thus, you are recommended to configure storm suppression by PPS.

4) The virtual cable test (VCT) function will fail if the connected peer port works at 100 Mbps in forced mode.
5) Gryffindor cannot assign ACLs with "neq" option due to chip limitations.

Feature List

Hardware Features

Table 3 Hardware features

Item		Switch 4500G 24-Port	Switch 4500G 48-Port	Switch 4500G 24-Port PWR	Switch 4500G 48-Port PWR
Dimensions (H × W × D)		43.6 × 440 × 300 mm (1.72 ×17.3 × 11.8 in.)		43.6 × 440 × 260 mm (1.72 × 17.3 × 10.2 in.)	
Weight		4 kg (8.1 lb)	4.5 kg (9.9 lb)	6 kg (13.2 lb)	6.5 kg (14.3 lb)
Console port		1			
GE ports on the front panel		24 × 10/100/1000M electrical ports 4 × Gigabit SFP Combo ports	48 × 10/100/1000M electrical ports 4 × Gigabit SFP Combo ports	24 × 10/100/1000M electrical ports 4 × Gigabit SFP Combo ports	48 × 10/100/1000M electrical ports 4 × Gigabit SFP Combo ports
Optional modules		1-port 10GE XFP module 2-port 10GE XFP module 2-port 10GE CX4 short haul module			
Power supply	AC	Rated voltage: 100 VAC to 240 V AC, 50 Hz to 60 Hz Input voltage: 90 VAC to 264 VAC, 47 Hz to 63 Hz			
	DC	None		Rated voltage range: -52 VDC to 55 VDC	
Power consumption (full load)		80 W	120 W	455 W: 85 W for system power consumption and 370 W for PoE power consumption	When no remote power supply RPS is connected, full-load power consumption is 500 W including system power consumption 130 W and PoE power consumption 370 W. When an RPS is connected, full-load power consumption is 870 W including system power consumption 130 W and PoE power consumption 740 W.
Operating temperature		0°C to 40°C			
Relative humidity (noncondensing)		10% to 90%			

Software Features

Table 4 Software features

Feature		Switch 4500G 24-Port	Switch 4500G 48-Port	Switch 4500G 24-Port PWR	Switch 4500G 48-Port PWR
Wire speed Lay-2 switching	Switching capacity (Full duplex)	128 Gbps	176 Gbps	128 Gbps	176 Gbps
	Packet forwarding rate	95.2 Mpps	130.9 Mpps	95.2 Mpps	130.9 Mpps
Power over Ethernet		Not supported		Supported	
Link aggregation		• Aggregation of GE ports • Aggregation of 10-GE ports • Static link aggregation • Dynamic link aggregation			
Flow control		IEEE 802.3x flow control and back pressure			
Jumbo Frame		Maximum frame size of 9 KB			
MAC address table		• 8K MAC addresses • 128 static MAC addresses • Blackhole MAC addresses • MAC address learning limit on a per port basis			
VLAN		• Port-based VLANs (4094 VLANs) • QinQ and selective QinQ • Voice VLAN • Protocol-based VLANs • MAC-based VLANs • IP subnet-based VLANs • GVRP • Isolate-user VLAN			
ARP		• 2K entries • 1K static entries • Gratuitous ARP • Standard proxy ARP and local proxy ARP • ARP source suppression • ARP detection (based on DHCP snooping entries/802.1x security entries/static IP-to-MAC bindings)			
ND		• 1K entries • 512 static entries			
VLAN virtual interface		• 64			

Feature	Switch 4500G 24-Port	Switch 4500G 48-Port	Switch 4500G 24-Port PWR	Switch 4500G 48-Port PWR
DHCP	• DHCP client • DHCP snooping • DHCP relay agent			
UDP Helper	• UDP Helper			
DNS	• Dynamic domain name resolution • Dynamic domain name resolution client • IPv4/IPv6 addresses			
IPv4 route	• 64 static routes • RIP (Routing Information Protocol) v1/2, supporting up to 512 IPv4 routes • Route policy			
IPv6 route	• 64 static routes • RIPng, supporting up to 256 IPv6 routes • Route policy			
IPv4 multicast	• IGMP Snooping v1/v2/v3 • Multicast VLAN • Multicast VLAN+			
IPv6 multicast	• MLD snooping v1/v2 • IPv6 multicast VLAN • IPv6 multicast VLAN+			
Broadcast/multicast/unicast storm control	• Storm control based on port rate percentage • PPS-based storm control			
MSTP	• STP/RSTP/MSTP • STP root guard • BPDU guard			
RRPP	• RRPP protocol • Multi-instance RRPP			
Smart link	• Smart link • Multi-instance smart link			
Monitor link	Supported			
Bpdu tunnel	• Cdp/dldp/eoam/gvrp/hgmp/lacp/lldp/pagp/pvst/stp/udldvtp			

Feature	Switch 4500G 24-Port	Switch 4500G 48-Port	Switch 4500G 24-Port PWR	Switch 4500G 48-Port PWR
QoS/ACL	• Sending/receiving rate limit on a per port basis with a granularity of 64 kbps. • Packet redirection • Committed access rate (CAR), with a granularity of 64 kbps. • Eight output queues per port • Flexible port/queue based queue scheduling algorithms , including SP, WRR, WFQ and SP + WRR. • Remarking of 802.1p and DSCP priorities • Packet filtering at Layer 2 through Layer 4; flow classification based on source MAC address, destination MAC address, source IP (IPv4/IPv6) address, destination IP (IPv4/IPv6) address, port, protocol, and VLAN. • Time range • User profile • Packet filter			
Mirroring	• Traffic mirroring • Port mirroring			
Remote mirroring	• Remote port mirroring			
Security	• Hierarchical management and password protection of users • AAA authentication • RADIUS authentication • HWTACACS • SSH 2.0 • Port isolation • Port security • MAC address authentication • IP-MAC-port binding • IP Source Guard • HTTPS • SSL • PKI • EAD			
802.1X	• Up to 1,024 users • Port-based and MAC address-based authentication • Guest VLAN • Trunk port authentication • 802.1X-based dynamic QoS/ACL/VLAN delivery • 802.1x re-authentication			
Loading and upgrading	• Loading and upgrading through XModem protocol • Loading and upgrading through FTP • Loading and upgrading through TFTP			

Feature	Switch 4500G 24-Port	Switch 4500G 48-Port	Switch 4500G 24-Port PWR	Switch 4500G 48-Port PWR
Management	• Configuration at the command line interface (CLI) • Remote configuration through Telnet • Configuration through Console port • Simple network management protocol (SNMP) • Remote monitoring (RMON) alarm, event and history recording • NMS • Web-based network management • System log • Hierarchical alarms • Huawei group management protocol (HGMP) v2 • NTP • Power supply alarm function • Fan and temperature alarms • IRF Lite • LLDP			
Maintenance	• Debugging information output • Ping and Tracert • NQA • Track • Remote maintenance through Telnet • Virtual cable test • 802.1ag • 802.3ah • DLDP			

Version Updates

Feature Updates

Table 5 Feature updates

Version Number	Item	Description
s3q05_02_00s56 (s168)p12	Changed Hardware Features	New Features: None Deleted Features: None

Version Number	Item	Description
	Changed Software Features	New Features: 1. 802.1X Online User Handshake Security; 2. MAC re-authenticate; 3. ACL Logging; 4. LACP-MAD passthrough; Deleted Features: None . Modified Features: None
s3q05_02_00s56 (s168)p02	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: 1. 802.1x re-authentication; 2. MAC-address based Guest VLAN; 3. TACACS+ accounting; 4. The protocol of LLDP can get the physical port information according to the device name; 5. Bpdu tunnel; 6. the protocol of Lacp marker; 7. configurable link aggregation load sharing by each link aggregation; 8. packet filter; Deleted Features: None . Modified Features: 1. modifying the “arp detection” mode change from “and” to “or”;
s3q05_02_00s56 (s168)p01	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: 1. BPDU Dropping; 2. the command alias function; Deleted Features: None . Modified Features: None
s3q05_02_00s56 (s168)	Changed Hardware Features	New Features: None Deleted Features: None

Version Number	Item	Description
	Changed Software Features	New Features: 1. Smart link; 2. Monitor link; 3. 802.1ag; 4. 802.3ah; 5. ARP detection; 6. ARP source suppression; 7. User profile; 8. Multiple voice VLAN; 9. LLDP; 10. DLDP; 11. Port security; 12. IP source guard; 13. sFlow; 14. Isolate-user VLAN; 15. RSPAN; 16. NQA; 17. Storm constrain; 18. Flow interval; 19. RRPP; 20. Subnet VLAN; 21. link aggregation load sharing configurable; 22. EAD; 23. IRF Lite; Deleted Features: None . Modified Features: Link aggregation
s3q05_01_03s56 (s168)	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: None Deleted Features: None Modified Features: None

Version Number	Item	Description
s3q05_01_02s56 (s168)	Changed Hardware Features	New Features: 100BASE-X-SFP and 1-10GE XFP module Deleted Features: None
	Changed Software Features	New Features: None Deleted Features: 802.3ad is modified; Pure dynamic LACP mode is not supported, and only manual and static LACP modes are supported. Modified Features: None .
s3q05_01_00s56 (s168)p01	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: None Deleted Features: None Modified Features: None

Command Line Updates

Table 6 Command line updates

Version Number	Item	Description
s3q05_02_00s56(s168)p12	New Commands	1. 802.1X Online User Handshake Security: **dot1x handshake secure** **Syntax** dot1x handshake secure undo dot1x handshake secure **View** Ethernet Interface view **Default Level** System level **Parameters** None **Description** Use the **dot1x handshake secure** command to enable the online user handshake security function so that the device can prevent users from using illegal

Version Number	Item	Description
		client software. Use the **undo dot1x handshake secure** command to disable the function. By default, the function is disabled. Note that: • The online user handshake security function is implemented based on the online user handshake function. To bring the security function into effect, keep the online user handshake function enabled. • The iNode client software and iMC server are recommended to ensure the normal operation of the online user handshake security function. Related commands: **dot1x handshake**. 2.ACL Logging **Syntax** **acl logging frequence** *frequence* **undo acl logging frequence** **View** System view **Description** Use the **acl logging frequence** command to set the interval for IPv4 packet filtering statistics. At the specified interval, the device outputs the statistics information, including the number of filtered packets, and the ACL rules used. Use the **undo acl logging frequence** command to restore the default. By default, the interval is 0, that is, no IPv4 packet filtering statistics is collected. **Syntax** **acl ipv6 logging frequence** *frequence* **undo acl ipv6 logging frequence** **View** System view **Description** Use the **acl ipv6 logging frequence**

Version Number	Item	Description
		command to set the interval for IPv6 packet filtering statistics. At the specified interval, the device outputs the statistics information, including the number of filtered packets, and the ACL rules used. Use the **undo ipv6 acl logging frequence** command to restore the default. By default, the interval is 0, that is, no IPv6 packet filtering statistics is collected.
	Deleted Commands	
	Modified Commands	
s3q05_02_00s56(s168)p02	New Commands	1. 802.1x re-authentication **Syntax** **dot1x re-authenticate** **undo dot1x re-authenticate** **View** Ethernet interface view **Description** Use the **dot1x re-authenticate** command to enable the periodic re-authentication function. Use the **undo dot1x re-authenticate** command to restore the default. **Syntax** **dot1x timer reauth-period** *reauth-period-value* **undo dot1x timer reauth-period** **View** System view **Description** Use the **dot1x timer** command to set 802.1x timers. Use the **undo dot1x timer** command to restore the defaults. 2. MAC-address based Guest VLAN **Syntax** **mac-authentication guest-vlan** *guest-vlan-id* **undo mac-authentication guest-vlan** **View** Layer 2 Ethernet interface view **Description** Use the **mac-authentication guest-vlan** command to specify a MAC-based guest VLAN (MGV) for MAC authentication. After the configured MGV takes effect, all users failing the authentication on the port will be added to the guest VLAN. Use the **undo mac-authentication guest-vlan** command to remove the guest VLAN configuration.

Version Number	Item	Description
		3. TACACS+ accounting **Syntax** **accounting command hwtacacs-scheme** *hwtacacs-scheme-name* **undo accounting command** **View** ISP domain view **Description** Use the **accounting command** command to specify the HWTACACS scheme for command line users. Use the **undo accounting command** command to restore the default. **Syntax** **command accounting** **undo command accounting** **View** User interface view **Description** Use the **command accounting** command to enable command accounting. Use the **undo command accounting** command to restore the default. **Syntax** **command authorization** **undo command authorization** **View** User interface view **Description** Use the **command authorization** command to enable command authorization. Use the **undo command authorization** command to restore the default. 4. The protocol of LLDP can get the physical port information according to the device name **Syntax** **display lldp neighbor-information** [**brief** | **interface** *interface-type interface-number* [**brief**] | **list** [**system-name** *system-name*]] **View** Any view **Description** Use the **display lldp neighbor-information** command to display the LLDP information about the neighboring devices received on the local device. The LLDP information is sent as TLVs. 5. Bpdu tunnel **Syntax** In Ethernet interface view or port group view: **bpdu-tunnel dot1q** { **cdp** | **dldp** | **eoam** | **gvrp** | **hgmp** | **lacp** | **lldp** | **pagp** | **pvst** |

Version Number	Item	Description
		stp | **udld** | **vtp** } **undo bpdu-tunnel dot1q** { **cdp** | **dldp** | **eoam** | **gvrp** | **hgmp** | **lacp** | **lldp** | **pagp** | **pvst** | **stp** | **udld** | **vtp** } In Layer 2 aggregate interface view: **bpdu-tunnel dot1q** { **cdp** | **gvrp** | **hgmp** | **pvst** | **stp** | **vtp** } **undo bpdu-tunnel dot1q** { **cdp** | **gvrp** | **hgmp** | **pvst** | **stp** | **vtp** } **View** Ethernet interface view, Layer 2 aggregate interface view, port group view **Description** Use the **bpdu-tunnel dot1q** command to enable BPDU tunneling for a protocol on the current port or ports. Use the **undo bpdu-tunnel dot1q** command to disable BPDU tunneling for a protocol on the port or ports. 6. configurable link aggregation load sharing by each link aggregation **Syntax** **link-aggregation load-sharing mode** { **destination-ip** | **destination-mac** | **source-ip** | **source-mac** } * **undo link-aggregation load-sharing mode** **View** Layer 2 aggregate interface view **Description** Use the **link-aggregation load-sharing mode** command to configure the aggregation group-specific link aggregation load sharing mode. 7. packet filter **Syntax** **packet-filter** { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** } **undo packet-filter** { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** } **View** Ethernet interface view, VLAN interface view **Description** Use the **packet-filter** command to apply an ACL to an interface to filter IPv4 packets or Ethernet frames. Use the **undo packet-filter** command to restore the default. **Syntax** **packet-filter ipv6** { *acl6-number* | **name** *acl6-name* } { **inbound** | **outbound** } **undo packet-filter ipv6** { *acl6-number* | **name** *acl6-name* } { **inbound** | **outbound** } **View** Ethernet interface view, VLAN interface

Version Number	Item	Description
		view **Description** Use the **packet-filter ipv6** command to apply a basic or advanced IPv6 ACL to an interface to filter IPv6 packets. Use the undo **packet-filter ipv6** command to restore the default.
	Deleted Commands	**Syntax** **port** *interface-list* **undo port** *interface-list* **View** VLAN view **Description** Use the **port** command to assign the specified access port(s) to the current VLAN. Use the **undo port** command to remove the specified access port(s) from the current VLAN. **Explain** Interface-list: not support the Layer 2 aggregate interface list any more.
	Modified Commands	**Syntax** **arp detection mode** { **dhcp-snooping** | **dot1x | static-bind** } **undo arp detection mode** { **dhcp-snooping** | **dot1x | static-bind** } **View** System view **Description** Use the **arp detection mode** command to specify an ARP attack detection mode. Use the **undo arp detection mode** command to cancel the specified ARP detection mode. **Explain** The “arp detection” mode change from “and” to “or”.

Version Number	Item	Description
s3q05_02_00s56(s168)p01	New Commands	1. BPDU Dropping **Syntax** **bpdu-drop any** **undo bpdu-drop any** **View** Ethernet interface view, port group view, Layer-2 aggregate interface view **Description** Use the **bpdu-drop any** command to enable BPDU dropping on the Ethernet port. Use the **undo bpdu-drop any** command to disable BPDU dropping on the Ethernet port. 2. The command alias function **Syntax** **command-alias enable** **undo command-alias enable** **View** System view **Description** Use the **command-alias enable** command to enable the command alias function. Use the **undo command-alias enable** command to disable the command alias function. **Syntax** **command-alias mapping** *cmdkey alias* **undo command-alias mapping** *cmdkey* **View** System view **Description** Use the **command-alias mapping** command to configure command aliases. Use the **undo command-alias mapping** command to delete command aliases. **Syntax** **display command-alias** **View** Any view **Description** Use the display command-alias command to display defined command aliases and the corresponding commands.
	Deleted Commands	None
	Modified Commands	
s3q05_02_00s56(s168)	New Commands	*3Com Switch 4500G Family Configuration Guide-V05.02.00 (6W100)* *3Com Switch 4500G Family Command Reference Guide-V05.02.00 (6W100)*
	Deleted Commands	None

Version Number	Item	Description
	Modified Commands	For link aggregation configuration commands, refer to: *3Com Switch 4500G Family Configuration Guide-V05.02.00 (6W100)* *3Com Switch 4500G Family Command Reference Guide-V05.02.00 (6W100)*
s3q05_01_03s56(s168)	New Commands	None
	Deleted Commands	None
	Modified Commands	None
s3q05_01_02s56(s168)	New Commands	None
	Deleted Commands	1.Deleted Command: [H3C-GigabitEthernet1/0/1] lacp enable [H3C-GigabitEthernet1/0/1] undo lacp enable Specification: The static LACP mode runs, and can replace pure dynamic LACP mode.
	Modified Commands	None
s3q05_01_00s56(s168)p01	New Commands	1. mac-authentication user-name-format mac-address [with-hyphen | without-hyphen]: Uses MAC addresses with hyphens or without hyphens as usernames and passwords; 2. mac-authentication user-name-format fixed [account STRING<1-55>] [password { simple STRING<1-256> | cipher STRING<1-256> }]: specifies the centralized MAC address authentication mode as fixed mode; 3. undo mac-authentication user-name-format: Restores the default centralized MAC address authentication mode.
	Deleted Commands	None
	Modified Commands	1. rsa local-key-pair export { ssh1 | ssh2 | openssh } [STRING<1-256>]: Execution view is changed from user view to system view; 2. rsa peer-public-key STRING<1-64> [import sshkey STRING<1-136>] is changed to rsa peer-public-key STRING<1-64> [import sshkey STRING<1-135>]

MIB Updates

Table 7 MIB updates

Version Number	Item	MIB File Name	Module Name	Description
s3q05_02_00s56(s168)p12	New	None		
	Modified	None		
s3q05_02_00s56(s168)p02	New	None		
	Modified	Reference Description		1. Modify dot1xPaePortTable of dot1xPaeSystem in IEEE8021X MIB ;
s3q05_02_00s56(s168)p01	New	None		
	Modified	None		1.
s3q05_02_00s56(s168)	New	Reference Description		1. A3COM-HUAWEI-MAC-INFORMATION-MIB. 2. A3COM-HUAWEI--CBQOS2-MIB; A3COM-HUAWEI--QOS-CAPABILITY-MIB 3. h3cEntityExtSFPPhony was added to common traps in the A3COM-HUAWEI-ENTITY-EXT-MIB. 4. h3cExpirationDate, h3cUserGroup and h3cUserGroupInfoTable in the A3COM-HUAWEI-USER-MIB 5. hwdot1xAuthMethod was added in hwdot1xPaeSystem group in the A3COM-HUAWEI-8021PAE-MIB. 6. hwIgmpSnoopingNonFloodingStatus, hwIgmpSnoopingStatsObjects, hwIgmpSnoopingVlanStatusTable in the HUAWEI-LswIGSP-MIB and H3C-MPM-MIB 7. Scalar Objects was added in the A3COM-HUAWEI-LswINF-MIB. 8. h3cSysCurBtmFileName and h3cSysCurUpdateBtmFileName in the A3COM-HUAWEI-SYS-MAN-MIB. 9. h3cProcessTable was added in H3C-ENTITY-EXT-MIB.

Version Number	Item	MIB File Name	Module Name	Description
	Modified	Reference Description		2. Description of h3cUserName was modified in the A3COM-HUAWEI-USER-MIB. 3. Details of ipv6IfDescr in the IPV6-MIB; 4. Description of h3cQinQProtocolIndex and h3cQinQBpduTunnelSwitch was modified in the A3COM-HUAWEI-QINQ-MIB. 5. Description of pingCtlDescr was modified in the DISMAN-PING-MIB. 6. Description of hwdot1qVlanIpAddress, and hwdot1qVlanIpAddressMask was modified in the A3COM-HUAWEI-LswVLAN-MIB. 7. Description of h3cUserIndex was modified in the A3COM-HUAWEI-USER-MIB. 8. Description of h3cRdAccRealTime was modified in the A3COM-HUAWEI-RADIUS-MIB. 9. H3C-RRPP-MIB was updated. 10. Description of h3cIdleCut was modified in the A3COM-HUAWEI-USER-MIB. 11. Description of ot3adAggTable and hwAggLinkTable was modified in the IEEE8023-LAG-MIB 12. Description of h3cCfgRunModifiedLast was modified in the A3COM-HUAWEI-CONFIG-MAN-MIB. 13. Description of hwNTPPeerRowStatus was modified in the H3C-NTP-MIB. 14. PDS of h3cRdPrimState, h3cRdSecState, h3cRdPrimAccState, h3cRdSecAccState was modified in the A3COM-HUAWEI-RADIUS-MIB. 15. Description of h3cVoiceVlanEnabledId and h3cVoiceVlanPortEnableList was modified in the A3COM-HUAWEI-VOICE-VLAN-MIB. 16. Description of H3C-SYS-MAN-MIB was modified.. 17. Description of eventDescription was modified in the RMON-MIB. 18. DISMAN-PING-MIB, H3C-NQA-MIB and HUAWEI-DISMAN-PING-MIB was modified.
September 30, 2009				19. Description of h3cCfgLogTable was modified in the A3COM-HUAWEI-STORM-CONSTRAIN.

Version Number	Item	MIB File Name	Module Name	Description
s3q05_01_03s56(s168)	New	None		
	Modified	None		1.
s3q05_01_02s56(s168)	New	Reference Description		1. { h3cevtPortSwitchType 187 }-- SGMII-100-BASE-LX-SFP Transceiver in the ENTITY-MIB 2. { h3cevtPortSwitchType 188} -- SGMII-100-BASE-FX-SFP Transceiver supporting 100BASE-X-SFP in the ENTITY-MIB
	Modified	Reference Description		Description of ntPhysicalVendorType of Section 5.1 was modified to support 1 -10GE XFP Module in the ENTITY-MIB.
s3q05_01_00s56(s168)p01	New	None		
	Modified	None		

Configuration Changes

Configuration Changes in s3q05_02_00s56(s168)p12

None

Configuration Changes in s3q05_02_00s56(s168)p02

The arp detection { dhcp-snooping | dot1x | static-bind } three mode relationship change from "and" to "or", then one of three pass the security check will be successful.

Configuration Changes in s3q05_02_00s56(s168)p01

None

Configuration Changes in s3q05_02_00s56(s168)

None

Configuration Changes in s3q05_01_03s56(s168)

None

Configuration Changes in s3q05_01_00s56(s168)p01

None

Configuration Changes in s3q05_01_00s56(s168)

First release

Open Problems and Workarounds

LSD35368

First found-in version: s3q05_02_00s56(s168)

Description: Disable "traffic redirect" function in web interface, but it can't be effective.

Workaround: Disable "traffic redirect" function by console.

LSD42808

First found-in version: s3q05_02_00s56(s168)

Description: Configure DHCP snooping on a device. A DHCP snooping trusted port on the device receives a DHCP discovery and then a DHCP request packet. After that, if the port receives a DHCP offer or DHCP ACK packet, the packet is forwarded through the receiving port.

Workaround: None

List of Resolved Problems

Resolved Problems in s3q05_02_00s56(s168)p12

LSD42556

First found-in version: s3q05_02_00s56(s168)

Condition: Several 4500G switches connect to the ports of Switch A through different link aggregation groups respectively.

Description: The MAC address of link aggregation group flaps between the ports of Switch A.

ZDTB00157

First found-in version: s3q05_02_00s56(s168)

Condition: Enable LLDP on a port. The VLANs to which the port belongs have no management address configured.

Description: The management address padded in the LLDP packets is 127.0.0.1.

LSD42433

First found-in version: s3q05_02_00s56(s168)

Condition: Connect a device to a huawei’s device(such as Quidway NE or Quidway 5300) through LLDP.

Description: The LLDP neighbor cannot be found.

LSD42556

First found-in version: s3q05_02_00s56(s168)

Condition: Several 4500G switches connect to the ports of Switch A through different link aggregation groups respectively.

Description: The MAC address of link aggregation group flaps between the ports of Switch A.

LSD41220

First found-in version: s3q05_02_00s56(s168)

Condition: Read the dot3adAggEntry mib node.

Description: A wrong value that the NMS cannot identify is returned.

LSD40942

First found-in version: s3q05_02_00s56(s168)

Condition: Connect a device to a CISCO device through LACP aggregation, and then add or remove VLANs on the device.

Description: The aggregation member ports on the CISCO device go down.

LSD40759

First found-in version: s3q05_02_00s56(s168)

Condition: A running device obtains and saves a local certificate and then restarts.

Description: After restart, the local certificate cannot recover, and consequently the functions using the certificate cannot work.

LSD40929

First found-in version: s3q05_02_00s56(s168)

Condition: A devices uses a certificate of a certificate chain that has three or more certificates.

Description: Using HTTPS to log in to the device causes it to reboot.

LSD38359

First found-in version: s3q05_02_00s56(s168)

Condition: A BPDU tunnel interface on the device receives PVST packets tagged with VLANs that are inexistent on the device.

Description: Such PVST packets cannot be encapsulated/de-encapsulated normally.

LSD38221

First found-in version: s3q05_02_00s56(s168)

Condition: Add a BPDU tunnel interface to a link aggregation group and then change the state of the link aggregation group from inactive to active.

Description: There is little probability that the BPDU tunnel interface cannot process received STP packets normally.

Resolved Problems in s3q05_02_00s56(s168)p02

LSD37931

First found-in version: s3q05_02_00s56(s168)p01

Condition: The device has both DHCP snooping and DHCP relay agent enabled.

Description: no record in DHCP-snooping.

Resolved Problems in s3q05_02_00s56(s168)p01

LSD36550

First found-in version: s3q05_02_00s56(s168)

Condition: Insert an RPS power supply into the device.

Description: The web interface displays the power input type of the RPS power supply as AC, which is DC in fact.

LSD37416

First found-in version: s3q05_02_00s56(s168)

Condition: Log out the CLI through the console port and log in to the web interface. Select “Cluster” ->”Setup”->” Build a cluster and to be commander” and configure parameters on the page.

Description: Click **Apply**. The device reboots.

LSD36607

First found-in version: s3q05_02_00s56(s168)

Condition: The device acts as an NTP client.

Description: After the device runs for a while, NTP synchronization fails.

LSD36365

First found-in version: s3q05_02_00s56(s168)

Condition: Configure RADIUS authentication on the device.

Description: The RADIUS packets sent by the device do not contain the Framed-Address standard attribute. This affects cooperation with the EAD solution.

Resolved Problems in s3q05_02_00s56(s168)

LSD10368

First found-in version: s3q05_01_03s56(s168)

Condition: Aggregate two 10GE ports on an expansion board and perform a hot-swap operation to the expansion board.

Description: Some multicast traffic is lost.

LSD10396

First found-in version: s3q05_01_03s56(s168)

Condition: None

Description: The **Xmodem** command is not available in user view, and thus the user can not use the Xmodem protocol to download files to the switch.

LSD10524

First found-in version: s3q05_01_03s56(s168)

Condition: Configure TACACS authentication for SSH users.

Description: SFTP users can access the switch without passing authentication.

LSD11771

First found-in version: s3q05_01_03s56(s168)

Condition: VLAN configuration is changed on a Trunk/Hybrid port.

Description: The port still sends loopback-detection packets with the previous VLAN IDs, and loopback-detection succeeds.

LSD12767

First found-in version: s3q05_01_03s56(s168)

Condition: Display the IPv6 routing table of the Device Manager software.

Description: The destination addresses and next hop addresses of route entries are all wrong.

LSD12783

First found-in version: s3q05_01_03s56(s168)

Condition: Enable 802.1X pap/chap authentication mode.

Description: The self-service function of iNode client software fails.

LSD13004

First found-in version: s3q05_01_03s56(s168)

Condition: MAC authentication is configured on the switch for a user. Modify the user's username and password on the switch when the user is online.

Description: The user cannot pass authentication at the next login.

LSD13018

First found-in version: s3q05_01_03s56(s168)

Condition: Modify a user's username and password used for MAC authentication, and modify the offline-detect timer. Then, tear down all connections.

Description: Some connections cannot be torn down.

LSD13223

First found-in version: s3q05_01_03s56(s168)

Condition: Enable 802.1X authentication on the switch and enable a client to upload its IP address.

Description: The client cannot pass 802.1X authentication.

LSD13239

First found-in version: s3q05_01_03s56(s168)

Condition: A 10 GE port has learned information about its IPv6 neighbor.

Description: The IPv6 neighbor cannot be displayed in Quidview software.

LSD13342

First found-in version: s3q05_01_03s56(s168)

Condition: Tear down a user connection on the CAMS server.

Description: The NAS client on the switch responds with wrong offline reason information showing "Nas Error".

LSD17237

First found-in version: s3q05_01_03s56(s168)

Condition: Add and then delete a MAC address for many times.

Description: A few MAC address deletion operations fail.

LSD22347

First found-in version: s3q05_01_03s56(s168)

Conditions: A 10GE card is inserted into the switch.

Symptoms: The cable type of a 10GE port is displayed as **Not Support** on the Web interface. After the cable type of the 10GE port is set to **Auto**, the cable type is displayed as **Normal**.

LSD22875

First found-in version: s3q05_01_03s56(s168)

Condition: The switch connects to multiple hosts through multiple ports. When STP converges, hosts repeatedly join/leave a multicast group, and 802.1X users log in/out repeatedly:

Description: A memory leak may occur to the 512-byte memory of the 0822 module on the switch.

Resolved Problems in s3q05_01_03s56(s168)

LSD22918

First found-in version: s3q05_01_02s56(s168)

Condition: Insert an SFP module to a Combo port.

Description: The switch cannot recognize the 3CSFP91 and 3CSFP92 SFP modules of FINSTAR.

Resolved Problems in s3q05_01_02s56(s168)

None

Resolved Problems in s3q05_01_00s56(s168) p01

LSD09766

First found-in version: s3q05_01_00s56(s168)

Condition: The Device Manager software is used.

Description: The 10GE ports layout of the CX4 expansion module in the rear panel is not correctly displayed.

LSD10312

First found-in version: s3q05_01_00s56(s168)

Condition: Add some cluster members to the blacklist, disable the cluster, and then enable the cluster.

Description: Those cluster members are still in the blacklist.

LSD10325

First found-in version: s3q05_01_00s56(s168)

Condition: Enable MAC authentication.

Description: MAC authentication currently supports MAC address format “XXXXXXXXXXXX” rather than MAC address format “XX-XX-XX-XX-XX-XX”.

LSD10349

First found-in version: s3q05_01_00s56(s168)

Condition: Enable terminal debugging in user view, and then execute the **pki request-certificate domain** <name> command in system view to retrieve a PKI certificate.

Description: If certificate retrieval fails, the system displays "Fail to retrieval CA certificate of the domain <name>", which should be changed to "Failed to receive a certificate from the CA domain <name>".

LSD10355

First found-in version: s3q05_01_00s56(s168)

Condition: Configure the host name of a server as the RSA public key.

Description: The configuration does not take effect.

LSD10359

First found-in version: s3q05_01_00s56(s168)

Condition: The Device Manager software is used.

Description: The expansion module is displayed on the front panel. In fact, the expansion module reside on the rear panel

LSD10369

First found-in version: s3q05_01_00s56(s168)

Condition: Configure a wrong MIB object index in RMON alarms.

Description: The Get operation works, but the value is meaningless.

LSD10373

First found-in version: s3q05_01_00s56(s168)

Condition: Set the SNMP RMON MIB node.

Description: The switch cannot process long OID variables correctly.

LSD10381

First found-in version: s3q05_01_00s56(s168)

Condition: Configure a multicast VLAN, and add an aggregate port into multiple multicast sub VLANs.

Description: Replication of some multicast traffic in the multicast VLAN may fail on the aggregate port.

LSD10388

First found-in version: s3q05_01_00s56(s168)

Condition: Perform a hot-swap operation to the expansion module during system power-on.

Description: The RMON statistics on the ports of the expansion module are wrong.

LSD10401

First found-in version: s3q05_01_00s56(s168)

Condition: Enable loopback-detection on a trunk port, change the trunk port to an access port, disable loopback-detection, and then change the access port to a trunk port.

Description: The **loopback-detection control enable** command has been executed and cannot be removed.

LSD10415

First found-in version: s3q05_01_00s56(s168)

Condition: Use the **command-privilege level 3 view shell debugging** command in system view to allow only level-3 privilege users to use debug commands.

Description: Lower-level privilege users can still use debug commands.

LSD10548

First found-in version: s3q05_01_00s56(s168)

Condition: The default value of RIP garbage-collect timer is 240 seconds.

Description: To make the value consistent with that defined in RFC, it is changed to 120 seconds.

LSD10591

First found-in version: s3q05_01_00s56(s168)

Condition: Enable RIP.

Description: The switch advertises inactive routes.

LSD10593

First found-in version: s3q05_01_00s56(s168)

Condition: Enable MLD-snooping in a VLAN. A port in the VLAN receives a join request from a host that wants to join a multicast group.

Description: The host cannot join the MLD multicast group.

LSD10597

First found-in version: s3q05_01_00s56(s168)

Condition: Configure a cluster.

Description: Switches in the cluster can't telnet to each other because the telnet server is disabled on a switch by default.

LSD10599

First found-in version: s3q05_01_00s56(s168)

Condition: Configure a cluster. Execute the **cluster switch-to administrator** command on the administrator unit.

Description: The system displays "Cannot execute this command", which is not clear enough. It is recommended to change it to "This is the administrator unit. Issue this command from a member unit".

LSD10680

First found-in version: s3q05_01_00s56(s168)

Condition: Set the maximum number of MAC addresses that a port can learn, and then display the setting on the web interface.

Description: The setting displayed on the web page is followed with "%".

LSD10994

First found-in version: s3q05_01_00s56(s168)

Condition: Enable loopback-detection on the ports of an aggregation group. Loopback-detection protocol packets are sent from a port of the aggregation group.

Description: If another port in the aggregation group receives the packets, this means that the loopback-detection function fails to work.

LSD11077

First found-in version: s3q05_01_00s56(s168)

Condition: Set a very long value for the MIB node etherStatsDataSource.

Description: The switch reboots.

LSD11764

First found-in version: s3q05_01_00s56(s168)

Condition: Enable STP.

Description: The switch cannot process received STP Topology Changes (TCN) packets.

LSD12291

First found-in version: s3q05_01_00s56(s168)

Condition: More than two ports form a link-aggregation group.

Description: The aggregate ports cannot send packets to the CPU.

Resolved Problems in s3q05_01_00s56(s168)

It is the first release of 4500G.

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

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.bin
[ftp] get switch.btm
[ftp] bye
<Switch> boot bootrom switch.btm
please wait ...
 Bootrom is updated!
```

```
<Switch> boot boot-loader switch.bin
<Switch> display boot-loader
The app to boot at the next time is: flash:/ switch.bin
<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 4500G 24-Port BOOTROM, Version 501                    *
  *                                                                            *
  ******************************************************************************
  Copyright(c) 2004-2008 3Com Corp. and its licensors. All rights reserved.
  Creation date   : Nov 12 2008, 19:42:13
  CPU Clock Speed : 264MHz
  BUS Clock Speed : 33MHz
  Memory Size     : 128MB
  Mac Address     : 00e0fc005502


Press Ctrl-B to enter Boot Menu... 5
```

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

Remember your Boot ROM password.

```
  BOOT  MENU


1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. 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.

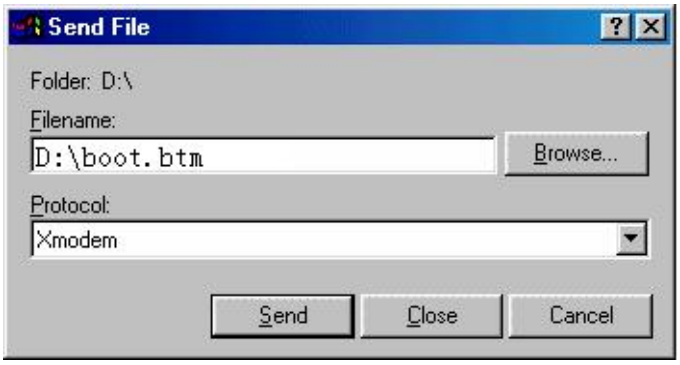

Figure 1 Send file dialog box

Send File

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

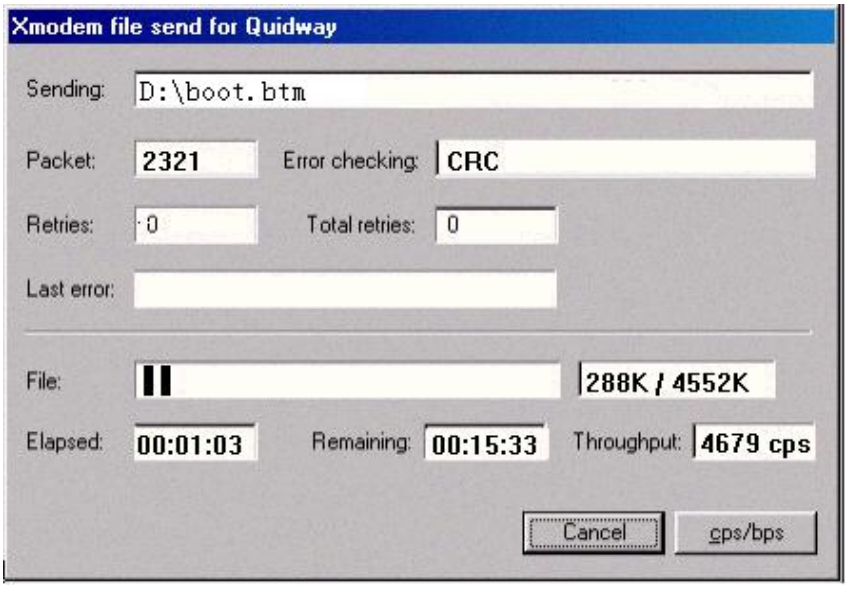

Figure 2 Xmodem File Send

Step 7: After downloading completes, the following information appears:

```
Loading ...CCCCCCCCCC done!
```

Using TFTP Through an Ethernet Interface

1) Introduction to TFTP

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

2) TFTP upgrading 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

Keep in mind your Boot ROM password.

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:

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

Using FTP Through an Ethernet Interface

1) Introduction to FTP

The 4500G can serve as an FTP server or client. In the following example, the 4500 serves as an FTP client.

2) Upgrade procedure

Step 1: Connect an Ethernet interface of the 4800G to the PC where the program files are located, and connect the console port of the switch to the same PC.

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!
```