Switch 4200G V3.02.07 Release Notes

Keywords: Unresolved problems, resolved problems, software upgrading.

Abstract: This release notes describes the Switch 4200G V3.02.07 release with respect to version information, solved and unresolved problems, and software upgrading.

Acronyms:

Abbreviations	Full spelling
ARP	Address Resolution Protocol
BPDU	Bridge Protocol Data Unit
ACL	Access Control List
CLI	Command line interface
DHCP	Dynamic Host Configuration Protocol
DLDP	Device Link Detection Protocol
DNS	Domain Name Server
DSCP	DiffServ Codepoint
FTP	File Transfer Protocol
GARP	Generic Attribute Registration Protocol
GVRP	GARP VLAN Registration Protocol
HGMP	Huawei Group Management Protocol
HTTP	Hypertext Transfer Protocol
IGMP	Internet Group Management Protocol
IGMP Snooping	Internet Group Management Protocol Snooping
IGSP	Internet Group Management Protocol Snooping
IP	Internet Protocol
LACP	Link Aggregation Control Protocol
MAC	Media Access Control
MIB	Management Information Base
MSTP	Multiple Spanning Tree Protocol
NDP	Neighbor Discovery Protocol
NTP	Net Time Protocol
PPS	Packet Per Second

Abbreviations	Full spelling
QOS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RMON	Remote Monitoring
RSTP	Rapid Spanning Tree Protocol
RSA	RSA encryption technique
SDWRR	Shaped Deficit Weighted Round Robin
SNMP	Simple Network Management Protocol
SP	Strict Priority
SSH	Secure Shell
STP	Spanning Tree Protocol
TCP	Transfer Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VLAN-VPN	VLAN-Virtual Private Network
VCT	Virtual Cable Test
3ND	3Com Network Director

Table of Contents

List of Tables

Version Information

Version Number

Version Information: 3Com OS V3.02.07s168

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
V3.02.07s168	V3.02.06s168	2012-12-18	Usage version
V3.02.06s168	V3.02.05s168	2012-10-19	Usage version
V3.02.05s168	V3.02.04s56 V3.02.04s168	2010-09-10	None
V3.02.04s56 V3.02.04s168	V3.02.03s56 V3.02.03s168	2010-03-11	None
V3.02.03s56 V3.02.03s168	V3.02.02s56 V3.02.02s168	2009-08-19	None
V3.02.02s56 V3.02.02s168	V3.02.01s56 V3.02.01s168	2009-06-30	None
V3.02.01s56 V3.02.01s168	V3.02.00s56 V3.02.00s168	2008-12-04	None
V3.02.00s56 V3.02.00s168	V3.01.00s56p02 V3.01.00s168p02	2007-11-20	None
V3.01.00s56p02 V3.01.00s168p02	V3.01.00s56p01 V3.01.00s168p01	2007-10-15	None
V3.01.00s56p01 V3.01.00s168p01	V3.01.00s56 V3.01.00s168	2007-08-28	None
V3.01.00s56 V3.01.00s168	First release	2006-07-03	None

Hardware and Software Compatibility Matrix

Table 2 Hardware and software compatibility matrix

Item	Specifications
Product family	4200G series

Hardware platform	4200G 12-Port 4200G 24-Port 4200G 48-Port 4200G PWR 24-Port
Minimum memory requirements	64 MB
Minimum flash requirements	16 MB
Boot ROM version	Version 2.04 (Note: The version number can be displayed with command **display version** in any view. Please see **Note**②)
Host software	s3t03_02_07s168.app (4,322,019 Bytes)
iMC version	iMC PLAT 5.1 SP1 (E0202P05) iMC UAM 5.1 SP1 (E0301P03) iMC EAD 5.1 SP1 (E0301P03) iMC QoSM 5.1 (E0201) iMC TAM 5.1 (E0301)
iNode version	iNode PC 5.1 (E0304)
Web version	s3v02_10.web
Remarks	s3t03_02_07s168.app uses 168-bit encryption for SSH.

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

```
<4200G>display version
3Com Corporation
Switch 4200G 24-Port Software Version 3Com OS V3.02.07s168  ------note①
Copyright(c) 2004-2012 3Com Corporation and its licensors, All rights reserved.
Switch 4200G 24-Port uptime is 0 week, 0 day, 0 hour, 15 minutes

Switch 4200G 24-Port with 1 MIPS Processor
64M   bytes DRAM
16M    bytes Flash Memory
Config Register points to FLASH

Hardware Version is REV.B
CPLD Version is 002
Bootrom Version is 2.04    ------ note②
[SubSlot 0] 24 GE ( 4 COMBO ) Hardware Version is REV.B
```

Restrictions and Cautions

When configuring the S4200G, be sure that you are aware of these restrictions and cautions:

1) If different traffic actions are defined in the same ACL, following conflicts will occur:

- The action 'deny' conflicts with all the rest actions except for the action 'traffic-statistic'.
- The action of inbound 'traffic-limit' conflicts with the action 'traffic-priority'.

2) Packets of some protocols, such as BPDU, IGMP, DLDP and GVRP, cannot be mirrored remotely.

3) The system allows you to create static link aggregation groups without any member ports, which, however, consume aggregation group resources. If you enable LACP when the maximum aggregation groups are configured, the device cannot create a dynamic aggregation group, while the peer device can. This will cause STP calculation errors.

4) Only the following port configurations can be synchronized between link-aggregation member ports.

- [undo] garp timer hold
- [undo] garp timer join
- [undo] garp timer leave
- [undo] gvrp
- [undo] gvrp registration
- traffic-limit
- traffic-priority
- traffic-redirect
- traffic-remark-vlanid
- traffic-shape
- traffic-statistic
- priority-trust
- packet-filter
- qos-profile
- port link-type { trunk | hybrid }
- [undo] port trunk permit vlan { xxxx | all }
- port trunk pvid vlan xxxx
- port access vlan xxxx
- port hybrid vlan xxxx { tagged | untagged }
- port hybrid pvid vlan xxxx
- port hybrid protocol-vlan vlan xxxx x
- vlan-vpn enable
- vlan-vpn uplink enable
- priority
- stp port priority
- stp cost
- stp enable/disable
- stp edged-port
- stp point-to-point
- stp mcheck
- stp transmit-limit
- stp config-digest-snooping
- stp no-agreement-check
- stp root-protection

- stp loop-protection
- stp compliance
- undo ndp enable
- undo ntdp enalbe

5) The CPU utilization becomes very high when more than two SSH users log in.

6) A version prior to V3.02.07 might not support the cipher and simple keywords or use a different password encryption algorithm than V3.02.07 or a later version. If you downgrade the software from V3.02.07 or a later version to a version prior to V3.02.07, or upgrade it to V3.02.07 or a later version and roll it back after saving the configuration file, the relevant configuration commands might get lost or the passwords might become invalid. For more information, see the change descriptions for the commands.

Feature List

Hardware Features

Table 3 Hardware features

Item	Switch 4200G 12-Port	Switch 4200G 24-Port	Switch 4200G 48-Port	Switch 4200G PWR 24-Port
Dimensions (H × W × D)	43.6 × 440 × 300 mm (1.72 × 17.32 × 11.81 in.)			43.6 × 440 × 420 mm (1.72 × 17.32 × 16.54 in.)
Weight	≤ 4 kg (8.8 lb)	≤ 4.2 kg (9.2 lb)	≤ 5 kg (11 lb)	≤ 6.9 kg (11 lb)
Management port	One Console port			
Service ports	12 10/100/1000 Mbps electric ports 4 Gigabit SFP Combo ports One 10-Gbps slot (for XFP interface cards /XENPAK optical modules)	24 10/100/1000 Mbps electric ports 4 Gigabit SFP Combo ports Two 10-Gbps slots (for XFP interface cards /XENPAK optical modules)	48 10/100/1000 Mbps electric ports 4 Gigabit SFP Combo ports Two 10-Gbps slots (for XFP interface cards /XENPAK optical modules)	24 10/100/1000 Mbps electric ports 4 Gigabit SFP Combo ports Two 10-Gbps slots (for XFP interface cards /XENPAK optical modules)
Input voltage	AC power input: • Rated voltage range: 100 VAC to 240 VAC, 50 Hz or 60 Hz • Max voltage range: 90 VAC to 264 VAC, 47 Hz or 63 Hz DC input (for 4200G PWR 24-Port only): • Voltage range: -52 VDC to -55 VDC			
Input current	1.5 A	1.5 A	1.5 A	AC input: 8 A DC input: 20 A
Maximum power consumption	40 W	68 W	116 W	AC input: 500 W DC input: 435 W

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

Software Features

Table 4 Software features

Category	Features
STP/RSTP/MSTP	• IEEE 802.1s • STP/RSTP/MSTP • Intra-domain maximum-weight spanning trees (up to 16 spanning tree instances supported) • STP root guard • BPDU guard
Port auto-sensing	Speed and duplex auto-negotiation
Jumbo frame	A maximum frame size of 9,216 bytes
Flow control	• IEEE 802.3x flow-control (full duplex) • Back-pressure based flow control (half duplex)
Link aggregation	• Up to 6 aggregation groups, each supporting eight GE or two 10GE ports • Dynamic link aggregation through Link Aggregation Control Protocol (LACP) • Manual link aggregation • Static link aggregation
VLAN	• IEEE 802.1Q • GVRP • Port-based VLANs, with a maximum number of 256 VLANs • Enabling/Disabling MAC address learning in VLANs • Selective QinQ
Broadcast storm suppression	Broadcast storm suppression based on rate (in pps) or bandwidth ratio per port
Internal/external loopback test	The internal loopback test detects the connectivity between switch chips and PHY chips. The 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.
Mirroring	• Port mirroring • Multi-source-port mirroring • Remote port mirroring
MAC address table	• MAC address learning • IEEE 802.1D • Multicast MAC address • Black hole MAC address

	• Up to 8K MAC addresses including 1K static MAC addresses
802.1X	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.
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.
Security features	• Hierarchical management and password protection of users • AAA authentication • RADIUS authentication • SSH 2.0 • Port isolation • Port security
Network Protocols	• TCP/IP protocol stack • ARP • Gratuitous ARP
IGMP snooping	IGMP snooping is a multicast constraining mechanism that runs on Layer 2 devices to manage and control multicast groups. Up to 128 multicast groups are supported.
Multicast VLAN	Based on the current multicast-on-demand mode, when users in different VLANs request the service, a multicast flow is duplicated in each VLAN This mode causes waste of a great deal of bandwidth. To save the bandwidth and enhance security, we provide the multicast VLAN feature. With this feature, you can add switch ports to a multicast VLAN and enable IGMP snooping to allow users in different VLANs to share the same multicast VLAN. As the multicast VLAN is isolated from user VLANs, this guarantees both security and enough bandwidth. The multicast VLAN feature ensures continuous transmission of multicast information flow to users.
Dropping of unknown multicast packets	Generally, if the multicast address of a multicast packet received is not registered on the local switch, the packet will be broadcast within the VLAN. With this feature enabled, the switch will drop any multicast packet with an unregistered multicast address to save bandwidth
DHCP client	A DHCP client uses DHCP to get an IP address and other configuration parameters from a DHCP server.
DHCP relay agent	A DHCP relay agent allows connected DHCP clients to contact a DHCP server on a different subnet to get configuration information. It helps implement centralized management and saves costs.
Static routing	• Up to 8 VLAN interfaces • Up to 32 route entries • Up to 256 ARP entries

UDP helper	UDP helper can convert specific UDP broadcast packets into unicast packets and send them to a designated server.
NTP	Clock synchronization among devices becomes increasingly important. The network time protocol (NTP) is a TCP/IP protocol that releases accurate time throughout the entire network.
QoS	• Port-based/flow-based rate limit, with the minimum granularity of 1kbps • IEEE 802.1p/DSCP priority • Each port supports eight queues. • SP/SDWRR/SP+SDWRR queue scheduling • Traffic classification • Traffic statistics • Port trust mode • Traffic shaping for ports and queues
Password recovery	Password recovery technique is adopted for the recovery of Boot ROM and APP passwords
Diagnostics and alarm output	Detects and reports hardware/software faults.
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.
Software update	• XMODEM protocol • FTP and TFTP • FTP/TFTP client, FTP server
System configuration and management	• Configuration methods supported: CLI, console port, telnet, and Modem • Features and functions supported: SNMP, system logging, hierarchical alarming, remote monitoring (RMON) 1/2/3/9 group MIBs, web NMS, Huawei Group Management Protocol (HGMP) v2, power status detection and alarming, fan alarming
Maintenance	Filtering and output of alarm/debug information Diagnostic tools: Ping, Trace, and so on Remote maintenance by Telnet and other ways

Version Updates

Feature Updates

Table 5 Feature updates

Version Number	Item	Description
V3.02.07	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software	New Features: None

	Features	Deleted Features: None Modified Features: None
V3.02.06	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: None Deleted Features: None Modified Features: None
V3.02.05	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: None Deleted Features: None Modified Features: None
V3.02.04	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: • Support IPv6 static route • Support MLD-Snooping • Support DHCP V6 snooping • Support IPv6 check • Support IPv6 am user-bind • Support SSHv6 • Support snmpv6 • Support ND detection • Support ND snooping • Support control multicast • Support multiple radius server • Support separate AAA • Support dot1x mandatory domain • Support dot1x IPv6 • Support triple authentication • Support unknown-unicast trigger dot1x authentication • Support web-authentication roaming • Support configure web-authentication proxy port number • Support DHCP server Deleted Features: None Modified Features: None
V3.02.03	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software	New Features:

	Features	• LACP MAD • Loopback-detection shutdown Deleted Features: None Modified Features: None
V3.02.02	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: • Web https • Loopback-detection trap Deleted Features: None Modified Features: None
V3.02.01	Changed Hardware Features	New Features: None. Deleted Features: None
	Changed Software Features	New Features: • Auto VLAN • Auto power down • Storm constrain • LLDP • VLAN VPN (Tunnel) • BPDU dropping • DHCP snooping • DHCP snooping option82 • DHCP security • DHCP option60 • PKI • Protocol VLAN • DLDP • Triple authentication • IP check • Link-delay • MAC based and VLAN based mirroring • Priority mapping • QoS profile • Flow redirection • Remarking of VLAN ID • Cluster stacking • Web authentication • Selective QinQ • ARP anti-attack • ARP/DHCP rate limit • Maximum ARP entries allowed to learn on a per port basis • ARP detection • User service by self

		• MAC learning control on a per VLAN basis • 802.1X handshake security • MSTP pathcost legacy • IPv6 ACL • UDP helper TTL control • Default gateway assignment through DHCP Deleted Features: None Modified Features: • Up to 16 K MAC addresses • Up to 1024 multicast entries • Up to 4094 VLANs
V3.02.00	Changed Hardware Features	New Features: New deliverable. Deleted Features: None
	Changed Software Features	New Features: • RSA key transformation • DNS client • Syslog enhancement • TCP/UDP ports are closed by default. • Reboot scheduling • Configurable flow interval • Port auto negotiation mode configuration • Control of port up/down traps/logs • 1000M port support for 100M optical module • Smart link • SNMP v3 support for AES encryption • Banner for FTP/HTTP • SSH2.0 support for DSA • SSH2.0 intercommunication with other clients • Disabling/enabling temperature-protection (only for PoE devices) • Copyright information for telnet login • Legal banner • The default information of banner is removed. • 802.1X re-authentication • 802.1X handshake controllable • Voice VLAN (including CDP) • Domain MIB support for AAA separation • Information center support for UTC time • MAC authentication enhancement • HWping • Burst mode • EAD fast deployment • The EAD NAS port ID is allowed to be modified. • Port security and/or mode • High-end memory recording function

		• VLAN ACL • Telnet authentication supports processing of RADIUS access challenge packets. • HWTACACS • PoE (only for PoE devices) • EAD solutions Deleted Features: None Modified Features: None
V3.01.00p02	Changed Hardware Features	New Features: Burst-mode function Deleted Features: None
	Changed Software Features	New Features: None Deleted Features: None Modified Features: None
V3.01.00	Changed Hardware Features	New Features: First release Deleted Features: None
	Changed Software Features	New Features: First release Deleted Features: None Modified Features: None

Command Line Updates

Table 6 Command line updates

Version Number	Item	Description
V3.02.07	New Commands	None.
	Deleted Commands	**local-user password-display-mode { auto | cipher-force }** **undo local-user password-display-mode**.
	Modified Commands	• Command1 Original command: **bims-server ip** *ip-address* **[port** *port-number* **] sharekey** *key* Modified command: **bims-server ip** *ip-address* **[port** *port-number* **] sharekey [cipher | simple]** *key* • Command2 Original command: **dhcp server bims-server ip** *ip-address* **[port** *port-number* **] sharekey** *key* **{ interface** *interface-type interface-number* **[to** *interface-type interface-number* **] | all }**

		Modified command: **dhcp server bims-server ip** *ip-address* **[port** *port-number* **] sharekey [cipher | simple]** *key* **{ interface** *interface-type interface-number* **[to** *interface-type interface-number* **] | all }** • Command3 Original command: **dldp authentication-mode { none | simple** *simple-password* **| md5** *md5-password* **}** Modified command: **dldp authentication-mode { none | { simple | md5 }** *password* **}** • Command4 Original command: **key { accounting | authentication | authorization }** *string* Modified command: **key { accounting | authentication | authorization } [cipher | simple]** *string* • Command5 Original command: **key { accounting | authentication }** *string* Modified command: **key { accounting | authentication } [cipher | simple]** *string* • Command6 Original command: **local-server nas-ip** *ip-address* **key** *password* Modified command: **local-server nas-ip** *ip-address* **key [cipher | simple]** *password* • Command7 Original command: **mac-authentication authmode usernameasmacaddress [usernameformat { with-hyphen | without-hyphen } { lowercase | uppercase } | fixedpassword** *password* **]** Modified command: **mac-authentication authmode usernameasmacaddress [usernameformat { with-hyphen | without-hyphen } { lowercase | uppercase } | fixedpassword [cipher | simple]** *password* **]**

		• Command8 Original command: **mac-authentication authpassword** *password* Modified command: **mac-authentication authpassword [cipher | simple]** *password* • Command9 Original command: **ntp-service authentication-keyid** *keyid* **authentication-mode md5** *value* Modified command: **ntp-service authentication-keyid** *keyid* **authentication-mode md5 [cipher | simple]** *value* • Command10 Original command: **password** *password* Modified command: **password [cipher | simple]** *password* • Command11 Original command: **primary accounting {** *ip-address* **| ipv6** *ipv6-address* **} [** *port-number* **] [key** *string* **]** Modified command: **primary accounting {** *ip-address* **| ipv6** *ipv6-address* **} [** *port-number* **] [key [cipher | simple]** *string* **]** • Command12 Original command: **primary authentication {** *ip-address* **| ipv6** *ipv6-address* **} [** *port-number* **] [key string]** Modified command: **primary authentication {** *ip-address* **| ipv6** *ipv6-address* **} [** *port-number* **] [key [cipher | simple]** *string* **]** • Command13 Original command: **secondary accounting {** *ip-address* **| ipv6** *ipv6-address* **} [** *port-number* **] [key** *string* **]** Modified command: **secondary accounting {** *ip-address* **| ipv6** *ipv6-address* **} [** *port-number* **] [key [cipher | simple]**

		string **]** • Command14 Original command: **secondary authentication {** *ip-address* **| ipv6** *ipv6-address* **} [** *port-number* **] [key** *string* **]** Modified command: **secondary authentication {** *ip-address* **| ipv6** *ipv6-address* **} [** *port-number* **] [key [cipher | simple]** *string* **]** • Command15 **set authentication password { simple | cipher }** *password* Before modification: When you specify the **cipher** keyword, you can enter a string of 1 to 16 characters or a string of 24 characters as the password. After modification: When you specify the **cipher** keyword, you can enter a string of 1 to 53 characters as the password. • Command16 **snmp-agent usm-user v3** *user-name group-name* **[[cipher] authentication-mode { md5 | sha }** *auth-password* **[privacy-mode { aes128 | des56 }** *priv-password* **]] [acl** *acl-number* **]** Before modification: Only authentication and privacy keys in hexadecimal format are supported. After modification: Both hexadecimal and non-hexadecimal format authentication and privacy keys are supported. • Command17 **super password [level user-level] { cipher | simple }** *password* Before modification: When you specify the **cipher** keyword, you can enter a string of 1 to 16 characters or a string of 24 characters as the password. After modification: When you specify the **cipher** keyword, you can enter a string of 1 to 53 characters as the password. • Command18 **password { cipher | simple }** *password* Before modification: If **cipher** is specified, you can set an 88-character password or a password of 1 to 63 characters. After modification: If **cipher** is specified, you can set a password of 1 to 117 characters.
V3.02.06	New Commands	None.
	Deleted Commands	None.

	Modified Commands	None.
V3.02.05	New Commands	None.
	Deleted Commands	None.
	Modified Commands	None.
V3.02.04	New Commands	**web-authentication move-mode** *{auto* | *secure}* **web-authentication web-proxy port** *proxy-port-id* **web-authentication free-user ip** *ip-address* **mac** *mac-address* **[interface** *interface-list***]** **igmp-snooping access-policy** *acl-number* **undo igmp-snooping access-policy {** *acl-number* **| all }** **mld-snooping access-policy** *acl6-number* **undo mld-snooping access-policy {** *acl6-number* **| all }** **acl ipv6 number** *acl6-number* **[name** *acl6-name* **] [match-order { auto | config }]** **undo acl ipv6 { all | name** *acl6-name* **| number** *acl6-number* **}** **acl ipv6 copy** *{ source-acl6-number* | **name** *source-acl6-name }* **to** *{ dest-acl6-number* | **name** *dest-acl6-name }* **acl ipv6 name** *acl6-name* **description** *text* **undo description** **display acl ipv6** *{ acl6-number* | **all | name** *acl6-name }* **hardware-count enable** **undo hardware-count enable** **reset acl ipv6 counter** *{ acl6-number* | **all** | **name** *acl6-name }* **rule** *[rule-id] {* **deny | permit** *} [* **counting** | **fragment** | **logging** | **source** *{ ipv6-address prefix-length* | *ipv6-address/prefix-length* | **any** *}* | **time-range** *time-range-name]* **undo rule** *rule-id [* **counting** | **fragment** | **logging** | **source** | **time-range** *]* **rule** *[rule-id] {* **deny** | **permit** *} protocol [{ {* **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value } ** | **established** *}* | **counting** | **destination** *{ dest dest-prefix* | *dest/dest-prefix* | **any** *}* | **destination-port** *operator port1 [port2]* | **dscp** *dscp* | **flow-label** *flow-label-value* | **fragment** | **icmpv6-type** *{ icmpv6-type icmpv6-code* | *icmpv6-message }* |

		logging | **source** *{ source source-prefix* | *source/source-prefix* | **any** *}* | **source-port** *operator port1 [port2]* | **time-range** *time-range-name]* **undo rule** *rule-id [{ { {* **ack** | **fin** | **psh** | **rst** | **syn** | **urg** *} ** | **established** *}* | **counting** | **destination** | **destination-port** | **dscp** | **flow-label** | **fragment** | **icmpv6-type** | **logging** | **source** | **source-port** | **time-range** *]* **rule** *protocol [* **addr-flag** *addr-flag* | **destination** *{ dest dest-prefix* | *dest/dest-prefix* | **any** *}* | **destination-port** *operator port1 [port2]* | **dscp** *dscp* | **frag-type** *{* **fragment** | **fragment-subseq** | **non-fragment** | **non-subseq** *}* | **icmpv6-type** *{ icmpv6-type icmpv6-code* | *icmpv6-message }* | **source** *{ source source-prefix* | *source/source-prefix* | **any** *}* | **source-port** *operator port1 [port2]* | **tcp-type** { **tcpurg** | **tcpack** | **tcppsh** | **tcprst** | **tcpsyn** | **tcpfin** *}]* **undo rule [addr-flag | destination | destination-port | dscp | frag-type | icmp6-type | source | source-port | tcp-type]** **rule** *rule-id* **comment** *text* **undo rule** *rule-id* **comment** **step** *step-value* **undo step** **dot1x auth-fail vlan** *authfail-vlan-id* **undo dot1x auth-fail vlan** **dot1x unicast-trigger** **undo dot1x unicast-trigger** **mac-authentication auth-fail vlan** *authfail-vlan-id* **undo mac-authentication auth-fail vlan** **web-authentication auth-fail vlan** *authfail-vlan-id* **undo web-authentication auth-fail vlan** **web-authentication select method extended** **undo web-authentication select** **dot1x mandatory-domain** *domain-name* **undo dot1x mandatory-domain** **authentication lan-access { local | none | radius-scheme** *radius-scheme-name* **[local | none] }** **undo authentication lan-access** **authentication login { hwtacacs-scheme** *hwtacacs-scheme-name* **[local] | local | none | radius-scheme** *radius-scheme-name* **[local] }**

		undo authentication login **authorization { hwtacacs-scheme** *hwtacacs-scheme-name* **[local] | local | none }** **undo authorization** **authorization login { hwtacacs-scheme** *hwtacacs-scheme-name* **[local] | local | none }** **undo authorization login** **accounting { hwtacacs-scheme** *hwtacacs-scheme-name* **[local] | local | none | radius-scheme** *radius-scheme-name* **[local] }** **undo accounting** **accounting lan-access { local | none | radius-scheme** *radius-scheme-name* **[local | none] }** **undo accounting lan-access** **accounting login { hwtacacs-scheme** *hwtacacs-scheme-name* **[local] | local | none | radius-scheme** *radius-scheme-name* **[local] }** **undo accounting login** **scheme lan-access { local | none | radius-scheme** *radius-scheme-name* **[local | none] }** **undo scheme lan-access** **scheme login { local | none | radius-scheme** *radius-scheme-name* **[local] | hwtacacs-scheme** *hwtacacs-scheme-name* **[local] }** **undo scheme login** **display domain [** *isp-name* **]** **primary authentication {** *ip-address* **| ipv6** *ipv6-address* **} [** *port-number* **] [key** *key-string***]** **undo primary authentication** **primary accounting {** *ip-address* **| ipv6** *ipv6-address* **} [** *port-number* **] [key** *key-string***]** **undo primary accounting** **secondary authentication {** *ip-address* **| ipv6** *ipv6-address* **} [** *port-number* **] [key** *key-string* **]** **undo secondary authentication {** *ip-address* **| ipv6** *ipv6-address* **}** **secondary accounting {** *ip-address* **| ipv6** *ipv6-address* **} [** *port-number* **] [key** *key-string* **]** **undo secondary accounting { ip-address | ipv6 ipv6-address }** **state { primary | secondary } { accounting | authentication } {** *ip-address* **| ipv6** *ipv6-address* **} { active | block }**

		ipv6 nd snooping enable **undo ipv6 nd snooping enable** **display ipv6 nd snooping** **ipv6 check source ip-address [** *mac-address* **]** **undo ipv6 check source ip-address [** *mac-address* **]** **ipv6 check source ip-address** **undo ipv6 check source ip-address** **ipv6 check source ip-address mac-address** **undo ipv6 check source ip-address mac-address** **ipv6 source static binding ip-address ip-address [mac-address** *mac-address* **]** **undo ipv6 source static binding ip-address ip-address** **ipv6 source static binding ip-address** **undo ipv6 source static binding ip-address** **display ipv6 source static binding [vlan** *vlan-id* **| interface interface-type** *interface-number* **]** **dhcp-snooping ipv6 enable** **undo dhcp-snooping ipv6 enable** **dhcp-snooping ipv6 trust** **undo dhcp-snooping ipv6 trust** **display dhcp-snooping ipv6 all** **reset dhcp-snooping ipv6 all** **am user-bind mac-addr mac-address ipv6** *ipv6-address* **[interface interface-type** *interface-number* **]** **undo am user-bind mac-addr mac-address ipv6** *ipv6-address* **[interface interface-type** *interface-number* **]** **display am user-bind ipv6 [interface interface-type** *interface-number* **| ipv6-address** *ipv6-address* **| mac-addr** *mac-address* **]**
	Deleted Commands	None.
V3.02.03	New Commands	**loopback-detection shutdown enable** **undo loopback-detection shutdown enable** **multicast-suppression** { *ratio* **| pps** *max-pps* } **undo multicast-suppression** **unicast-suppression** { *ratio* **| pps** *max-pps* }

		undo unicast-suppression
	Deleted Commands	None.
	Modified Commands	None.
V3.02.02	New Commands	**display ip https** **ip https acl** *acl-number* **undo ip https acl** **ip https certificate access-control-policy** *policy-name* **undo ip https certificate access-control-policy** **ip https enable** **undo ip https enable** **ip https ssl-server-policy** *policy-name* **undo ip https ssl-server-policy** **ciphersuite** [**rsa_3des_ede_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_256_cbc_sha** | **rsa_des_cbc_sha** | **rsa_rc4_128_md5** | **rsa_rc4_128_sha**] **client-verify enable** **undo client-verify enable** **close-mode wait** **undo close-mode wait** **display ssl client-policy** { *policy-name* | **all** } **display ssl server-policy** { *policy-name* | **all** } **handshake timeout** *time* **undo handshake timeout** **pki-domain** *domain-name* **undo pki-domain** **prefer-cipher** { **rsa_3des_ede_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_256_cbc_sha** | **rsa_des_cbc_sha** | **rsa_rc4_128_md5** | **rsa_rc4_128_sha** } **undo prefer-cipher** **session** { **cachesize** *size* | **timeout** *time* } **undo session** { **cachesize** | **timeout** } **ssl client-policy** *policy-name* **undo ssl client-policy** { *policy-name* | **all** } **ssl server-policy** *policy-name* **undo ssl server-policy** { *policy-name* | **all** }

		version { **ssl3.0** | **tls1.0** } **undo version**
	Deleted Commands	None
	Modified Commands	None
V3.02.01	New Commands	Please refer to the command manuals.
	Deleted Commands	Please refer to the command manuals.
	Modified Commands	Please refer to the command manuals.
V3.02.00	New Commands	Please refer to the command manuals.
	Deleted Commands	Please refer to the command manuals.
	Modified Commands	Please refer to the command manuals.
V3.01.00p02	New Commands	Command1 Syntax: **burst-mode enable** undo burst-mode enable View: System view Parameter: none Description: Use the **burst-mode enable command** to enable the burst function. Use the **undo burst-mode enable** command to disable the burst function. By default, the burst function is disabled. Example: `[4200G] burst-mode enable`
	Deleted Commands	None
	Modified Commands	None
V3.01.00	New Commands	First release
	Deleted Commands	First release
	Modified Commands	First release

MIB Updates

Table 7 MIB updates

Version Number	Item	MIB file	Module	Description
V3.02.07	New	None	None	None
	Modified	None	None	None
V3.02.06	New	None	None	None
	Modified	None	None	None

V3.02.05	New	None	None	None
	Modified	None	None	None
V3.02.04	New	None	None	None
	Modified	None	None	None
V3.02.03	New	None	None	None
	Modified	None	None	None
V3.02.02	New	a3com-huawei-lpbkdt.mib	A3COM-HUAWEI-LPBKDT	loopback detection send trap
	Modified	None	None	None
V3.02.01	New	h3c-radius.mib	H3C-RADIUS	Support accounting-on MIB
	Modified	IEEE8021-PAE-MIB	dot1xPaePortInitialize	After you set the attribute of the module to true, all 802.1X users on the corresponding port are disconnected, and then the attribute of the module returns to false. If you perform get operations on the module, it always returns “false”. (This module did not function in the past.)

Configuration Changes

Configuration Changes in V3.02.07

None

Configuration Changes in V3.02.06

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

Configuration Changes in V3.02.05

1) The Changes of syslog records WEB user’s name

Before Modification:

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
```

After Modification:

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

Before Modification:

LLDP packets are forwarded to other ports if LLDP function is disabled globally.

After Modification:

LLDP packets aren't forwarded if LLDP function is disabled globally.

3) The Changes of of the bootp reply packet's length

Before Modification:

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.

After Modification:

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.

Configuration Changes in V3.02.04

1) The changes in Operations of ARP filter binding numbers on one port

Before modification:

On one port, only one ARP filter binding item can be set to.

After modification:

On one port, eight ARP filter binding items can be set to.

2) The change to web-authentication free-user buildrun

Before modification:

Web-authentication free-user is displayed on global view .

After modification:

Web-authentication free-user is displayed on port view.

3) The change to DHCP server, DHCP snooping and DHCP Relay

Before modification:

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

After modification:

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.

Configuration Changes in V3.02.03

1) The change to the broadcast-suppression

Before modification:

The broadcast-suppression command will suppress both the unknown-multicast packets and unknown-unicast packets.

After modification:

The broadcast-suppression command, multicast-suppression command and unicast-suppression command can be configured separately. Each of them will be covered by each other, and the last command take effect.

2) The change to the Syslog

Before modification:

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

After modification:

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

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

Before modification:

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.

After modification:

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.

4) The change to the storm constrain function

Before modification:

Can not configure storm constrain function after a fabric port is enabled.

After modification:

User can configure storm constrain function after a fabric port is enabled.

Configuration Changes in V3.02.02

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

Before modification:

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

After modification:

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

2) The operation about Management address in LLDP packets

Before modification:

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.

After modification:

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

(b) 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;

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

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

Before modification:

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.

After modification:

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

Configuration Changes in V3.02.01

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

Before modification:

The interval for sending 802.1X multicast requests set with the **dot1X timer tx-period** command is in the range 10 to 120 seconds. If a port joins the guest VLAN upon receiving no response for an 802.1X multicast request, the shortest time for the port to join the guest VLAN is about 10 seconds.

After modification:

The interval for sending 802.1X multicast requests set with the **dot1X timer tx-period** command is in the range 1 to 120 seconds. If a port joins to the guest VLAN upon receiving no response for an 802.1X multicast request, the shortest time for the port to join the guest VLAN is about 1 second.

Configuration Changes in V3.02.00

None

Open Problems and Workarounds

None

List of Resolved Problems

Resolved Problems in V3.02.07

LSOD010584

- First Found-in Version: V3.02.05
- Condition: Configure password in ciphertext.
- Description: Because of the weak cryptographic algorithm there is a risk that the stored passwords possibly be cracked.

Resolved Problems in V3.02.06

LSOD010576

- First Found-in Version: V3.02.05
- Condition: Access the hh3cUserPassword node of hh3cUserInfoTable by SNMP.
- Description: When access the hh3cUserPassword node of hh3cUserInfoTable by SNMP, the device returns the user's password.

Resolved Problems in V3.02.05

LSOD10073

- First Found-in Version: V3.02.01
- Condition: If the original version is V3.02.00, update to later version.
- Description: Manufacture information is lost.

LSOD09902

- First Found-in Version: V3.02.04
- Condition: CPU is busy and there is a lot of trap information in a moment.
- Description: device reboots abnormally.

LSOD09931

- First Found-in Version: V3.02.04
- Condition: configured **'snmp-agent target-host trap address udp-domain A.B.C.D (D>223) params securityname RADAR'** in system view.
- Description: execute **'undo snmp-agent target-host A.B.C.D (D>223) securityname RADAR'** unsuccessfully.

ZDD03035

- First Found-in Version: V3.02.04
- 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.

LSOD10018

- First Found-in Version: V3.02.04
- 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.

LSOD09927

- First Found-in Version: V3.02.04
- Condition: Switch serves as DHCP relay and DHCP snooping, PC requests IP address through switch.
- Description: PC can get IP address successfully, but DHCP snooping can not record item.

LSOD09838

- First Found-in Version: V3.02.04
- 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.

LSOD09895

- First Found-in Version: V3.02.04
- Condition: In radius scheme, configure primary authentication server with an IPv4 address, and secondary authentication server with an IPv6 address. Do dot1X authentication with RADIUS server. The dot1X client uploads both IPv4 and IPv6 address at the same time.
- Description: If primary server has no response, the device will do authentication with secondary server, but it can't succeed. The device reboots probably.

LSOD09897

- First Found-in Version: V3.02.04
- Condition: Dot1X user login on port A, and authorization VLAN X is assigned. Than this user moves to login on port B, and the authorization VLAN X still is assigned.
- Description: After moving to port B, MAC-based VLAN of the user is lost.

LSOD09925

- First Found-in Version: V3.02.04
- 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.

LSOD09926

- First Found-in Version: V3.02.04
- 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.

ZDD02870

- First Found-in Version: V3.02.04
- 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.

LSOD09844

- First Found-in Version: V3.02.04
- Condition: In radius scheme, configure primary authentication server with IPv4 address, and secondary authentication server with IPv6 address. Do 802.1X authentication with RADIUS server. The 802.1X client uploads both IPv4 and IPv6 address simultaneously.
- Description: If primary server has no response, the device will do authentication with secondary server, but it can't succeed.

LSOD09845

- First Found-in Version: V3.02.04
- Condition: Enable MAC-based VLAN on the port. The 802.1X user logs in successfully on the port, and authorization VLAN ID A is assigned to the user. When 802.1X re-authentication occurs, authorization VLAN ID B is assigned to the user.
- Description: After re-authentication, the MAC address of the user in VLAN A still exists.

LSOD09849

- First Found-in Version: V3.02.04
- Condition: Enable MAC-based VLAN on the port. Configure both '**dot1x auth-fail vlan**' and '**mac-authentication auth-fail vlan**' to VLAN X. MAC-address A enters '**dot1x auth-fail vlan**', MAC-address B enters '**mac-authentication auth-fail vlan**'.
- Description: MAC-address A or B can not be deleted after shutdown the port.

LSOD09873

- First Found-in Version: V3.02.04
- Condition: Neither 'dot1x authentication' nor mac-authentication is enabled on the port. Only web-authentication is enabled. The user fails in authentication and enters the auth-fail VLAN.
- Description: The user ACL isn't deleted after the user logs out from auth-fail VLAN.

LSOD09865

- First Found-in Version: V3.02.04
- Condition: Both the 'Mac-authentication' and 'mac-authentication guest-vlan' are enabled on the port. User A is online, and user B tries to log in by 'mac-authentication'.
- Description: User B can not pass the 'mac-authentication'.

LSOD09834

- First Found-in Version: V3.02.04
- Condition: When an HGMP stack is established, two communities named public and private are automatically created for this stack. Create a new SNMP community named public or private, and associate an ACL with this community. Save the configuration. Then reboot the device, or disable and then enable the stack.
- Description: The SNMP community is not associated with an ACL.

LSOD09836

- First Found-in Version: V3.02.04

- Condition: The device had a static ND entry whose layer 3 interface is Interface_A. The Interface_A was deleted.
- Description: The ACL resource was not freed.

TCD02292

- First Found-in Version: V3.02.04
- Condition: The switch receives many MLD snooping report packets.
- Description: The memory will be exhausted.

LSOD09860

- First Found-in Version: V3.02.04
- Condition: Perform ‘mac-authentication’ and ‘dot1x authentication’ on port.
- Description: After user passed ‘mac-authentication’, the same user can not do ‘dot1x authentication’ successfully.

TCD02318

- First Found-in Version: V3.02.04
- Condition: Configure default static route ‘**ipv6 route-static :: 0 xxx**’, and do not learn the ND of the nexthop.
- Description: IPv6 multicast packet can not be forward.

LSOD09174

- First Found-in Version: V3.02.01
- Condition: Decompress and run app in bootrom, the switch can not receive packets forward to cpu.
- Avoidance: Do not Decompress and run app in bootrom.

Resolved Problems in V3.02.04

LSOD09831

- First Found-in Version: V3.02.03
- Condition: The client application does dot1x authentication with TTLS certification.
- Description: By chance, the device reboots abnormally for dead loop.

LSOD09755

- First Found-in Version: V3.02.03
- Condition: The DLDP state of the port is active and the opposite port state is disabled.
- Description: The state-machine of DLDP switches between ‘disable’ and ‘active’, so the port goes up/down endless.

LSOD09701

- First Found-in Version: V3.02.03
- Condition: The web-authentication and MAC-authentication are both enabled on two ports, and a user passes the MAC-authentication on one port. The user moving to another port does MAC -authentication.

- Description: The mac-authentication will fail.

LSOD09733

- First Found-in Version: V3.02.03
- Condition: Configure an invalid user-defined IPv6 ACL rule, for example, a rule containing an incorrect subnet mask, at the web interface.
- Description: The invalid rule is applied on the device successfully and included in the running configuration, but it does not take effect. The rule cannot survive a root, even if you have saved configuration.

LSOD09676

- First Found-in Version: V3.02.03
- Condition: Client perform web authentication.
- Description: Client cannot relet IP address before pass web authentication.

LSOD09810

- First Found-in Version: V3.02.03
- 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.

LSOD09646

- First Found-in Version: V3.02.03
- Condition: The network device acted as SSH server, and received specific SSH attack packets.
- Description: The device will be rebooted abnormally.

LSOD09656

- First Found-in Version: V3.02.03
- Condition: Configure '**mac-authentication timer guest-vlan-reauth**'.
- Description: The timer doses not take effect.

LSOD09326

- First Found-in Version: V3.02.03
- Condition: As the following operation:Create an SSL server policy, example: ssl server-policy myssl1;Https use this SSL server policy, example: ip https ssl-server-policy myssl1;Undo use this SSL server policy, example: undo ip https ssl-server-policy.
- Description: This ssl server policy can't be deleted.

LSOD09654

- First Found-in Version: V3.02.03
- 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.

LSOD09566

- First Found-in Version: V3.02.03
- Condition: Configure '**accounting optional**'. Configure '**dot1x timer server-timeout**' to X seconds. Do dot1X authentication with RADIUS server. When logging in, accounting-Start packet from the switch to the RADIUS server gets no response.
- Description: After log out, the client can not log in again until X seconds after.

LSOD09624

- First Found-in Version: V3.02.03
- Condition: Disable LLDP on device globally. Port X received LLDP packet.
- Description: The LLDP packet is forwarded to the other ports which should be discarded.

LSOD09555

- First Found-in Version: V3.02.03
- 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: V3.02.03
- 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.

LSOD09537

- First Found-in Version: V3.02.03
- 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.

LSOD09498

- First Found-in Version: V3.02.03
- 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.

LSOD09434

- First Found-in Version: V3.02.03
- 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: V3.02.03
- 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: V3.02.03
- 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: V3.02.03
- Condition: Configure DHCP rate limit on port, and display the configuration.
- Description: The switch shows the default configuration.

LSOD09374

- First Found-in Version: V3.02.03
- Condition: Configure **'ipv6-acl-template dest-port ip-protocol'** and **'ipv6-acl-template ip-protocol dest-port'**.
- Description: The operation of **'ipv6-acl-template dest-port ip-protocol'** returns error, but the operation of **'ipv6-acl-template ip-protocol dest-port'** returns ok. The configuration may fail because of the different sequence of the parameters.

LSOD09048

- First Found-in Version: V3.02.03
- 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.

LSOD09439

- First Found-in Version: V3.02.03
- 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: V3.02.03
- Condition: Connect device to HUAWEI S2300 and running LLDP.
- Description: The device can not find S2300 as LLDP neighbor.

LSOD09399

- First Found-in Version: V3.02.03

- Condition: Perform packet-filter with IPv6 user-defined ACL matching DSCP
- Description: Can not match IPv6 packet with specified DSCP

LSOD09653

- First Found-in Version: V3.02.03
- 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 V3.02.03

LSOD09106

- First found-in version: V3.02.02
- 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.

LSOD08774

- First found-in version: V3.02.02
- Condition: Do EAD authentication with IMC server.
- Description: The user goes off-line soon after passing the security checking.

LSOD09095

- First found-in version: V3.02.02
- 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: V3.02.02
- 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: V3.02.01
- 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.

LSOD08988

- First found-in version: V3.02.02
- Condition: One user with privilege level 0 login the web management interface.
- Description: WEB can not show the page of "Help".

LSOD09075

- First found-in version: V3.02.02
- Condition: Configure “storm-constrain control shutdown” mode on device.
- Description: Fail to perform “shutdown” on the device when it reach to the upper limitation of broadcast packets.

ZDD02152

- First found-in version: V3.02.02
- Condition: Switch work as Telnet client or server. Input non-english character after login.
- Description: Possible unexpected logout.

LSOD09059

- First found-in version: V3.02.00
- 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.

Resolved Problems in V3.02.02

LSOD08968

- First found-in version: V3.02.00
- 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: V3.02.01
- 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.

LSOD08575

- First found-in version: V3.02.01
- Condition: Configure “IGMP-snooping nonflooding” and NTP multicast client.
- Description: The device can not synchronize the timer from NTP server.

ZDD02002

- First found-in version: V3.02.01
- Condition: Enable the function of DHCP SNOOPING on switch.
- Description: If the UDP port number of the packet is not 67 or 68, the switch can not transmit the DHCP packet correctly.

LSOD08743

- First found-in version: V3.02.01
- Condition: Open web page "Port>Administration [Summary]", then select feature "Flow Control".
- Description: An "Internal error" message is displayed.

LSOD08065

- First found-in version: V3.02.01
- Condition: Create cluster first. Then Login Web Management, and open the page of "Cluster>Cluster Upgrade [Summary]" to check the Web version in the page list.
- Description: The Web version is not correct.

LSOD08932

- First found-in version: V3.02.01
- Condition: Reboots the device.
- Description: In a very small chance, exception would occur, and the device would reboot repeatedly.

LSOD08273

- First found-in version: V3.02.01
- Condition: Configure "* ?" (* denotes any character) on the port that supports the stack port attribute.
- Description: The stack-port command will appear in the help info list.

LSOD08600

- First found-in version: V3.02.01
- Condition: Configure Quick EAD Deployment and am user-bind on the same port.
- Description: The ip address designated by am user-bind is permitted without authentication.

LSOD08571

- First found-in version: V3.02.01
- Condition: Configure am user-bind on the port.
- Description: Switch drop the ARP packet with the IP address.

LSOD08756

- First found-in version: V3.02.01
- Condition: Plug in 3Com customized SFP module to the device which manufacturer is not 3Com.
- Description: The vendor name information is displayed as "3Com" in command "display transceiver" which should be the actual manufacturer name.

Resolved Problems in V3.02.01

LSOD08147

- First found-in version: V3.02.00
- Condition: Configure password information.
- Description: The password can be displayed in log information, which compromises security.

LSOD08283

- First found-in version: V3.02.00
- Condition: Specify an NTP server (1.1.1.2, for example) without specifying a source interface or source address on the device that acts as an NTP client. The device will select a source address automatically (1.1.1.1, for example) to communicate with the specified server for time synchronization. Then, 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 (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.

LSOD08206

- First found-in version: V3.02.00
- Condition: Configure an ACL rule to deny packets with the specified IP destination address.
- Description: The ARP packets whose target IP address is that specified IP address are dropped.

LSOD08070

- First found-in version: V3.02.00
- Condition: Configure “dot1x authentication-method eap” in system view. Configure "port-security port-mode mac-and-userlogin-secure" or "port-security port-mode mac-and-userlogin-secure-ext" on a port. Connect a PC to that port. The PC fails MAC authentication, but passes 802.1X authentication.
- Description: The PC can access the network. In fact, it must pass both authentication methods before it can access the network.

LSOD08123

- First found-in version: V3.02.00
- Condition: A VLAN interface receives a packet whose MAC address is its MAC address and whose IP address is not its IP address.
- Description: The device forwards that packet through software.

LSOD08049

- First found-in version: V3.02.00
- Condition: The device receives a packet whose destination MAC address is the broadcast address and whose destination IP address is a unicast IP address (the destination MAC is FF:FF:FF:FF:FF:FF; the destination IP address is not the IP address of the receiving VLAN interface).

- Description: The switch cannot send a redirect packet for that packet.

LSOD07871

pc1---SWA====SWB---pc2

- First found-in version: V3.02.00
- Condition: As shown in the above network, two switches are connected through a link aggregation group, and only two member ports are up. PC1 and PC2 ping each other. During the ping process, plug in and out the two member ports in turn to leave only one port being up at a time.
- Description: Other link-down ports learn the MAC address of PC1 or PC2, and communication between the PCs is broken for a long time.

LSOD06981

- First found-in version: V3.02.00
- 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.

LSOD07200

- First found-in version: V3.02.00
- Condition: A NEC 1XGate client passes 802.1X authentication on the device and gets online. Then, reboot the device.
- Description: After reboot, the client is shown on the device as an “unauthenticated user” and the device does not respond to the 802.1X authentication requests from the client.

LSOD07145

- First found-in version: V3.02.00
- 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.

LSOD07143

- First found-in version: V3.02.00
- Description: 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.

LSOD06680/LSOD07269

- First found-in version: V3.02.00
- 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: V3.02.00
- 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.

LSOD06906

- First found-in version: V3.02.00
- Condition: Configure 8 global ACLs and delete one of them. Then, configure global ACLs continuously until ACL resources become insufficient.
- Description: The item 'Remaining number' shown with the command **display acl remain entry** is '-16'.

TCD00877

- First found-in version: V3.02.00
- Condition: Configure 802.1X authentication on the device.
- Description: When the authentication method is EAP, authentication cannot succeed. When the authentication method is PAP or CHAP, authentication succeeds.

Resolved Problems in V3.02.00

None

Resolved Problems in V3.01.00p02

LSOD06047

- First found-in version: V3.01.00p01
- Condition: The switch runs IGMP snooping, and multiple multicast groups exist.
- Description: Some ports that have no multicast receivers connected are added to the multicast groups, which results in traffic congestion.

Resolved Problems in V3.01.00p01

LSOD04710

- First found-in version: V3.01.00
- Condition: The device uses FTP to download a configuration file whose name contains the unit number of the device.
- Description: It can not download the configuration file successfully.

LSOD04835

- First found-in version: V3.01.00
- Condition: Disable a port from forwarding Jumbo frames through the web interface.
- Description: The Jumbo frame forwarding state of the port is “enabled” on the details web page.

LSOD05192

- First found-in version: V3.01.00

- Condition: Backup the current configuration file through EMS (Enterprise Management Suite), and then upload the configuration file to the device by using FTP.
- Description: The configuration file can be uploaded to the device successfully. However, the device can not set the starting flag for the file.

Resolved Problems in V3.01.00

First release

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.

Traditionally, the loading of switch software is accomplished through the serial port. This approach is slow, inconvenient, and cannot be used for remote real-time loading. To resolve these problems, the TFTP and FTP modules are introduced into the switch. With these modules, the software and files can be loaded through an Ethernet port conveniently.

This chapter introduces how to load BootROM and host software into a switch locally and remotely.

Introduction to Loading Modes

You can load the software locally by using:

- XModem via the console port
- TFTP via an Ethernet port
- FTP via an Ethernet port

You can load the software remotely by using:

- FTP
- TFTP

Note

Make sure that the BootROM software version matches the host software version.

Local Software Loading

Before loading the software, make sure that the configuration terminal is correctly connected to the switch.

Note

The loading process of the BootROM software is the same as that of the host software, except that during the BootROM loading process, you should enter a different digit after entering the Boot Menu and the system gives somewhat different prompts. The following mainly describes the BootROM loading process.

Boot Menu

```
Starting......


          ************************************************************
          *                                                          *
          *         Switch 4200G 24-Port BOOTROM, Version 2.00       *
          *                                                          *
          ************************************************************

          Copyright (c) 2004-2006 3Com Corporation and its licensors.
          Creation date   : Nov 20 2007, 17:02:48
          CPU type        : BCM5836
          CPU Clock Speed : 200MHz
          BUS Clock Speed : 33MHz
          Memory Size     : 64MB
          Mac Address     : 0016e01f7a40


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

Press <Ctrl + B>. The system displays:

```
Password :
```

Note

To enter the Boot Menu, you should press <Ctrl+B> within five seconds after the information “Press Ctrl-B to enter Boot Menu...” appears. Otherwise, the system starts to decompress the program; and if you want to enter the Boot Menu at this time, you will have to restart the switch.

Input the correct BootROM password (by default, no password is set on the switch). The system enters the Boot Menu:

```
          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):
```

Loading Software Using XModem Through Console Port

Introduction to XModem

XModem is a file transfer protocol that is widely used due to its simplicity and good performance. XModem transfers files via the console port. It supports two types of data packets (128 bytes and 1 KB), two check methods (checksum and CRC), and an error packet retransmission mechanism (generally the maximum number of retransmission attempts is ten).

The XModem transmission procedure is completed by the cooperation of a receiving program and a sending program. The receiving program sends a negotiation packet to negotiate a packet check method. After the negotiation, the sending program starts to transmit data packets. When receiving a complete packet, the receiving program checks the packet using the agreed method. If the check succeeds, the receiving program sends an acknowledgement packet and the sending program proceeds to send another packet; otherwise, the receiving program sends a negative acknowledgement packet and the sending program retransmits the packet.

Loading BootROM software

Step 1: At the prompt "Enter your choice(0-9):" select 6 in the Boot Menu and then press <Enter> to enter the BootROM update menu shown below:

```
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 in the above menu to load the BootROM software using XModem. The system displays the following download baud rate setting menu:

```
Please select your download baudrate:
1.* 9600
2. 19200
3. 38400
4. 57600
5. 115200
0. Return
Enter your choice (0-5):
```

Step 3: Choose an appropriate download baud rate. For example, if you enter 5, the 115200 bps rate is chosen, and the system displays the following information:

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

Now, press <Enter>.

Note

If you have chosen 9600 bps, you do not need to modify the HyperTerminal's baud rate, and therefore you can skip Step 4 and 5 below and proceed to Step 6 directly. In this case, the system will not display the above information.

Step 4: Choose [File/Properties] in HyperTerminal, click <Configuration> in the popup dialog box, select the baud rate of 115200 bps in the appeared console port configuration dialog box.

Figure 1 Properties dialog box

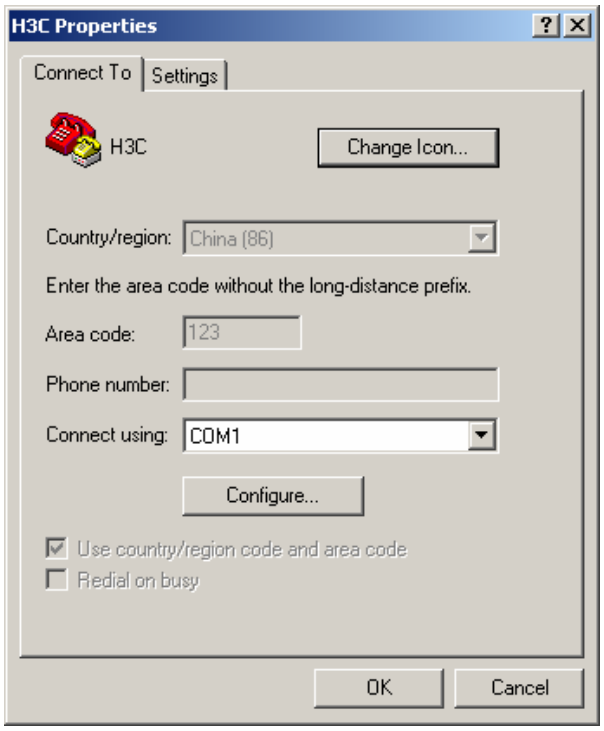
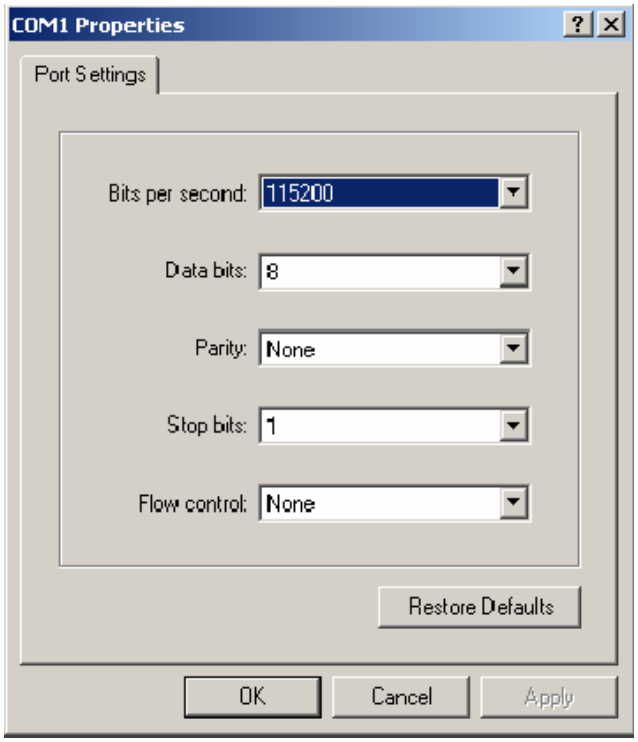
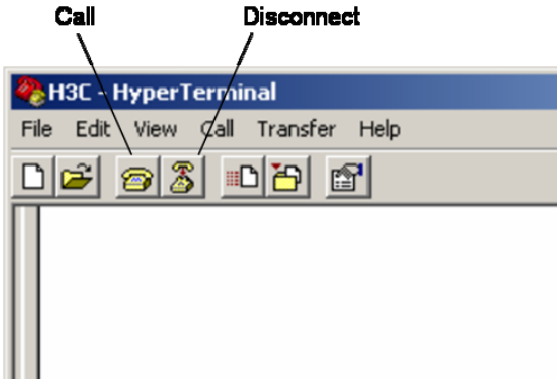


Figure 2 Console port configuration dialog box



Step 5: After setting the baud rate, you need to disconnect and then reconnect HyperTerminal so that the baud rate setting takes effect. Click the <Disconnect> button to disconnect the HyperTerminal from the switch and then click the <Call> button to reconnect the HyperTerminal to the switch.

Figure 3 Call and disconnect buttons



Note

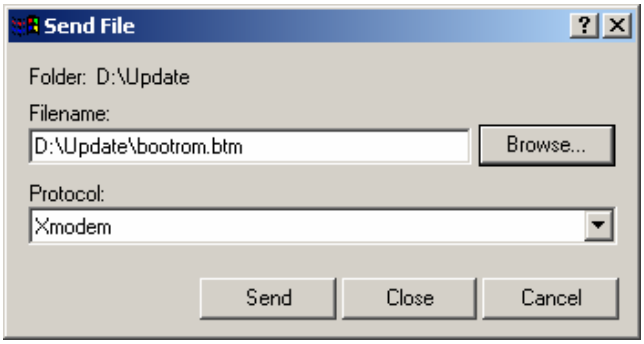
The new baud rate takes effect only after you disconnect and reconnect the terminal emulation program.

Step 6: Press <Enter> to start downloading the program. The system displays the following information:

```
Now please start transfer file with XMODEM protocol.
If you want to exit, Press <Ctrl+X>.
Loading ...CCCCCCCCCC
```

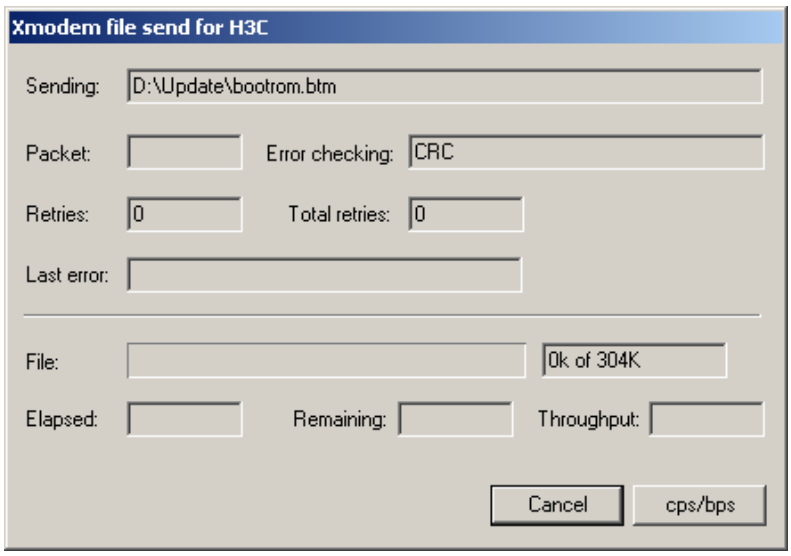
Step 7: Choose [Transfer/Send File] in the HyperTerminal's window, and in the following popup dialog box click <Browse>, select the software you need to send, and set the protocol to XModem.

Figure 4 Send file dialog box



Step 8: Click <Send>. The system displays the following page.

Figure 5 Send file page



Step 9: After the download completes, the system displays the following information:

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

Note

You do not need to reset the HyperTerminal's baud rate and can skip the last step if you have chosen 9600 bps. In this case, the system display the prompt "BootROM is updating now.....done!" instead of the prompt "Your baudrate should be set to 9600 bps again! Press enter key when ready".

Step 10: Reset HyperTerminal's baud rate to 9600 bps (refer to Step 4 and 5). Then, press any key as prompted. The system will display the following information when it completes the loading.

```
Bootrom updating.....................................done!
```

Loading host software

Step 1: Select 1 in Boot Menu. The system displays the following information:

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

To load the host software through XModem, select 3.

The subsequent steps are the same as those for loading the BootROM software, except that the system gives the prompt for host software loading instead of BootROM loading.

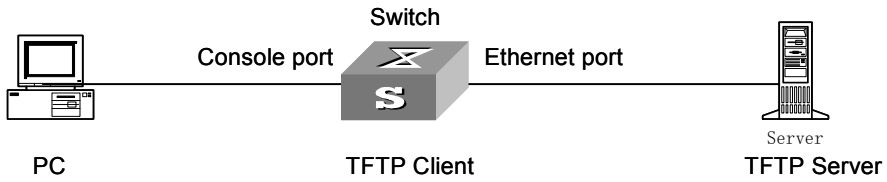
Loading Software Using TFTP through Ethernet Port

Introduction to TFTP

Trivial File Transfer Protocol (TFTP), a protocol in TCP/IP protocol suite, is used for trivial file transfer between client and server. It uses UDP to provide unreliable data stream transfer service.

Loading BootROM software

Figure 6 Local loading using TFTP



Step 1: As shown in Figure 6, connect the switch through an Ethernet port to the TFTP server, and connect the switch through the console port to the configuration PC.

Note

You can use one PC as both the configuration terminal and TFTP server.

Step 2: Run the TFTP server program on the TFTP server, and specify the path of the program to be loaded.

Caution

The TFTP server program is not provided with the H3C series switches.

Step 3: Run the terminal emulation program on the configuration PC, and start the switch to enter the Boot Menu. At the prompt "Enter your choice(0-9):" select 6 in the Boot Menu and then press <Enter> to enter the BootROM update menu shown below:

```
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 4: Select 1 to download the BootROM software using TFTP. Then set the following TFTP-related parameters as required:

```
Load File name           :Bootrom.btm
Switch IP address        :1.1.1.2
Server IP address        :1.1.1.1
```

Step 5: Press <Enter>. The system displays the following information:

```
Are you sure to update your bootrom?Yes or No(Y/N)
```

Step 6: Enter Y to start file downloading or N to return to the Bootrom update menu. If you enter Y, the system begins to download and update the BootROM software. Upon completion, the system displays the following information:

```
Loading.....................................done
Bootrom updating.........done!
```

Loading host software

Step 1: Select 1 in Boot Menu. The system displays the following information:

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

To load the host software through TFTP, select 1.

The subsequent steps are the same as those for loading the BootROM software, except that the system gives the prompt for host software loading instead of BootROM loading.

Loading Software Using FTP through Ethernet Port

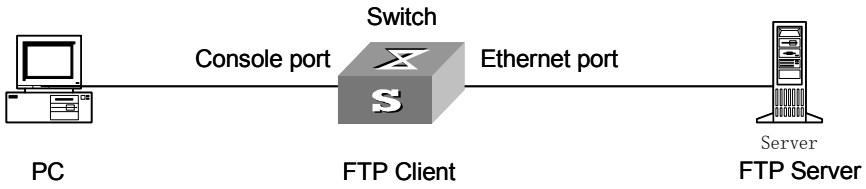
Introduction to FTP

The File Transfer Protocol (FTP) is an application-layer protocol in the TCP/IP protocol suite. It is used for transferring files between server and client, and is widely used in IP networks.

You can use FTP to load software onto the switch through an Ethernet port. In this case, the switch can act as an FTP server or an FTP client. In the following example, the switch acts as an FTP client.

Loading BootROM software

Figure 7 Local loading using FTP



Step 1: As shown in Figure 7, connect the switch through an Ethernet port to the TFTP server, and connect the switch through the console port to the configuration PC.

Note

You can use one PC as both the configuration terminal and FTP server.

Step 2: Run the FTP server program on the FTP server, configure an FTP user name and password, and specify the path of the program to be downloaded.

Step 3: Run the terminal emulation program on the configuration PC, and start the switch to enter the Boot Menu.

At the prompt "Enter your choice(0-9):" select 6 in the Boot Menu, and then press <Enter> to enter the BootROM update menu shown below:

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 4: Enter 2 in the above menu to download the BootROM software using FTP. Then set the following FTP-related parameters as required:

```
Load File name          :Bootrom.btm
Switch IP address       :10.1.1.2
Server IP address       : 1.1.1.1
FTP User Name           :4200
FTP User Password       :abc
```

Step 5: Press <Enter>. The system displays the following information:

```
Are you sure to update your bootrom?Yes or No(Y/N)
```

Step 6: Enter Y to start file downloading or N to return to the Bootrom update menu. If you enter Y, the system begins to download and update the program. Upon completion, the system displays the following information:

```
Loading.....................................done
Bootrom updating.........done!
```

Loading host software

Step 1: Select 1 in Boot Menu. The system displays the following information:

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

To load the host software through FTP, select 2.

The subsequent steps are the same as those for loading the BootROM software, except that the system gives the prompt for host software loading instead of BootROM loading.

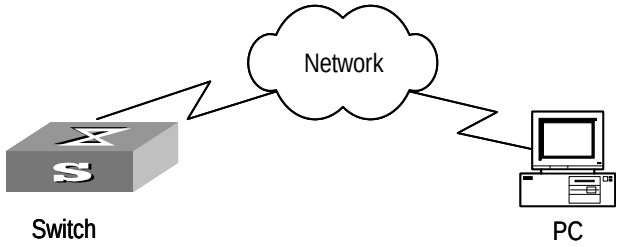
Remote Software Loading

If your terminal is indirectly connected to the switch through the Internet, you can telnet to the switch, and use FTP or TFTP to load BootROM and host software remotely.

Remote Loading Using FTP

As shown in Figure 8, a PC is used as both the configuration terminal and FTP server. You can telnet to the switch, and then execute the FTP commands to download the host software program 4200G.app and the BootROM program Bootrom.btm from the remote FTP server (with IP address 1.1.1.1) to the switch.

Figure 8 Remote loading using FTP



Step 1: Download the software to the switch using FTP commands.

```
<H3C> ftp 1.1.1.1
Trying ...
Press CTRL+K to abort
Connected.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
```

```
User(none):abc
331 Give me your password, please
Password:
230 Logged in successfully
[ftp] get 4200G.app
[ftp] get Bootrom.btm
[ftp] bye
```

Step 2: Update the BootROM program on the switch.

```
<H3C> boot bootrom 4200G.app
please wait ...
Bootrom is updated!
```

Step 3: Update the host software on the switch.

```
<H3C> boot boot-loader 4200G.app
<H3C> display boot-loader
Unit 1:
   The current boot app is: 4200G.app
   The main boot app is:    4200G.app
   The backup boot app is:
```

Step 4: Restart the switch.

```
<H3C> reboot
```

Note

Before restarting the switch, make sure other configurations are all saved to avoid the loss of configuration information.

After the steps above, the BootROM and host software loading is completed.

Note that:

- Host software loading takes effect only after you restart the switch with the **reboot** command.
- If the space of the flash memory is not enough, you can delete the useless files in the flash memory before software downloading.
- Power interruption is not allowed during software loading.

Remote Loading Using TFTP

The remote loading by using TFTP is similar to the remote loading by using FTP. The only difference is that the switch can only be used as a TFTP client.