Switch Management and Maintenance

XXXX Communication Technology Co., Ltd

Tel: (86)

Fax: (86)

URL:

Email:

XXXX values and appreciates comments you may have concerning our products or this document. Please address comments to:

XXXX Communication Technology Co., Ltd
Tel:
Fax:
URL:
Email:

Contents

Chapter 1 Configuration File Management

1.1 Introduction to Configuration File

Configuration file records and stores user configurations performed to a switch. It also enables users to check switch configurations easily.

Upon powered on, a switch loads the configuration file known as saved-configuration file, which resides in the Flash, for initialization. If the Flash contains no configuration file, the system initializes using the default settings. Comparing to saved-configuration file, the configuration file which is currently adopted by a switch is known as the current-configuration.

A configuration file conforms to the following conventions:

The content of a configuration files is a series of commands.

Only the non-default configuration parameters are saved.

The commands are grouped into sections by command configuration mode. The commands that are of the same configuration mode are grouped into one section. Sections are separated by empty lines or comment lines. (A line is a comment line if it starts with the character “!”.)

The sections are listed in this order: system configuration section, physical port configuration section, logical interface configuration section, routing protocol configuration section, and so on.

A configuration file ends with an “exit”.

1.2 Configuration File-Related Operations

You can perform the following operations on the switch:

Modify uploaded configuration file. The configuration file is in the form of text, which can be uploaded to the PC through FTP and TFTP. Please use text tools (such as windows notepad) to edit the uploaded configuration file.

Modify and save the current configuration to a configuration file.

Removing a configuration file from the Flash;

Execute saved configuration file;

Checking/Setting the configuration file to be used when the switch starts the next time;

Setting a configuration file to be the primary configuration file;

Change the executing mode of configuration file.

Perform the following configuration in privileged configuration mode.

Figure 1-1 Configure a configuration file

Operation	Command	Description
Save current operation	copy running-config startup-config	The saved configuration will be the start-up configuration of the next rebooting.
Clear saved configurations	clear startup-config	If the saved configuration is cleared, the system will restore to factory setting after rebooting.
Execute saved configuration	copy startup-config running-config	Configuration file is executed in global configuration mode by default. Enter global configuration mode first by using **configure terminal** in privilege mode. Prompts for not executable command during execution: [Line:xxxx]invalid: %s——Cannot execute. [Line:xxxx]failed: %s——Execution failed. [Line:xxxx]failed: too long command: %s——Not execute command which is beyond 512 characters. "xxxx" means the line number of the command. "%s" means command characters. Not executable command includes commands with grammar error and unmatched mode.
Show saved configuration	show startup-config [*module-list*]	
Show current configuration	show running-config [*module-list*]	
Execute mode of configuration files	**buildrun mode** {stop | continue}	Stop means configuration file executing would be stopped and the error will show if there is an error. Continue means configuration file executing would not be stopped and the error will show if there is an error.

Note:

Currently, the extension of a configuration file is bin. Configuration files are saved in the root directory of the Flash.

In the following conditions, it may be necessary for you to remove the configuration files from the Flash:

The system software does not match the configuration file after the software of the Ethernet switch is updated.

The configuration files in the Flash are damaged. The common reason is that wrong configuration files are loaded.

Chapter 2 BootROM and Host Software Loading

Traditionally, the loading of switch software is accomplished through a serial port. This approach is slow, inconvenient, and cannot be used for remote loading. To resolve these problems, the TFTP and FTP modules are introduced into the switch. With these modules, you can load/download software/files conveniently to the switch through an Ethernet port.

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

2.1 Introduction to Loading Approaches

You can load software locally by using:

XMODEM through Console port

TFTP through Ethernet port

FTP through Ethernet port

You can load software remotely by using:

FTP

TFTP

Note:

The BootROM software version should be compatible with the host software version when you load the BootROM and host software.

2.2 Local Software Loading

If your terminal is directly connected to the switch, you can load the BootROM and host software locally.

Before loading the software, make sure that your terminal is correctly connected to the switch to insure successful loading.

Note:

The loading process of the BootROM software is the same as that of the host software, except that during the former process, the system gives different prompts. The following text mainly describes the BootROM loading process.

2.2.1 Loading Software Using XMODEM through Console Port

I. Introduction to XMODEM

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

The XMODEM transmission procedure is completed by a receiving program and a sending program: The receiving program sends negotiation characters to negotiate a packet checking 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 character and the sending program proceeds to send another packet; otherwise, the receiving program sends a negative acknowledgement character and the sending program retransmits the packet.

II. Loading BootROM software

The following text mainly describes the BootROM loading process. Follow these steps to load the BootROM software:

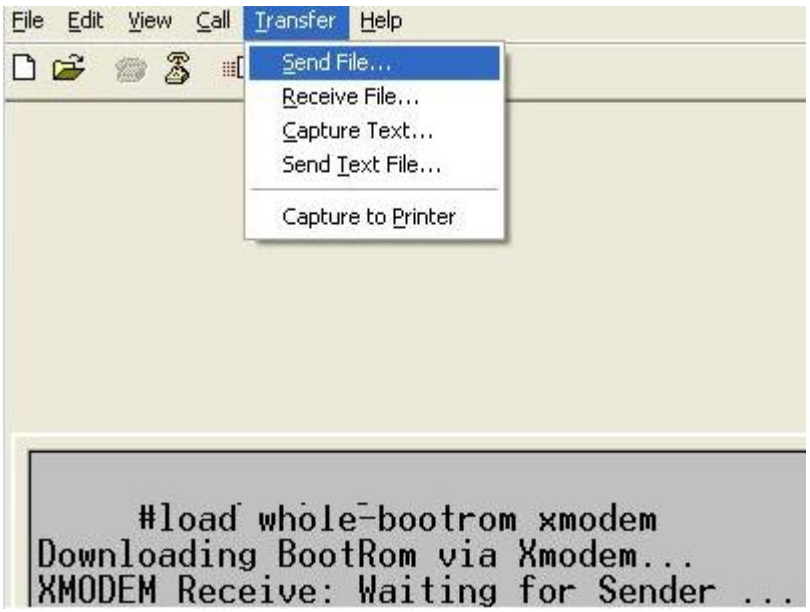
Step 1: enter following command in privileged mode:

Switch#load whole-bootrom xmodem

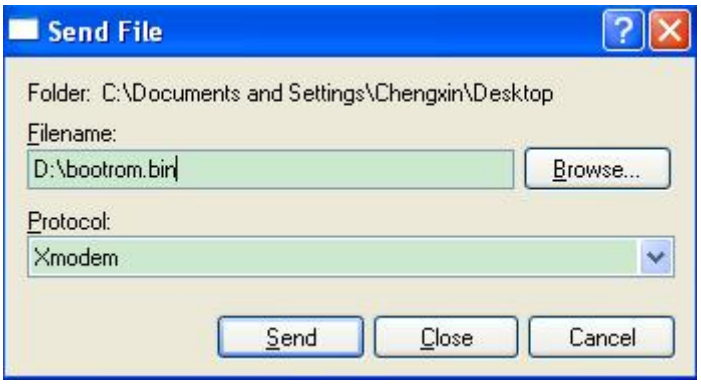
Downloading BootRom via Xmodem...

XMODEM Receive: Waiting for Sender ...

Step 2: Choose [Transfer/Send File] in the HyperTerminal's window, as shown in Picture 1-1, and click <Browse> in pop-up dialog box. Select the software you need to download, and set the protocol to XMODEM, as shown in Picture 1-2.

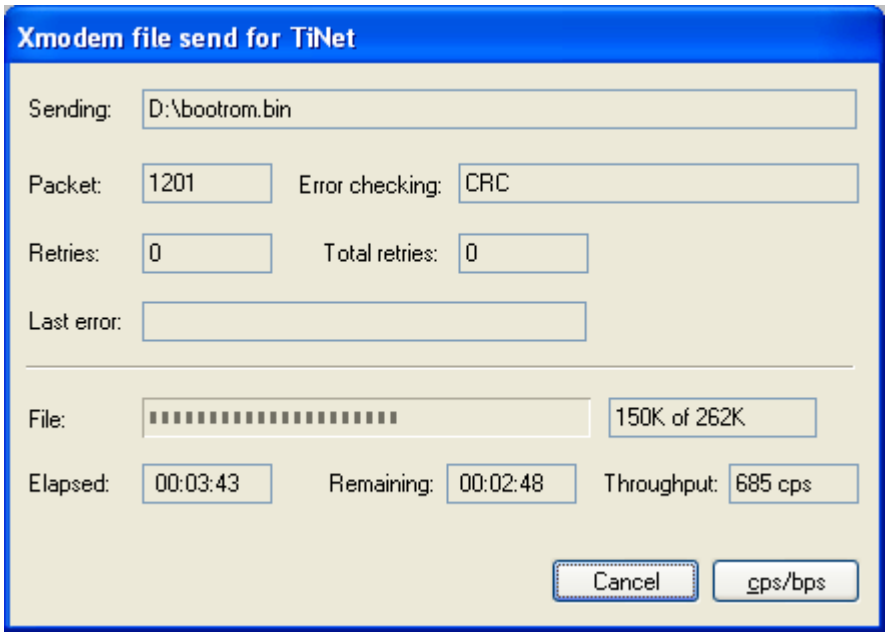


Picture 1-1 Choose [Transfer/Send File]



Picture 1-2 Send file dialog box

Step 3: Click <Send>. The system displays the page, as shown in Figure 1-3.



Picture 1-3 Sending file page

Step 4: After the download completes, the system displays the following information:

Download wholeBootRom successfully.

Update BootRom successfully.

Download BootRom via Xmodem successfully.

III. Loading host software

Follow these steps to load the host software:

Step 1: Enter following command in privileged mode:

Switch#load application xmodem

Downloading application via Xmodem...

XMODEM Receive: Waiting for Sender ...

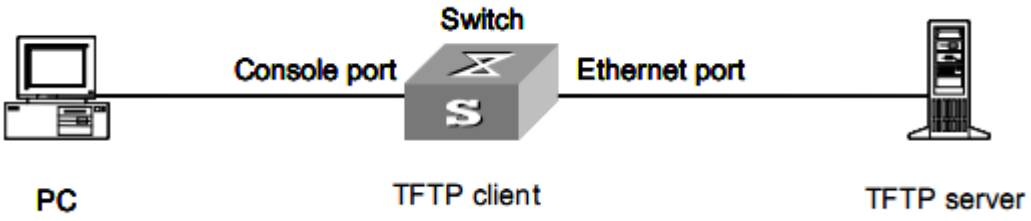
The subsequent steps are the same as those for loading the BootROM software, except that the system gives the prompt for host software loading instead of BootROM loading.

2.2.2 Loading Software Using TFTP through Ethernet Port

I. Introduction to TFTP

TFTP, one 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.

II. Loading BootROM software



Picture 1-4 Local loading using TFTP

Step 1: As shown in Picture 1-4, 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 device and the TFTP server.

Step2: Run the TFTP server program on the TFTP server, and specify the path of the program to be downloaded.

Caution:

TFTP server program is not provided with the Switch Series Ethernet Switches.

Step 3: Run the HyperTerminal program on the configuration PC. Start the switch. Then enter the privileged mode. Then set the following TFTP-related parameters as required:

Switch#**load whole-bootrom tftp** *tftpserver-ip filename*

Caution:

Load File name: bootrom.bin

Switch IP address: A.B.C.D

Server IP address: A.B.C.E

Step 4: Press <Enter>. The system displays the following information:

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

Step 5: 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:

Download wholeBootRom successfully.

Update BootRom successfully.

Download BootRom via TFTP successfully.

III. Loading host software

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

Caution:

When loading BootROM and host software using TFTP, you are recommended to use the PC directly connected to the device as TFTP server to promote upgrading reliability.

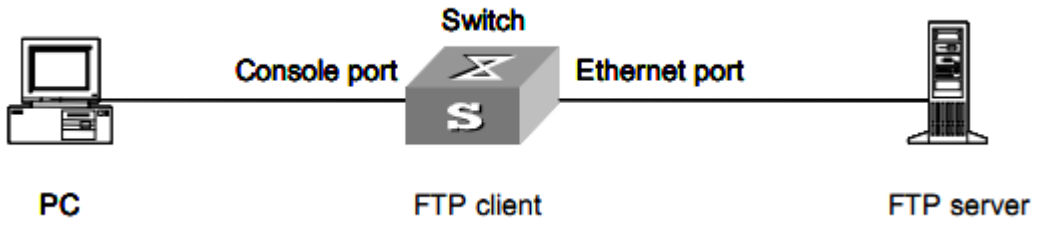
2.2.3 Loading Software Using FTP through Ethernet Port

I. Introduction to FTP

FTP is an application-layer protocol in the TCP/IP protocol suite. It is used for file transfer between server and client, and is widely used in IP networks.

You can use the switch as an FTP client or a server, and download software to the switch through an Ethernet port. The following is an example.

II. Loading BootROM software



Picture 1-5 Local loading using FTP client

Step 1: As shown in Figure 1-5, connect the switch through an Ethernet port to the FTP server, and connect the switch through the Console port to the configuration PC.

Note:

You can use one computer as both configuration device and FTP server.

Step 2: Run the FTP server program on the FTP server, configure an FTP user name and password, and copy the program file to the specified FTP directory.

Step 3: Run the HyperTerminal program on the configuration PC. Start the switch. Then enter the privileged mode. Then set the following FTP-related parameters as required:

Switch#**load whole-bootrom ftp** *ftpserver-ip filename ftp-username user-password*

Caution:

Load File name: bootrom.bin

Switch IP address: A.B.C.D

Server IP address: A.B.C.E

Step 4: Press <Enter>. The system displays the following information:

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

Step 5: 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:

Download wholeBootRom successfully.

Update BootRom successfully.

Download BootRom via FTP successfully.

III. Loading host software

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

Caution:

When loading BootROM and host software using FTP, you are recommended to use the PC directly connected to the device as FTP server to promote upgrading reliability.

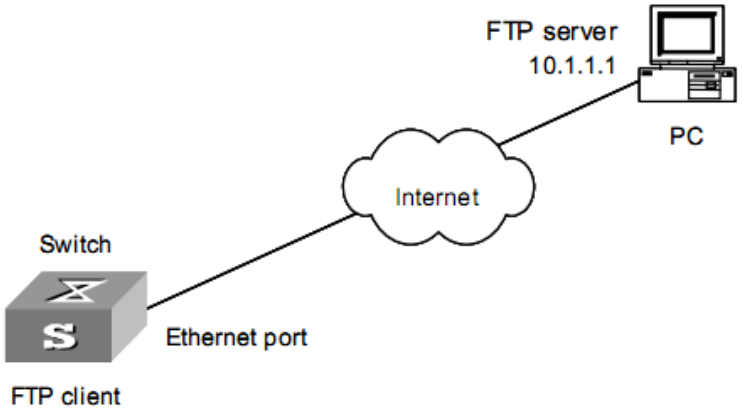
2.3 Remote Software Loading

If your terminal is not directly connected to the switch, you can telnet to the switch, and use FTP or TFTP to load BootROM and host software remotely.

2.3.1 Remote Loading Using FTP

I. Loading BootROM

As shown in Picture 1-6, a PC is used as both the configuration device and the FTP server. You can telnet to the switch, and then execute the FTP commands to download the BootROM program bootrom.bin from the remote FTP server (with an IP address 10.1.1.1) to the switch.



Picture 1-6 Remote loading using FTP

Step 1: Open FTP software and set host IP address to be 10.1.1.1. Set the username and password;

Note:

When using different FTP server software on PC, different information will be output to the switch.

The subsequent steps are the same as those for 1.1.4 Loading BootROM software. Make sure the PC can ping the switch.

2.3.2 Remote Loading Using TFTP

The remote loading using TFTP is similar to that using FTP.

Chapter 3 Basic System Configuration & Debugging

This section includes:

3.1 Basic System Configuration

Perform following commands in global configuration mode.

Table 1-1 Basic system configuration tasks

Operation	Command	Description
Configure the host name of the device.	**hostname** *hostname*	By default, the hostname is Switch.
Configure system time zone	**clock timezone** name hour minute	By default, it is the UTC time zone.
enter the privileged mode. Configure system clock	**clock set** HH:MM:SS YYYY/MM/DD	By default, it is 00:00:00 01/01/2001 when the system starts up.

3.2 SNMP

3.2.1 SNMP Overview

By far, the simple network management protocol (SNMP) has gained the most extensive application in the computer networks. SNMP has been put into use and widely accepted as an industry standard in practice. It is used for ensuring the transmission of the management information between any two nodes. In this way, network administrators can easily search and modify the information on any node on the network. In the meantime, they can locate faults promptly and implement the fault diagnosis, capacity planning and report generating.

SNMP adopts the polling mechanism and provides the most basic function set. It is most applicable to the small-sized, fast-speed and low-cost environment. It only requires the connectionless transport layer protocol UDP; and is thus widely supported by many products.

I. SNMP Operation Mechanism

SNMP can be divided into two parts, namely, Network Management Station and Agent: Network management station (NMS) is the workstation for running the client program. At present, the commonly used NMS platforms include QuidView, Sun NetManager and IBM NetView.

Agent is the server software operated on network devices.

The NMS can send GetRequest, GetNextRequest and SetRequest messages to the Agent. Upon receiving the requests from the NMS, Agent will perform Read or Write operation according to the message types, generate and return the Response message to the NMS.

Agent will send Trap message on its own initiative to the NMS to report the events whenever the device status changes or the device encounters any abnormalities such as restarting the device.

II. SNMP Versions

Currently SNMP Agent of the device supports SNMP V3, and is compatible with SNMP V1 and SNMP V2C.

SNMP V3 adopts user name and password authentication.

SNMP V1 and SNMP V2C adopt community name authentication. The SNMP packets failing to pass community name authentication are discarded. The community name is used to define the relation between SNMP NMS and SNMP Agent. The community name can limit access to SNMP Agent from SNMP NMS, functioning as a password.

You can define the following features related to the community name.

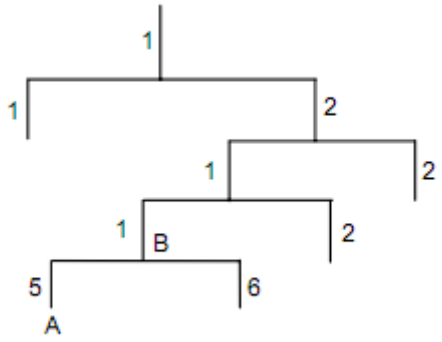
Define MIB view that a community can access.

Set read-only or read-write right to access MIB objects for the community. The read-only community can only query device information, while the read-write community can configure the device.

Set the basic ACL specified by the community name.

III. MIBs Supported by the Device

The management variable in the SNMP packet is used to describe management objects of a device. To uniquely identify the management objects of the device in SNMP messages, SNMP adopts the hierarchical naming scheme to identify the managed objects. It is like a tree, and each tree node represents a managed object, as shown in Picture 1-7. Thus the object can be identified with the unique path starting from the root.



Picture 1-7 Architecture of the MIB tree

The management information base (MIB) is used to describe the hierarchical architecture of the tree and it is the set defined by the standard variables of the monitored network device. In the above figure, the managed object B can be uniquely specified by a string of numbers {1.2.1.1}. The number string is the Object Identifier of the managed object.

3.2.2 Configuring SNMP Basic Functions

Perform following commands in global configuration mode.

Table 1-x Configuring SNMP Basic Functions

Operation	Command	Description
Configure community name and some other info	**snmp-server community** *community* { **ro | rw } { deny | permit** } [**view** *view-name*]	
Configure system administrator's contact	**snmp-server contact** *syscontact*	If there is space in the *syscontact* keywords, it should be quoted by quotation mark.
Enable destination host address	**snmp-server host** *host-addr* [**version** {**1** | **2c** | **3** [**auth** | **noauthpriv** | **priv**]}] *community-string* [**udp-port** *port*] [**notify-type** [*notifytype-list*]]	The community name in **snmp-server host version** should not be empty.
Configure system location	**snmp-server location** *syslocation*	By default, the *syslocation* is"sample sysLocation factory default" If there is space in the keywords, it should be quoted by quotation mark.
Configure system name	**snmp-server name** *sysname*	By default, the *sysname* is "Switch " If there is space in the keywords, it should be quoted by quotation mark.

Enable SNMP server to send notification	**snmp-server enable traps** [*notificationtype-list*]	The default notification type is trap, and it is defaulted to be disabled.
Configure local engine id or remote engine id.	**snmp-server engineid** { **local** engineid-string **| remote** ip-address [**udp-port** port-number] engineid-string }	By default, the device local engine ID is 134640000000000000000000. The local engine cannot be deleted and at most 32 remote engines can be configured.
Configure view	**snmp-server view** *view-name oid-tree* { included | excluded }	There are three default views: iso, internet and sysview. At most 64 views can be configured. The character number of the view-name plus the number of OID nodes is not more than 62.
Configure access control group	**snmp-server group** *groupname* { **1** | **2c** | **3** [**auth** | **noauthpriv** | **priv**] [**context** context-name]} [**read** *readview*] [**write** writeview] [**notify** notifyview]	There are two defaulted groups:(1)security model is v3 and security level is initial (2) security model is v3 initial At most 64 groups can be configured.
Configure user in snmpv3	**snmp-server user** *username groupname* **[remote** *ipaddress* **[udp-port** *port-number***]] [auth { md5 | sha } { auth-password** *authpassword* **| auth-key** *authkey* **} [priv des priv-key { auth-key** *privkey* **| auth-password** *privpassword* **}]]**	There are three default users: (1)initialmd5 (HMACMD5AuthProtocol), (2) initialsha (HMACSHAAuthProtocol), (3) initialnone (NoauthProtocol) At most 64 users can be configured.

3.2.3 Displaying SNMP

After the above configuration is completed, execute the display command in any mode to view the running status of SNMP, and to verify the configuration.

Table 1-3 Display SNMP

Operation	Command	Description
Display the currently configured community name	show snmp community	
Display system administrator's contact	show snmp contact	
Display Trap list information	show snmp host	
Display all notification status	show snmp notify	
Display system location	show snmp location	

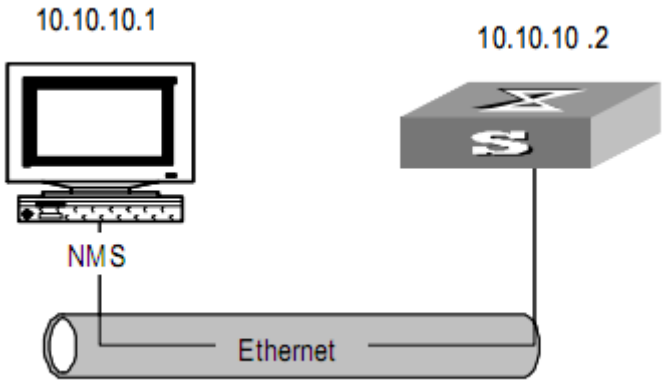
Display the engine ID of the current device	show snmp engineid [*local* | *remote*]	*local* means to show local engine and *remote* means to show recognizable remote engine.
Display group information about the device	show snmp group	
Display SNMP user information	show snmp user	
Display the currently configured view	show snmp view	

3.2.4 SNMP Configuration Example

I. Network requirements

An NMS and Switch A are connected through the Ethernet. The IP address of the NMS is 10.10.10.1 and that of the VLAN interface on Switch A is 10.10.10.2.
Perform the following configuration on Switch A: setting the community name and access authority, administrator ID, contact and switch location, and enabling the switch to sent trap packet.

II. Network diagram



Picture 1-8 Network diagram for SNMP

III. Network procedure

! Set the community name, group name and user.
Switch(config)# snmp-server community XXXX ro permit
Switch(config)# snmp-server group grp1 1 read internet write internet notify Internet
Switch(config)# snmp-server user user1 grp1
! Enable the SNMP agent to send Trap packets to the NMS whose IP address is 10.10.10.1. The SNMP community is XXXX.
Switch(config)#snmp-server host 1.1.1.2 version 3 auth 1 notify-type interfaces

3.3 Network Connectivity Test

3.3.1 Ping

You can use the ping command to check the network connectivity and the reachability of a host.

Table 1-2 The ping command

Operation	Command
Check the IP network connectivity and the reachability of a host	**ping** [**-i** *ttl value*] [**-l** *packet length*] [**-n** *ping packet number*] [**-s** *source IP*] [**-t** *time out*] *A.B.C.D* *ip address with A.B.C.D*

This command can output the following results:
Response status for each ping packet. If no response packet is received within the timeout time, the message "Request time out" is displayed. Otherwise, the number of data bytes, packet serial number, TTL (time to live) and response time of the response packet are displayed.
Final statistics, including the numbers of sent packets and received response packets, the irresponsive packet percentage, and the minimum, average and maximum values of response time.

3.3.2 Tracert

You can use the **tracert** command to trace the gateways a packet passes during its journey from the source to the destination. This command is mainly used to check the network connectivity. It can help you locate the trouble spot of the network.

The executing procedure of the **tracert** command is as follows: First, the source host sends a data packet with the TTL of 1, and the first hop device returns an ICMP error message indicating that it cannot forward this packet because of TTL timeout. Then, the source host resends the packet with the TTL of 2, and the second hop device also returns an ICMP TTL timeout message. This procedure goes on and on until the packet gets to the destination. During the procedure, the system records the source address of each ICMP TTL timeout message in order to offer the path that the packet passed through to the destination.

Table 1-8 The tracert command

Operation	Command
Trace the gateways a packet passes from the source host to the destination	**tracert** [**-u** | **-c**] | **-f** *first_ttl* | **-h** *maximum_hops* | **-w** *time_out*] *target_name*

3.4 Device Management

3.4.1 System IP Address configuration

IP address is the Internet Protocol address, the IP Address abbreviation. IP address is a uniform address format IP protocol provides, it is assigned a logical address for each network on the Internet and each host in order to mask the differences between the physical address

For Layer 2 device globally configure the system to automatically obtain an IP address or IP

Table 1-9 System IP address configuration tasks

操作	命令	备注
Enter the global configuration mode	**configure terminal**	
Get IP by Bootp protocol	**bootp**	optional
Get IP by DHCP protocol	**dhcp**	optional
Manually configure the IP and vlan	**ipaddress** ***{****ip-addr netmark gateway****|vlan*** *vlan-id****}***	optional
Display Manage IP and VLAN	**show ip**	-

3.4.2 MAC address Table management

I. Overview

1) Introduction to MAC Address Learning

An Ethernet switch maintains a MAC address table to forward packets quickly. A MAC address table is a port-based Layer 2 address table. It is the base for Ethernet switch to perform Layer 2 packet forwarding. Each entry in a MAC address table contains the following fields:

- Destination MAC address
- ID of the VLAN which a port belongs to
- Forwarding port number

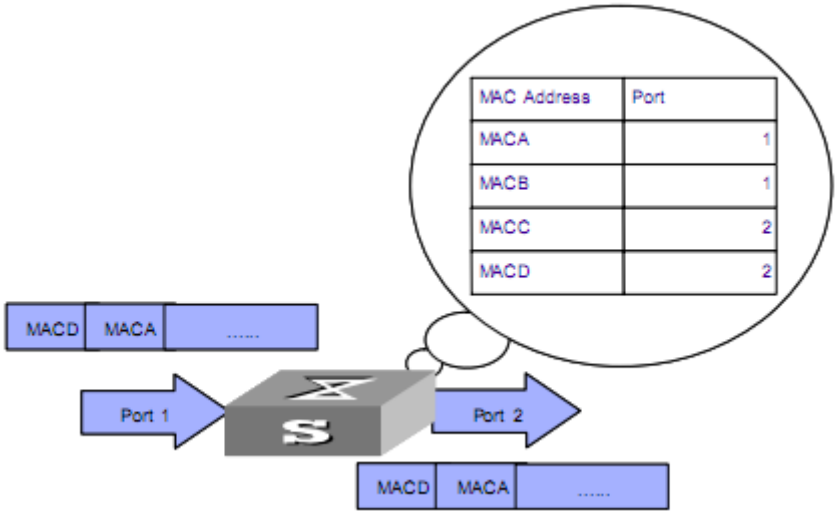
Upon receiving a packet, a switch queries its MAC address table for the forwarding port number according to the destination MAC address carried in the packet and then forwards the packet through the port.

The dynamic address entries (not configured manually) in the MAC address table are learned by the Ethernet switch. When an Ethernet switch learns a MAC address, the following occurs:

When a switch receives a packet from one of its ports (referred to as Port 1), the switch extracts the source MAC address (referred to as MAC-SOURCE) of the packet and considers that the packets destined for MAC-SOURCE can be forwarded through Port 1.

➢ If the MAC address table already contains MAC-SOURCE, the switch updates the corresponding MAC address entry.

➢ If MAC-SOURCE does not exist in the MAC address table, the switch adds MAC-SOURCE and Port 1 as a new MAC address entry to the MAC address table.



Picture 1-x A switch uses a MAC address table to forward packets.

After learning the source address of the packet, the switch searches the MAC address table for the destination MAC address of the received packet:

➢ If it finds a match, it directly forwards the packet.

➢ If it finds no match, it forwards the packet to all ports, except the receiving port, within the VLAN to which the receiving port belongs. Normally, this is referred to as broadcasting the packet.

After the packet is broadcast:

➢ If the network device returns a packet to the switch, this indicates the packet has been sent to the destination device. The MAC address of the device is carried in the packet. The switch adds the new MAC address to the MAC address table through address learning. After that, the switch can directly forward other packets destined for the same network device by using the newly added MAC address entry.

➢ If the destination device does not respond to the packet, this indicates that the destination device is unreachable or that the destination device receives the packet but gives no response. In this case, the switch still cannot learn the MAC address of the destination device. Therefore, the switch will still broadcast any other packet with this destination MAC address.

To fully utilize a MAC address table, which has a limited capacity, the switch uses an aging mechanism for updating the table. That is, the switch removes the MAC address entries related to a network device if no packet is received from the device within the aging time. Aging time only applies to dynamic MAC address entries.

You can manually configure (add or modify) a static or dynamic MAC address entry based on the actual network environment.

Note:

The switch learns only unicast addresses by using the MAC address learning mechanism but directly drops any packet with a broadcast source MAC address.

2) Entries in a MAC Address Table

Entries in a MAC address table fall into the following categories according to their characteristics and configuration methods:

- Static MAC address entry: This type of MAC address entries are added/removed manually and cannot age out by themselves. Using static MAC address entries can reduce broadcast packets remarkably and are suitable for networks where network devices seldom change, but it will be lost after reboot if the configuration is saved.
- Dynamic MAC address entry: This type of MAC address entries age out after the configured aging time. They are generated by the MAC address learning mechanism or configured manually.
- Blackhole MAC address entry: This type of MAC address entries are configured manually. A switch discards the packets destined for or originated from the MAC addresses contained in blackhole MAC address entries
- Permanent MAC address entry: This type of MAC address entries own the same features as the static MAC address entries, but it will be reserved at reboot if the configuration is saved.

Table 1-x lists the different types of MAC address entries and their characteristics.

MAC address entry	Configuration method	Aging time	Reserved or not at reboot (if the configuration is saved)
Static MAC address entry	Manually configured	Unavailable	No
Dynamic MAC address entry	Manually configured or generated by MAC address learning mechanism	Available	No
Blackhole MAC address entry	Manually configured	Unavailable	Reserved
Permanent MAC address entry	Manually configured	Unavailable	Reserved

II. Configuring MAC Address Table Management

1) Configuring a MAC Address Entry

You can add, modify, or remove one MAC address entry, remove all MAC address entries (unicast MAC addresses only) concerning a specific port, or remove specific type of MAC address entries (dynamic or static MAC address entries).

You can add a MAC address entry in global configuration mode or interface configuration mode.

Perform following commands in global configuration mode.

Table 1-x Add a MAC address entry

Operation	Command	Description
Add a MAC address entry	**mac-address-table** { static | permanent | dynamic } *mac* **interface** *interface-num* **vlan** *vlan-id*	This command for adding static/permanent/dynamic mac address entry.
	mac-address-table blackhole *mac* **vlan** *vlan-id*	This command is only for adding blackhole mac address entry.

Caution:

When you add a MAC address entry, the port specified by the interface argument must belong to the VLAN specified by the vlan argument in the command. Otherwise, the entry will not be added.

2) Setting the Aging Time of MAC Address Entries

Setting aging time properly helps implement effective MAC address aging. The aging time that is too long or too short results in a large amount of broadcast packets wandering across the network and decreases the performance of the switch.

➢ If the aging time is too long, excessive invalid MAC address entries maintained by the switch may fill up the MAC address table. This prevents the MAC address table from varying with network changes in time.

➢ If the aging time is too short, the switch may remove valid MAC address entries. This decreases the forwarding performance of the switch.

Table 1-x Set aging time of MAC address entries

Operation	Command	Description
Set the aging time of MAC address entries	**mac-address-table age-time** [*agetime* | disable]	The default aging time is 300 seconds.

This command is used in global configuration mode and applies to all ports. Aging applies to only dynamic MAC addresses that are learnt or configured to age.
Normally, you are recommended to use the default aging time, namely, 300 seconds. The no-aging keyword specifies that MAC address entries do not age out.

3) Setting the Maximum Number of MAC Addresses a Port Can Learn

The MAC address learning mechanism enables an Ethernet switch to acquire the

MAC addresses of the network devices on the segment connected to the ports of the switch. The switch directly forwards the packets destined for these MAC addresses. A MAC address table too big in size may decrease the forwarding performance of the switch.

By setting the maximum number of MAC addresses that can be learnt from individual ports, you can control the number of the MAC address entries the MAC address table can dynamically maintains. When the number of the MAC address entries learnt from a port reaches the set value, the port stops learning MAC addresses.

Perform following commands in interface configuration mode.

Table 1-x Set the maximum number of MAC addresses a port can learn

Operation	Command	Description
Enable MAC addresses table learning	**mac-address-table learning**	This command can be used in both global configuration mode and interface configuration mode. By default, this function is enabled.
Set the maximum number of MAC addresses the port can learn	**mac-address-table max-mac-count** *max-mac-count*	By default, the number of the MAC addresses a port can learn is not limited.

III. Displaying and Maintaining MAC Address Table Configuration

To verify your configuration, you can display information about the MAC address table by executing the display command in any mode.

Table 1-x Display and maintain MAC address table configuration

Operation	Command
Display information about the MAC address table	**show mac-address-table** **show mac-address-table** { *interface-num* [**vlan** *vlan-id*] | **cpu** } **show mac-address-table** *mac* [**vlan** *vlan-id*] **show mac-address-table** { static | dynamic | permanent | blackhole } [**vlan** *vlan-id*] **show mac-address-table** { static |dynamic | permanent | blackhole } **interface** *interface-num* [**vlan** *vlan-id*] **show mac-address-table vlan** *vlan-id*
Display the aging time of the dynamic MAC address entries in the MAC address table	**show mac-address-table age-time**
Display MAC addresses table learning status	**show mac-address-table learning**

IV. Configuration Example

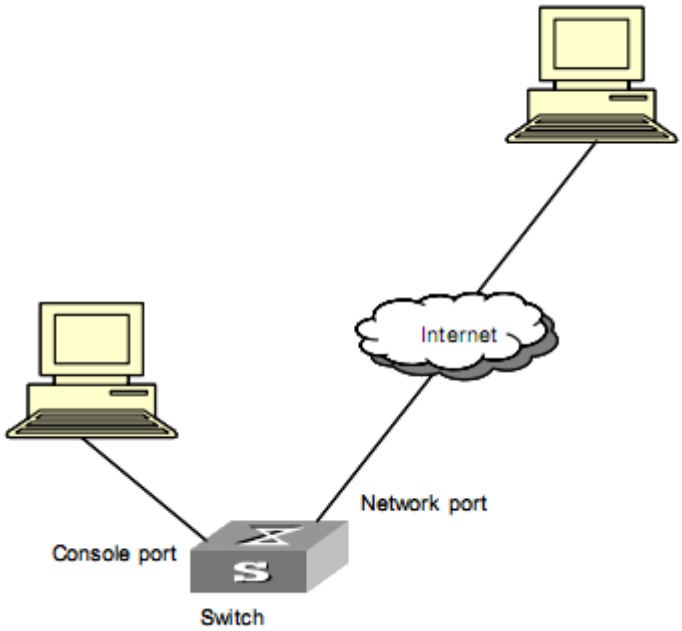
1) Network requirements

➢ Log in to the switch through the Console port and enable address table configuration.

➢ Set the aging time of dynamic MAC address entries to 500 seconds.

➢ Add a static MAC address entry 00:01:fc:00:0c:01 for GigabitEthernet0/0/2 port (assuming that the port belongs to VLAN 1)

2) Network diagram



Picture 1-x Network diagram for MAC address table configuration

3) Configuration procedure

! Add a MAC address, with the VLAN, ports, and states specified.

Switch(config)#mac-address-table static 00:01:fc:00:0c:01 interface ethernet 0/0/2 vlan 1

Add ARL table entry successfully.

! Set the aging time of dynamic MAC addresses to 500 seconds.

Switch(config)#mac-address-table age-time 500

Config MAC address table aging time successfully !

! Display the information about the MAC address entries in global configuration mode.

Switch(config)#show mac-address-table interface ethernet 0/0/2

MAC Address	VLAN ID	port	status
00:01:fc:00:0c:01	1	0/0/2	static

Total entries: 1 .

3.4.3 Restarting the Ethernet Switch

You can perform the following operation in privileged mode when the switch is in

trouble or needs to be restarted.

Table 1-x Restart the Ethernet switch

Operation	Command	Description
Restart the Ethernet switch	**reboot**	

Note:

When rebooting, the system checks whether there is any configuration change. If there is, it prompts you to indicate whether or not to proceed. This prevents you from losing your original configuration due to oblivion after system reboot.

3.5 System Maintenance

3.5.1 Basic Maintenance

Perform following commands in global configuration mode:

Operation	Command	Description
Configure whether to transmit destination-unknown packet	**dlf-forward** { multicast | unicast }	By default, destination-unknown unicast and multicast packets will be transferred. This command can be used in **interface configuration mode.**
Configure whether to transmit BPDU packet	**discard-bpdu**	By default, all BPDU packets will be transferred.
Enable loopback test	**loopback** { internal | external }	This command can be used in both global configuration mode and interface configuration mode. Insert outer loop wire before external loopback test.
Configure cpu rate for receiving packet	**cpu-car** *target_rate*	

3.5.2 Access-limit Management

A switch provides ways to control different types of login users, as Telnet, SNMP and WEB. Here is by IP address. Perform following commands in global configuration mode:

Operation	Command	Description
Configure the permitted IP address for managing switch through web, snmp and telnet	**login-access-list** { web | snmp | telnet|telnet-limit } *ip-address wildcard*	Delete IP address 0.0.0.0 255.255.255.255 first.
Display all permitted IP address for managing switch through web, snmp and telnet	**show login-access-list**	

3.5.3 Telnet Client

After logging in the switch, the Telnet client can be enabled to log in other switch or Telnet server.

Perform following commands in privileged mode.

Operation	Command	Description
Enable telnet client	**telnet** *ip-addr* [*port-num*] [**/localecho**]	By default, *port-num* is 23 and local echo is disabled.
Configure the number of user permitted by telnet	**login-access-list telnet-limit** *limit-no*	By default, the number of max permitted user is 5. This command can be used in global mode
Force telnet client to stop	**stop telnet client** { **all** | *term-id* }	Only the super admin "administrator" can use this command.
Display telnet client	**show telnet client**	

3.5.4 Cpu-alarm

System can monitor CPU utilization. If it is beyond cpu busy threshold, system will send CPU busy alarm. If CPU utilization is under cpu unbusy threshold, system will send CPU busy alarm.

Perform following commands in global configuration mode:

Operation	Command	Description
Enable/disable cpu alarm	**alarm cpu**	By default, this function is enabled.
Configure CPU busy/unbusy threshold	**alarm cpu threshold [busy** *busy* **] [unbusy** *unbusy* **]**	By default, CPU busy threshold is 90 and unbusy threshold is 60. Busy threshold must larger than unbusy threshold.
Display cpu alarm info	**show alarm cpu**	

3.5.5 Mail-alarm

Perform following commands in global configuration mode:

Operation	Command	Description
Enable mail alarm	**mailalarm**	By default, this function is disabled.
Configure smtp server	**mailalarm server** *server-addr*	By default, the smtp server is 0.
Configure the email address of the mail receiver	**mailalarm receiver** *receiver-addr*	By default, the email address of the mail receiver is empty.
Configure Carbon copy receiver	**mailalarm ccaddr** cc-*addr*	By default, the Carbon copy receiver is empty. At most 4 Carbon copy receivers can be configured.
Enable smtp authentication and configure the username and password	**mailalarm smtp authentication username** *username* { **passwd** *passwd* | **encrypt-passwd** *encrypt-passwd* }	By default, this function is disabled. The keyword "encrypt-password" can only be used in the command generated by

		de-compilation
Configure the syslog level for sending mail alarm	**mailalarm logging level** *level*	By default, the syslog level is 0. The syslog whose level is lower than configured will be sent by email.
Display mail alarm info	**show mailalarm**	

3.5.6 Anti-Dos Attack

The IP fragment packet number the system can receive does not occupy the all received packet resources, so it can normally deal with non-fragment packets if there is IP fragment attack.

Perform following commands in global configuration mode:

Operation	Command	Description
Configure the max number of IP fragment packet the system can receive	**anti-dos ip {ttl|fragment** *maxnum* **}**	By default, the number is 800.
Display anti-dos info	**show anti-dos**	

3.5.7 Displaying System Status

You can use the following show commands to check the status and configuration information about the system. For information about protocols and ports, and the associated display commands, refer to relevant sections.

Perform following commands in any mode:

Table 1-2 System display commands

Operation	Command
Display version info	**show version**
Display	**show username**
Display the administrator logged in switch	**show users**
Display system info	**show system**
Display memory info	**show memory**
Display system clock	**show clock**
Display cpu utilization	**show cpu-utilization**
Display cpu-car value	**show cpu-car**
Display packet statistics sent to cpu	**show cpu-statistics**
Clear packet statistics sent to cpu	**clear cpu-statistics**
Display dhcp-server client info	**show dhcp-server clients** [*ip* [*mask*] | *mac* | *poolname*]