Basic Configuration

Table of Contents

Chapter 1   System Management Configuration

1.1   File Management Configuration

1.1.1   Managing the file system

The filename in flash is no more than 20 characters and filenames are case insensitive.

1.1.2   Commands for the file system

The boldfaces in all commands are keywords. Others are parameters. The content in the square brakcet "[ ]" is optional.

Command	Description
format	Formats the file system and delete all data.
dir [filename]	Displays files and directory names. The file name in the symbol "[]" means to display files starting with several letters. The file is displayed in the following format: Index number file name <FILE> length established time
delete filename	Deletes a file. The system will prompt if the file does not exist.
md dirname	Creates a directory.
rd dirname	Deletes a directory. The system will prompt if the directory is not existed.
more filename	Displays the content of a file. If the file content cannot be displayed by one page, it will be displayed by pages.
cd	Changes the path of the current file system.
pwd	Displays the current path.

1.1.3   Starting up from a file manually

monitor#boot flash <*local_filename*>

The previous command is to start a switch software in the flash, which may contain multiple switch software.

Parameter description

Parameter	Description
local_filename	A file name stored in the flash memory Users must enter the file name.

Example

monitor#boot flash switch.bin

1.1.4   Updating software

User can use this command to download switch system software locally or remotely to obtain version update or the custom-made function version (like data encryption and so on).

There are two ways of software update in monitor mode.

1. Through TFTP

monitor#copy tftp flash [ip_addr]

The previous commad is to copy file from the tftp server to the flash in the system. After you enter the command, the system will prompt you to enter the remote server name and the remote filename.

Parameter description

Parameter	Description
ip_addr	IP address of the tftp server If there is no specified IP address, the system will prompt you to enter the IP address after the **copy** command is run.

Example

The following example shows a **main.bin** file is read from the server, written into the switch and changed into the name **switch. Bin**.

monitor#copy tftp flash

Prompt: Source file name[]?main.bin

Prompt: Remote-server ip address[]?192.168.20.1

Prompt: Destination file name[main.bin]?switch.bin

please wait ...
##
##
##
##
##
###
TFTP:successfully receive 3377 blocks ,1728902 bytes
monitor#

2. Through serial port communication protocol－zmodem

Use the **download** command to update software. Enter **download ?** to obtain help.

monitor#download   c0   *<local_filename>*

This command is to copy the file to the flash of system through zmodem. The system will prompt you to enter the port rate after you enter the command.

Parameter description

Parameter	Description
local_filename	Filename stored in the flash Users must enter the filename.

Example

The terminal program can be the Hyper Terminal program in WINDOWS 95, NT 4.0 or the terminal emulation program in WINDOWS 3.X.

monitor#download c0 switch.bin

Prompt: speed[9600]?<u>115200</u>

Then, modify the rate to 115200. After reconnection, select **send file** in the transfer menu of hyper terminal (terminal emulation). The **send file** dialog box appears as follows:

Figure 1- 1   Send files

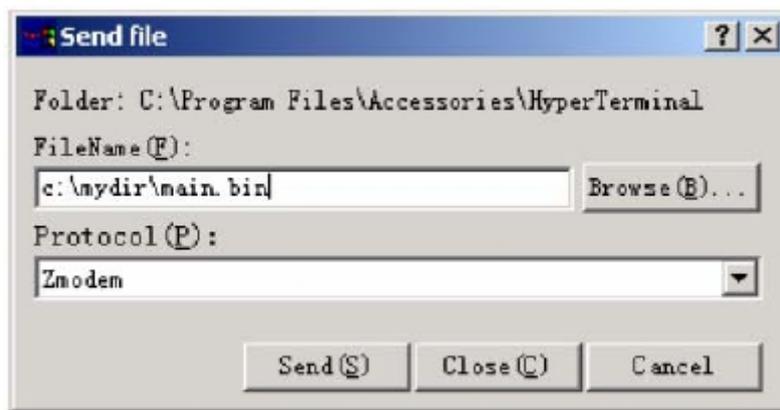Enter the all-path of the switch software **main.bin** that our company provides in the filename input box, choose Zmodem as the protocol. Click **send** to send the file.

After the file is transferred, the following information appears:

ZMODEM:successfully receive 36 blocks ,18370 bytes

It indicates that the software update is completed, and then the baud rate of the hyper terminal should be reset to 9600.

Note:

The maximum download rate of switch S2026,S2224 is 38400 through the zmodem protocol.

1.1.5 Updating configuration

The switch configuration is saved as a file, the filename is startup-config. You can use commands similar to software update to update the configuration.

1. Through TFTP

monitor#copy tftp flash startup-config

2. Through serial port communication protocol－zmodem.

monitor#download c0 startup-config

1.1.6 Using ftp to perform the update of software and configuration

config #copy ftp flash [ip_addr|option]

Use ftp to perform the update of software and configuration in formal program management. Use the **copy** command to download a file from ftp server to switch, also to upload a file from file system of the switch to ftp server. After you enter the command, the system will prompt you to enter the remote server name and remote filename.

copy{**ftp**:[[[//login-name:[login-password]@]location]/directory]/filename}|**flash**:filename e>}{**flash**<:filename>|**ftp**:[[[//login-name:[login-password]@]location]/directory]/filename e}<blksize><mode><type>

Parameter description

Parameter	Description
login-nam	Username of the ftp server If there is no specified username, the system will prompt you to enter the username after the **copy** command is run.
login-password	Password of the ftp server If there is no specified password, the system will prompt you to enter the password after the **copy** command is run.
nchecksize	The size of the file is not checked on the server.
vrf	Provides vrf binding function for the device that supports MPLS.
blksize	Size of the data transmission block Default value: 512
ip_addr	IP address of the ftp server If there is no specified IP address, the system will prompt you to enter the IP address after executing the **copy** command.
active	Means to connect the ftp server in active mode.

passive	Means to connect the ftp server in passive mode.
type	Set the data transmission mode (ascii or binary)

Example

The following example shows a **main.bin** file is read from the server, written into the switch and changed into the name **switch. Bin**.

config#copy ftp flash

Prompt: ftp user name[anonymous]? login-nam

Prompt: ftp user password[anonymous]? login-password

Prompt: Source file name[]?main.bin

Prompt: Remote-server ip address[]?192.168.20.1

Prompt: Destination file name[main.bin]?switch.bin

or

config#copy ftp://login-nam:login-password@192.168.20.1/main.bin flash:switch.bin
##
##
FTP:successfully receive 3377 blocks ,1728902 bytes
config#

Note:

1) When the ftp server is out of service, the wait time is long. If this problem is caused by the tcp timeout time (the default value is 75s), you can configure the global command **ip tcp synwait-time** to modify the tcp connection time. However, it is not recommended to use it.

2) When you use ftp in some networking conditions, the rate of data transmission might be relatively slow. You can properly adjust the size of the transmission block to obtain the best effect. The default size is 512 characters, which guarantee a relatively high operation rate in most of the networks.

1.2   Basic System Management Configuration

1.2.1   Configuring Ethernet IP address

monitor#ip address *<ip_addr> <net_mask>*

This command is to configure the IP address of the Ethernet. The default IP address is 192.168.0.1, and the network mask is 255.255.255.0.

Parameter description

Parameter	Description

ip_addr	IP address of the Ethernet
net_mask	Mask of the Ethernet

Example

monitor#ip address 192.168.1.1 255.255.255.0

1.2.2   Configuring default route

monitor#ip route default <*ip_addr*>

This command is used to configure the default route. You can configure only one default route.

Parameter description

Parameter	Description
ip_addr	IP address of the gateway

Example

monitor#ip route default 192.168.1.1

1.2.3   Using ping to test network connection state

monitor#ping <*ip_address*>

This command is to test network connection state.

Parameter description

Parameter	Description
ip_address	Destination IP address

Example

monitor#ping 192.168.20.100
PING 192.168.20.100: 56 data bytes
64 bytes from 192.168.20.100: icmp_seq=0. time=0. ms
64 bytes from 192.168.20.100: icmp_seq=1. time=0. ms
64 bytes from 192.168.20.100: icmp_seq=2. time=0. ms
64 bytes from 192.168.20.100: icmp_seq=3. time=0. ms
----192.168.20.100 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms)   min/avg/max = 0/0/0

Chapter 2   Terminal Configuration

2.1   VTY Configuration Introduction

The system uses the **line** command to configure terminal parameters. Through the command, you can configure the width and height that the terminal displays.

2.2   Configuration Task

The system has four types of lines: console, aid, asynchronous and virtual terminal. Different systems have different numbers of lines of these types. Refer to the following software and hardware configuration guide for the proper configuration.

Line Type	Interface	Description	Numbering
CON(CTY)	Console	To log in to the system for configuration.	0
VTY	Virtual and asynchronous	To connect Telnet, X.25 PAD, HTTP and Rlogin of synchronous ports (such as Ethernet and serial port) on the system	32 numbers starting from 1

2.2.1   Relationship between line and interface

1. Relationship between synchronous interface and VTY line

The virtual terminal line provides a synchronous interface to access to the system. When you connect to the system through VTY line, you actually connects to a virtual port on an interface. For each synchronous interface, there can be many virtual ports.

For example, if several Telnets are connecting to an interface (Ethernet or serial interface), you need to do the following steps for the VTY configuration:

(1)   Log in to the line configuration mode.

(1)   Configure the terminal parameters.

For VTY configuration, refer to Part 2.4   "VTY configuration example".

2.3   Monitor and Maintenance

Run **showline** to chek the VTY configuration.

2.4 VTY Configuration Example

It shows how to cancel the limit of the line number per screen for all VTYs without **more** prompt:

config#line vty 0 32
config_line#length 0

Chapter 3   Network Management Configuration

3.1   Configuring SNMP

3.1.1   Introduction

The SNMP system includes the following parts:

- SNMP management side (NMS)

- SNMP agent (AGENT)

- Management information base (MIB)

SNMP is a protocol   working on the application layer. It provides the packet format between SNMP management side and agent.

SNMP management side can be part of the network management system (NMS, like CiscoWorks). Agent and MIB are stored on the system. You need to define the relationship between network management side and agent before configuring SNMP on the system.

SNMP agent contains MIB variables. SNMP management side can check or modify value of these variables. The management side can get the variable value from agent or stores the variable value to agent. The agent collects data from MIB. MIB is the database of device parameter and network data. The agent also can respond to the loading of the management side or the request to configure data. SNMP agent can send trap to the management side. Trap sends alarm information to NMS indicating a certain condition of the network. Trap can point out improper user authentication, restart, link layer state(enable or disable), close of TCP connection, lose of the connection to adjacent systems or other important events.

1. SNMP notification

When some special events occur, the system will send 'inform' to SNMP management side. For example, when the agent system detects an abnormal condition, it will send information to the management side.

SNMP notification can be treated as trap or inform request to send. Since the receiving side doesn't send any reply when receiving a trap, this leads to the receiving side cannot be sure that the trap has been received. Therefore the trap is not reliable. In comparison, SNMP management side that receives "inform request" uses PDU that SNMP echoes as the reply for this information. If no "inform request" is received on the management side, no echo will be sent. If the receiving side doesn't send any reply, then you can resend the "inform request". Then notifications can reach their destination.

Since inform requests are more reliable, they consume more resources of the system and network. The trap will be discarded when it is sent. The "inform request" has to be stored in the memory until the echo is received or the request timeouts. In addition, the

trap is sent only once, while the "inform request" can be resent for many times. Resending "inform request" adds to network communications and causes more load on network. Therefore, trap and inform request provide balance between reliability and resource. If SNMP management side needs receiving every notification greatly, then the "inform request" can be used. If you give priority to the communication amount of the network and there is no need to receive every notification, then trap can be used.

This switch only supports trap, but we provide the extension for "inform request".

2. SNMP version

System of our company supports the following SNMP versions:

●   SNMPv1---simple network management protocol,a complete Internet standard,which is defined in RFC1157.

●   SNMPv2C--- Group-based Management framework of SNMPv2, Internet test protocol, which is defined in RFC1901.

Layer 3 switch of our company also supports the following SNMP:

●   SNMPv3--- a simple network management protocol version 3, which is defined in RFC3410.

SNMPv1 uses group-based security format. Use IP address access control list and password to define the management side group that can access to agent MIB.

SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network.

The security features provided in SNMPv3 are:

•Message integrity—Ensuring that a packet has not been tampered with in-transit.

•Authentication—Determining the message is from a valid source.

•Encryption—Scrambling the contents of a packet prevent it from being seen by an unauthorized source.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level will determine which security mechanism is employed when handling an SNMP packet. Three security models are available, that is, authentication and encryption, authentication and no encryption, no authentication.

You need to configure SNMP agent to the SNMP version that the management working station supports. The agent can communicate with many management sides.

3. Supported MIB

SNMP of our system supports all MIBII variables (which will be discussed in RFC 1213) and SNMP traps (which will be discussed in RFC 1215).

Our system provides its own MIB extension for each system.

3.1.2   SNMP Configuration Tasks

●   Configuring SNMP view

●   Creating or modifying the access control for SNMP community

●   Configuring the contact method of system administrator and the system's location

●   Defining the maximum length of SNMP agent data packet

●   Monitoring SNMP state

●   Configuring SNMP trap

●   Configuring SNMP binding source address

●   Configuring NMPv3 group

●   Configuring NMPv3 user

●   Configuring NMPv3 EngineID

1. Configuring SNMP view

The SNMP view is to regulate the access rights (include or exclude) for MIB. Use the following command to configure the SNMP view.

Command	Description
snmp-server view *name oid*] [exclude | include]	Adds the subtree or table of OID-specified MIB to the name of the SNMP view, and specifies the access right of the object identifier in the name of the SNMB view. Exclude: decline to be accessed Include: allow to be accessed

The subsets that can be accessed in the SNMP view are the remaining objects that "include" MIB objects are divided by "exclude" objects.   The objects that are not configured are not accessible by default.

After configuring the SNMP view, you can implement SNMP view to the configurtation of the SNMP group name, limiting the subsets of the objects that the group name can access.

2. Creating or modifying the access control for SNMP community

You can use the SNMP community character string to define the relationship between SNMP management side and agent. The community character string is similar to the password that enables the access system to log in to the agent. You can specify one or multiple properties releavant with the community character string. These properties are optional:

Allowing to use the community character string to obtain the access list of the IP address at the SNMP management side

Defining MIB views of all MIB object subsets that can access the specified community

Specifying the community with the right to read and write the accessible MIB objects

Configure the community character string in global configuration mode using the following command:

Command	Function
snmp-server community *string* [**view** *view-name*] [**ro** | **rw**] [*word*]	Defines the group access character string.

You can configure one or multiple group character strings. Run **no snmp-server community** to remove the specified community character string.

For how to configure the community character string, refer to the part "SNMP Commands".

3. Configuring the contact method of system administrator and the system's location

SysContact and sysLocation are the management variables in the MIB's system group, respectively defining the linkman's identifer and actual location of the controlled node. These information can be accessed through **config.** files. You can use the following commands in global configuration mode.

Command	Function
snmp-server contact *text*	Sets the character string for the linkman of the node.
snmp-server location *text*	Sets the character string for the node location.

4. Defining the maximum length of SNMP agent data packet

When SNMP agent receives requests or sents respons, you can configure the maximum length of the data packet. Use the following command in global configuration mode:

Command	Function
snmp-server packetsize *byte-count*	Sets the maximum length of the data packet.

5. Monitoring SNMP state

You can run the following command in global configuration mode to monitor SNMP output/input statistics, including illegal community character string items, number of mistakes and request variables.

Command	Function
show snmp	Monitores the SNMP state.

6. Configuring SNMP trap

Use the following command to configure the system to send the SNMP traps (the second task is optional):

● Configuring the system to send trap

Run the following commands in global configuration mode to configure the system to send trap to a host.

Command	Function
snmp-server host host community-string [trap-type]	Specifies the receiver of the trap message.
snmp-server host *host* [traps|informs]{version {v1 | v2c | v3 {auth | noauth | priv } }}*community-string* [*trap-type*]	Specifies the receiver, version number and username of the trap message. Note: For the trap of SNMPv3, you must configure SNMP engine ID for the host before the host is configured to receive the trap message.

When the system is started, the SNMP agent will automatically run. All types of traps are activated. You can use the command **snmp-server host** to specify which host will receive which kind of trap.

Some traps need to be controlled through other commands. For example, if you want SNMP link traps to be sent when an interface is opened or closed, you need to run **snmp trap link-status** in interface configuration mode to activate link traps. To close these traps, run the interface configuration command **snmp trap link-stat**.

You have to configure the command **snmp-server host** for the host to receive the traps.

● Modifying the running parameter of the trap

As an optional item, it can specify the source interface where traps originate, queue length of message or value of resending interval for each host.

To modify the running parameters of traps, you can run the following optional commands in global configuration mode.

Command	Function
snmp-server trap-source *interface*	Specifies the source interface where traps originate and sets the source IP address for the message.
snmp-server queue-length *length*	Creates the queue length of the message for each host that has traps. Default value: 10
snmp-server trap-timeout *seconds*	Defines the frequency to resend traps in the resending queue. Default value: 30 seconds

3.1.3 Configuration example

1. Example 1

snmp-server community public RO

snmp-server community private RW

snmp-server host 192.168.10.2 public

The above example shows:

- how to set the community string **public** that can only read all MIB variables.

- how to set the community string **private** that can read and write all MIB variables.

You can use the community string **public** to read MIB variables in the system. You can also use the community string **private** to read MIB variables and write writable MIB variables in the system.

The above command specifies the community string **public** to send traps to 192.168.10.2 when a system requires to send traps. For example, when a port of a system is in the **down** state, the system will send a **linkdown** trap information to 192.168.10.2.

2. Example 2

snmp-server engineID remote 90.0.0.3 80000523015a000003

snmp-server group getter v3 auth

snmp-server group setter v3 priv write v-write

snmp-server user get-user getter v3 auth sha 12345678

snmp-server user set-user setter v3 encrypted auth md5 12345678

snmp-server user notifier getter remote 90.0.0.3 v3 auth md5 abcdefghi

snmp-server host 90.0.0.3 informs version v3 auth notifier

snmp-server view v-write internet included

The above example shows how to use SNMPv3 to manage devices. Group **getter** can browse device information, while group **setter** can set devices. User **get-user** belongs to group **getter** while user **set-user** belongs to group **setter**.

For user **get-user**, its security level is **authenticate but not encrypt**, its password is **12345678**, and it uses the sha arithmetic to summarize the password.

For user **set-user**, its security level is **authenticate and encrypt**, its password is **12345678**, and it uses the md5 arithmetic to summarize the password.

When key events occur at a device, use username **notifier** to send **inform** messages to host 90.0.0.3 of the administrator.

3.2 RMON Configuration

3.2.1 RMON configuration task

RMON configuration tasks include:

- Configuring the rMon alarm function for the switch

- Configuring the rMon event function for the switch

- Configuring the rMon statistics function for the switch

●   Configuring the rMon history function for the switch

●   Displaying the rMon configuration of the switch

1. Configuring rMon alarm for switch

You can configure the rMon alarm function through the command line or SNMP NMS. If you configure through SNMP NMS, you need to configure the SNMP of the switch. After the alarm function is configured, the device can monitor some statistic value in the system. The following table shows how to set the rMon alarm function:

Command	Function
configure	Enter the global configuration mode.
rmon alarm index variable *interval* {**absolute** | **delta**} **rising-threshold** *value* [*eventnumber*] **falling-threshold** *value* [*eventnumber*] [**owner** *string*]	Add a rMon alarm item. **index** is the index of the alarm item. Its effective range is from 1 to 65535. **variable** is the object in the monitored MIB. It must be an effective MIB object in the system. Only obejects in the Integer, Counter, Gauge or TimeTicks type can be detected. **interval** is the time section for sampling. Its unit is second. Its effective value is from 1 to 4294967295. **absolute** is used to directly monitor the value of MIB object. **delta** is used to monitor the value change of the MIB objects between two sampling. **value** is the threshold value when an alarm is generated. **eventnumber** is the index of an event that is generated when a threshold is reached. **eventnumber** is optional. **owner string** is to describe the information about the alarm.
exit	Enter the management mode again.
write	Save the configuration.

After a rMon alarm item is configured, the device will obtain the value of variable-specified oid after an interval. The obtained value will be compared with the previous value according to the alrm type (absolute or delta). If the obtained value is bigger than the previous value and surpasses the threshold value specified by **rising-threshold**, an event whose index is **eventnumber** (If the value of **eventnumber** is 0 or the event whose index is **eventnumber** does not exist in the event table, the event will not occur). If the variable-specified oid cannot be obtained, the state of the alarm item in this line is set to **invalid**. If you run **rmon alarm** many times to configure alarm items with the same index, only the last configuration is effective. You can run **no rmon alarm index** to cancel alarm items whose indexes are **index**.

2. Configuring eMon event for switch

The steps to configure the rMon event are shown in the following table:

Step	Command	Purpose
1.	**configure**	Enter the global configuration mode.
2.	**rmon event index** [**description** *string*] [**log**]	Add a rMon event item.

	[owner *string*] [trap community]	**index** means the index of the event item. Its effective range is from 1 to 65535.
		description means the information about the event.
		log means to add a piece of information to the log table when a event is triggered.
		trap means a trap message is generated when the event is triggered. **community** means the name of a community.
		owner string is to describe the information about the alarm.
3.	**exit**	Enter the management mode again.
4.	**write**	Save the configuration.

After a rMon event is configured, you must set the domain **eventLastTimeSent** of the rMon event item to **sysUpTime** when a rMon alarm is triggered. If the **log** attribute is set to the rMon event, a message is added to the log table. If the **trap** attribute is set to the rMon event, a trap message is sent out in name of community. If you run **rmon event** many times to configure event items with the same index, only the last configuration is effective. You can run **no rmon event index** to cancel event items whose indexes are **index**.

3. Configuring rMon statistics for switch

The rMon statistics group is used to monitor the statistics information on every port of the device. The steps to configure the rMon statistics are as follows:

Step	Command	Purpose
1.	**configure**	Enter the global configuration mode.
2.	**interface iftype ifid**	Enter the port mode.
		iftype means the type of the port.
		ifid means the ID of the interface.
3.	**rmon collection stat index** [**owner** *string*]	Enable the statistics function on the port.
		index means the index of the statistics.
		owner string is to describe the information about the statistics.
4.	**exit**	Enter the global office mode.
5.	**exit**	Enter the management mode again.
6.	**write**	Save the configuration.

If you run **rmon collection stat** many times to configure statistics items with the same index, only the last configuration is effective. You can run **no rmon collection stats index** to cancel statistics items whose indexes are **index**.

4. Configuring rMon history for switch

The rMon history group is used to collect statistics information of different time sections on a port in a device. The rMon statistics function is configured as follows:

Step	Command	Purpose

1.	configure	Enter the global configuration command.
2.	interface iftype ifid	Enter the port mode. **iftype** means the type of the port. **ifid** means the ID of the interface.
3.	rmon collection history index [buckets bucket-number] [interval second] [owner owner-name]	Enable the history function on the port. **index** means the index of the history item. Among all data collected by history item, the latest **bucket-number** items need to be saved. You can browse the history item of the Ethernet to abtain these statistics values. The default value is 50 items. **second** means the interval to abtain the statistics data every other time. The default value is 1800 seconds. **owner string** is used to describe some information about the history item.
4.	exit	Enter the global office mode again.
5.	exit	Enter the management mode again.
6.	write	Save the configuration.

After a rMon history item is added, the device will obtain statistics values from the specified port every **second** seconds. The statistics value will be added to the history item as a piece of information. If you run **rmon collection history index** many times to configure history items with the same index, only the last configuration is effective. You can run **no rmon history index** to cancel history items whose indexes are **index**.

Note:

Too much system sources will be occupied in the case the value of **bucket-number** is too big or the value of **interval second** is too small.

5. Displaying rMon configuration of switch

Run **show** to display the rMon configuration of the switch.

Command	Purpose
show rmon [alarm] [event] [statistics] [history]	Displays the rmon configuration information. **alarm** means to display the configuration of the alarm item. **event** means to show the configuration of the event item and to show the items that are generated by the occurance of events and are contained in the log table. **statistics** means to display the configuration of the statistics item and statistics values that the device collects from the port. **history** means to display the configuration of the history item and statistics values that the device collects in the latest specified intervals from the port.