Basic Configuration Commands

Table of Contents

Chapter 1 System Management Commands

1.1 Configuring File Management Commands

- copy
- delete
- dir
- ip address
- ip route
- show configuration
- format
- more
- download
- upload

1.1.1 Copy

To read a file from the tftp server to a switch, use the copy command.

copy tftp<*:filename*> {**flash**<*:filename*>|**rom**} [*ip_addr*]

Parameter

Parameter	Description
tftp<:filename>	Read a file from the tftp server. Filename indicates the relevant filename. If not specified the filename, the system will prompt user to input the filename after executing the copy command.
flash <:filename>	Write a file to the flash memory of the switch. Filename indicates the relevant filename. If not specified the filename, the system will prompt user to input the filename after executing the copy command.
rom	Updates bootrom for the switch.
ip_addr	Specifies the IP address of tftp srever. If not specified, the system will prompt user to input the IP address after executing the copy command.

Default

Command mode

monitor mode

Instrution

Example

monitor#copy tftp:switch.bin flash:switch.bin 192.2.2.1

The example shows how to read the **switch.bin** file from the tftp server to the flash memory of the switch.

Related commands

1.1.2   Delete

To delete a file, use the delete command.

delete   *file-name*

Parameter

Parameter	Description
file-name	Specifies the filename (maximum 20 characters)

Default

If the file name is not specified, the system will delete the **startup-config** file by default.

Command mode

monitor mode

Instruction

Related commands

1.1.3   dir

To display filename, use the dir command.

dir   *file-name*

Parameter

Parameter	Description
file-name	Specifies the filename (maximum 20 characters)

Default

Command mode

monitor mode

Instruction

Related commands

1.1.4   ip address

To set an IP address for an Ethernet interface, use the ip address command.

ip address *ip-address mask*

Parameter

Parameter	Description
ip-address	IP address
mask	IP network mask

Default

Command mode

monitor mode

Instruction

Example

monitor#ip address 192.168.1.1 255.255.255.0

Related commands

ip route

ping

1.1.5   ip route

To specify a default gateway, use the ip route default command.

ip route default gw_ip_addr

Parameter

Parameter	Description
gw_ip_addr	Default gateway address

Default

Command mode

monitor mode

Instrution

Example

monitor#ip route default 192.168.1.3

Related commands

ip address

1.1.6   show configuration

To display the running configuration file, use the show configuration command.

show configuration

Parameter

Default

Command mode

monitor mode

Instrution

Related commands

1.1.7   format

To format file system, use the format command.

format

Parameter

Default

Command mode

EXEC

Instrution

All files in the file system will de deleted after executing the format command.

Related commands

1.1.8　more

To display the contents of a file, use the more command.

more　*file-name*

Parameter

Parameter	Description
file-name	Specifies the name of a file (maximum 20 characters)

Default

Command mode

EXEC

Instrution

If all files are displayable characters, they will be displayed in ASCII format, or they will be displayed binary format.

Related commands

1.2　BasicSystemManagementCommands

- bootflash

- cd
- chinese
- english
- chram
- date
- debub job
- md
- pwd
- rd
- rename
- reboot
- show break
- show memory
- alias
- boot system flash
- help
- history
- job
- jobd
- show alias
- show job

1.2.1 boot flash

To enable the system from the specified file in monitor mode, use the boot flash command.

boot flash *filename*

parameter

parameter	Description
filename	The specified file name.

default

command mode

monitor mode

command mode

Use the boot flash command to enable the device after user entering the monitor mode.

example

> monitor#boot flash switch.bin

related commands

> none

1.2.2   cd

> To change the current directory, use the cd command.
>
> **cd**   *directory|..*

parameter:

parameter	description
directory	Name of the directory. (maximum 20 characters)
..	Upper directory.

default

> none

command mode

> monitor mode

command mode

> none

example

> monitor#cd my_dir

related commands

> pwd

1.2.3   chinese

> To switch command prompt to chinese mode, use the chinese command.

parameter

> ✧ none

default

> none

command mode

>   monitor mode

command mode

>   none

example

>   none

related commands

>   none

1.2.4   chram

>   To modify memory data, use the chram command.

>   **chram** *mem_addr value*

parameter

parameter	description
mem_addr	Memory address in Hex format. Range is from 0 to 0x01FFFF00 (it depends on the memory volume of the switch)
value	Memory data in Hex format

default

>   none

command mode

>   Monitor mode

command mode

>   This is a debugging command which is not recommended for user to use.

example

>   none

related commands

>   none

1.2.5   date

>   To set the absolute time, use the date command.

parameter

default

command mode

monitor mode

command mode

This command is used to set the abslute time for the system. For the switch with a battery-powered clock, the clock will be powered by the battery. If the clock doesn't keep good time, you need to change the battery.

For the swich without a battery-powered clock, the system date is configured to July 1st, 1970 after the reboot of the switch, and user needs to set the current time each time when starting the switch.

example

monitor#date
The current date is 2000-7-27 21:17:24
Enter the new date(yyyy-mm-dd):2000-7-27
Enter the new time(hh:mm:ss):21:17:00

related commands

1.2.6　english

To switch the command prompt to english mode, use the english command.

parameter

default

command mode

monitor

instruction

example

> none

related commands

> none

1.2.7 md

> **md** *directory*

parameter

parameter	description
directory	Name of directory (maximum 20 characters)

default

> none

command mode

> monitor

instruction

> To set a directory, use the md command

related commands

> none

1.2.8 pwd

parameter

> none

default

> none

command mode

> monitor mode

instruction

> to display the current directory, use the pwd command

related commands

1.2.9 rd

rd *directory*

parameter

parameter	Description
directory	Name of the directory(maximum 20 characters)

default

command mode

monitor mode

instruction

The system prompts if the directory is not empty. The system prompts if the directory doesn't exist. To delete a command, use the rd command.

related commands

1.2.10 rename

To rename a file in a file system, use the rename command.

rename *old_file_name* *new_file_name*

parameter

parameter	description
old_file_name	The original filename.
new_file_name	The new filename.

default

command mode

monitor mode

instruction

related commands

1.2.11 reboot

To reboot a switch, use the reboot command.

parameter

default

command mode

monitor mode

instruction

related commands

1.2.12 alias

[no] history [+ *<count>* | - *<count>* | clear]

parameter

parameter	description
+ <count>	To display the count<1-20> historial command from the beginning to the end
- <count>	To display the count<1-20> historial command from the end to the beginning

default

If there are no more than 20 commands executed, all historical command lines will be displayed from the beginning to the end. If there are more than 20 commands executed, all historical command lines will be displayed from the beginning to the end.

comand mode

Random command mode

explanation

The modularized switch can save up to 20 historical commands. You can invoke these commands with the "up" or "down" key or directly use it after edition. The command is used to browse the **history** command. You can run the **[no] history** command to delete the **history** command.

example

The following example shows the latest five historical commands from the end to the beginning:

switch#history - 5
config
int e0/1
no ip addr
ip addr 192.2.2.49 255.255.255.0
exit

relative command

None

1.2.13   boot system flash

Run the **boot system flash** command to specify the systematic mirroring files when the system is started up. Run the **no boot system flash** command to delete the previous configuration.

boot system flash *filename*

no boot system flash *filename*

Parameter

Parameter	Description
filename	It is the specified filename, which contains no more than 20 characters.

Default

None

Command mode

Global configuration mode

Instruction

If you have not configured the command, the system will execute the first systematic mirroring file in the flash file system. If you have configured multiple commands, the system will execute the mirroring files one by one. If the file does not exist or the check sum is wrong, the system will execute the next file. If both fail, the system will run at the monitoring state.

Example

config#boot system flash switch.bin

Relative command

None

1.2.14 help

help

Parameter

None

Default

None

Command mode

Management mode

Instruction

The command is used to display the help system of the switch.

Example

After you enter the command, the help system of the switch is displayed.

switch# help
Help may be requested at any point in a command by entering a question mark '?',If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a command argument (e.g.'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'interface e?'.)

Relative command

None

1.2.15 history

The command is used to check the historical commands. Run the **[no] history** command to delete the historical commands.

[no] history [+ *<count>* | - *<count>* | clear]

Parameter

Parameter	Description

+ \<count\>	Displays the count\<1-20\> historial command from the beginning to the end.
- \<count\>	Displays the count\<1-20\> historial command from the end to the beginning.

Default

If there are no more than 20 commands executed, all historical command lines will be displayed from the beginning to the end. If there are more than 20 commands executed, all historical command lines will be displayed from the beginning to the end.

Command mode

Abandom command mode

Instruction

The modularized switch can save up to 20 historical commands. You can invoke these commands with the "up" or "down" key or directly use it after edition.

Example

The following example shows the latest five commands from the end to the beginning:

switch#history - 5
config
int e1/1
no ip addr
ip addr 192.2.2.49 255.255.255.0
exit

Relative command

None

1.2.16   show alias

It is used to display all aliases or the designated alias.

show alias [\<*alias name*\>]

Parameter

Parameter	Description
alias name	The alias of the command

Default

Display all aliases according the format "alias name=command line".

Command mode

Management mode or configuration mode

Instruction

None

Example

The following example shows how to display all aliases of the current system:

switch_config#show alias
hualab=date
router=snmp

Relative command

alias

1.2.17 show job

It is used to display the parameters of the job and the information about job execution:

show job {*paramter | status*}

Parameter

Parameter	Description
paramter	Displays the parameters of the job.
status	Displays the execution state of the job.

Default

None

Command mode

Management mode or configuration mode

Instruction

Run the **show job** command to browse the defined parameters and the dynamic execution state of the job.

Example

The following example shows how to display the parameters of the job:

switch_config#show job parameter
<showver> fires interval, first at 5, re-fires per 5 secs, on error stop
        will do "show ver"

The following example shows how to display the dynamic execution state of the job:

Jobd disabled at 245218 seconds
 Name: job's name
 Type: none - Not scheduled, interval - Fire interval, one-shot - Fire once
 Status: null - Not scheduled, idle - To fire first
         started - Fired ever, to fire again, stopped - Can't fire

First: first time to fire
Last: last time of firing or restarting
Next-due: next time to fire(after now)
Times: times fired ever
Cause: auto - Automatic, error - Error meeting, command - By command

Job's status and statistics

============================

Name	Type	State	First	Last	Next-due	Times	Cause
showver	interval	idle	5	*	*	2	auto

Total 1 jobs, 0 null, 1 idle, 0 started, 0 stopped

Relative command

debug job

job

jobd

1.2.18   show break

It is used to display the abnormal information of the system. The system stores all abnormal information in the latest running. The abnormal information contains the times of abnormity, the stack content and the invoked functions when abnormity occurs.

Parameter

None

Default

None

Command mode

Monitoring state

Instruction

The command is only used for debugging.

Relative command

None

1.2.19   show memory

It is used to display the content of the system memory.

show memory *mem_addr*

Parameter

Parameter	Description

mem_addr	Memory address in hex, which ranges from 0 to 0x01FFFF00 (decided by the memory capacity of the switch).

Default

None

Command mode

Monitoring state

Instruction

None

Relative command

None

1.3 HTTP Configuration Command

The following are HTTP configuration commands:

- ip http access-class
- ip http port
- ip http server
- debug ip http

1.3.1 ip http access-class

Command description

ip http access-class *string*

no ip http access-class

Run the command **ip http access-class** to ensure the designated HTTP query is accepted.

Parameter

Parameter	Description
string	The designated standard access list whose range is N/A.

Default

no ip http access-class

Instruction

Set the designated standard access list before running the command.

Run the command **no ip http access-class** to cancel the HTTP service limitation of the access list.

Command mode

Global configuration mode

Example

switch_config# ip access-list standard http-acl
switch_config_std_nacl# permit 192.2.2.37 255.255.255.0
switch _config_std_nacl# exit
switch _config# ip http access-class http-acl

1.3.2   ip http port

Command description

ip http port *number*

Run the command **ip http port** to designate the listening port of the http service.

Parameter

Parameter	Description
number	The service port number, ranging from 1 to 65535

Default

The default HTTP service port number of the browser is 80.

Explanation

After running the **http port** command, shut down the previous listening port and then use the designated port to accept the http service request if the http service is started up. If the http service is not started, the **ip http port** command is temporarily useless.

Command mode

Global configuration mode

Example

The following example shows how to modify the http port from 80 to 90:

switch _config# ip http server
switch _config# ip http port 90

1.3.3   ip http server

Command description

ip http server

no ip http server

To start up the http service, run the command **ip http server**.

Parameter

None

Default

no ip http server

Instruction

Run the command **ip http server** to enable the switch to accept the HTTP service request through the designated port, handle the request and return the result to the browser.

Command mode

Global configuration mode

Example

The following example shows how to start up the http service:

switch _config# ip http server

1.3.4   debug ip http

Command description

debug ip http

The previous command is used to export the debugging information during http service running. You can use the **no** command to resume the default value.

Parameter

None

Default

no debug ip http

Instruction

None

Command mode

Global configuration mode

Example

The following example shows how to enable HTTP debugging output:

switch# **debug ip http**
switch#

Chapter 2   Terminal Service Configuration Command

2.1   Telnet Configuration Command

The chapter describes telnet and relative commands. The **telnet** command is used to establish a session with the remote server. The **telnet** command is always working at the UNIX operating systems. Option negotiation is required. Telnet does not provide itself the login authentication. Telnet is different from Rlogin because telnet does not provide itself password check.

The following are telnet configuration commands:

- telnet
- ip telnet
- where
- disconnect
- resume
- switchkey
- switchmsg
- sequence-char
- clear Telnet
- show Telnet
- debug Telnet

2.1.1   telnet

The following is a command sentence for establishing a telnet session:

telnet *server-ip-addr/server-host-name* [**/port** *port*][**/source-interface** *interface*] [**/local** *local-ip-addr*] [**/debug**][**echo/noecho**] [**/script** *scriptname*]

Parameter

Parameter	Description
server-ip-addr	Dotted-decimal IP address of the remote server
server-host-name	Name of the remote server, which is configured by the **ip host** command
port	Telnet port of the remote server
interface	Local interface where the telnet connection is originated
local-ip-addr	Local IP address where the telnet connection is originated
/debug	A negotiation process for openning the debug at the client side and printing the connection
echo/noecho	Enable or disable the local echo. The default value is **noecho**.
scriptname	A script name used for auto login

Default

The default port number is 23. The interface has no default number.

Command mode

Management mode

Instruction

You can use one of the following command lines to establish a remote login.

telnet server-ip-addr/server-host-name

In this case, the application program directly sends the telnet login request to port 23 of the remote server. The local IP address is the IP address which is nearest to the peer and found by the routing table.

telnet server-ip-addr/server-host-name /port port

In this case, the application program sends a telnet login request to the port of the peer.

telnet server-ip-addr/server-host-name /source-interface interface

In this case, the application program uses the IP address on the interface ass the local IP address.

telnet server-ip-addr/server-host-name /debug

In this case, the application program opens the debug and exports the connection at the client side.

telnet server-ip-addr/server-host-name echo/noecho

In this case, the application program enables or disables the local echo. The local echo is disabled by default. The echo is completed at the server side. Only when the server is not in charge of echo is the local echo enabled.

telnet server-ip-addr/server-host-name /script scriptname

Before executing the automatic login command of the script, run the command **ip telnet script** to configure the script.

The previous commands can be used together.

During the session with the remote server, you can press the **Q** button to exit the session. If the session is not manually closed, the session will be complete after a 10-second timeout.

Example

Suppose you want to telnet server 192.168.20.124, the telnet port of the server is port 23 and port 2323, and the local two interfaces are e1/1(192.168.20.240) and s1/0(202.96.124.240). You can run the following operations to complete the remote login.

1．telnet 192.168.20.124 /port 2323

In this case, the telnet connection with port 2323 of the peer is to be established. The local IP address of the peer is 192.168.20.240.

2．telnet 192.168.20.124 /source-interface s1/0

In this case, the telnet connection with port 23 of the peer is to be established. The local IP address of the peer is 202.96.124.240.

3．telnet 192.168.20.124 /local 192.168.20.240

In this case, the telnet connection with port 23 of the peer is to be established. The local IP address of the peer is 192.168.20.240.

4．telnet 192.168.20.124 /debug

In this case, the telnet connection negotiation with port 23 of the peer will be printed out.

5．telnet 192.168.20.124 /echo

In this case, the local echo is enabled. If the echo is also enabled at the server side, all input will be echoed twice.

6．telnet 192.168.20.124 /script s1

Use login script S1 for automatic login.

2.1.2   ip telnet

The following are the configuration command formats of the telnet session:

ip telnet source-interface vlan *value*

ip telnet access-class *accesslist*

ip telnet listen-port *start-port [end-port]*

ip telnet script *scriptname 'user_prompt' user_answer 'pwd_prompt' pwd_answer*

Parameter

Parameter	Description
value	Local interface where the telnet request is originated
accesslist	Access list name to limit the source address when the local client receives the connection
start-port	Starting port number designated at the listening port area
end-port	End port number designated at the listening port area
scriptname	Name of the login script
user_prompt	Username prompt returned by the telnet server
user_answer	Username response information from the client side
pwd_prompt	Password prompt returned by the telnet server
pwd_answer	Password response information submitted by the client side

Default

None

Command mode

Global configuration

Instruction

- Run the following command to configure the local interface for originating the telnet connection:

  ip telnet source-interface *interface*

In this case, all telnet connections originated afterwards are through the interface. The configuration command is similar to the command **telnet source-interface** *interface*. However, the **telnet** command has no interface parameters followed. When the interface is configured and the **telnet** command has interface parameters, the interface followed the telnet command is used.

● Run the following command to configure the name of the access list which performs limitation on local telnet connection reception.

ip telnet access-class *accesslist*

In this case, the access list will be checked when the server accepts all telnet connections.

● Run the following command to configure a port, except the default port 23, to receive the telnet service.

ip telnet listen-port *start-port [end-port]*

Explanation: If the end port number is not designated, the listening will be executed at a specific port. The number of the designated ports cannot be bigger than 16 and the port number ranges between 3001 and 3999.

● Run the following command to configure the telnet login script.

ip telnet script s1 'login:' switch 'Password:' test

Explanation: When the script is configured, the username prompt and password prompt and their answers must be correctly matched, especially the prompt information is capital sensitive and has inverted comma (''). If one of them is wrongly configured, the automatic login cannot be performed.

Note:

You can add the NO prefix on the above four commands and then run them to cancel previous configuration.

Example

1．ip telnet source-interface s1/0

In this case, the s1/0 interface will be adopted to originate all telnet connections afterwards.

2．ip telnet access-class abc

In this case, all the received telnet connections use access list **abc** to perform the access list check.

3．ip telnet listen-port 3001 3010

Except port 23, all ports from port 3001 to port 3010 can receive the telnet connection.

4．ip telnet script s1 'login:' switch 'Password:' test

The login script **s1** is configured. The username prompt is **login:** and the answer is **switch**. The password prompt is **Password:** and the answer is **test**.

2.1.3   ctrl-shift-6+x (the current connection is mounted)

Run the following command to mount the current telnet connection:

ctrl-shift-6+x

Parameter

None

Default

None

Command mode

Any moment in the current telnet session

Instruction

You can use the shortcut key to mount the current telnet connection at the client side.

Example

switchA>telnet 192.168.20.1
Welcome to Multi-Protocol 2000 Series switch
switchB>ena
switchB#(press ctrl-shift-6+x)
switchA>

You press **ctrl-shift-6+x** to mount the telnet connection to switch B and return to the current state of switch A.

2.1.4 where

Run the following command to check the currently mounted telnet session:

where

Parameter

None

Default

None

Command mode

Global configuration

Instruction

You can use the command to check the mounted outward telnet connection at the client side. The displayed information contains the serial number, peer address, local address and local port.

Note:

The **where** command is different from the **show telnet** command. The former is used at the client side and the displayed information is the outward telnet connection. The latter is used at the server and the displayed information is the inward telnet connection.

Example

    switchA>telnet 192.168.20.1
    Welcome to Multi-Protocol 2000 Series switch
    switchB>ena
    switchB#(Press ctrl-shift-6+x)
    switchA> telnet 192.168.20.2
    Welcome to Multi-Protocol 2000 Series switch
    switchC>ena
    switchC#(Press ctrl-shift-6+x)
    switchA>where
    NO.   Remote Addr   Remote Port   Local Addr   Local Port
     1   192.168.20.1   23   192.168.20.180   20034
     2   192.168.20.2   23   192.168.20.180   20035

Enter where at switch A. The mounted outward connection is displayed.

2.1.5   resume

It is used to resume the currently mounted outward telnet connection:

resume *no*

 Parameter

Parameter	Description
no	Number of the currently mounted telnet session that is checked through the **where** command

Default

None

Command mode

Global configuration

Instruction

The command can be used to resume the currently mounted outward telnet connection at the client side.

Example

    switchA>telnet 192.168.20.1
    Welcome to   Multi-Protocol 2000 Series switch
    switchB>ena
    switchB#(press ctrl-shift-6+x)
    switchA> telnet 192.168.20.2
    Welcome to Multi-Protocol 2000 Series switch
    switchC>ena
    switchC#(press ctrl-shift-6+x)
    switchA>where

NO.	Remote Addr	Remote Port	Local Addr	Local Port
1	192.168.20.1	23	192.168.20.180	20034
2	192.168.20.2	23	192.168.20.180	20035

switchA>Resume 1
  [Resuming connection 1 to 192.168.20.73 . . .]
(enter)
switchB#

After you enter **where** at switch A and the mounted outward connection of switch A is displayed, enter **Resume1**. You will be prompted that connection 1 is resumed. The command prompts of switch B are displayed after the **Enter** key is pressed.

2.1.6   disconnect

The following command is used to clear the currently mounted outward telnet session:

disconnect *no*

Parameter

Parameter	Description
no	Number of the currently mounted telnet session that is checked through the **where** command

Default

None

Command mode

Global configuration

Instruction

The command can be used to clear the currently mounted outward telnet connection at the client side.

Note:

The **disconnect** command is different from the **clear telnet** command. The former is used at the client side and clears the outward telnet connection. The latter is used at the server and clears the inward telnet connection.

Example

switchA>telnet 192.168.20.1
  Welcome to Multi-Protocol 2000 Series switch
switchB>ena
switchB#(press ctrl-shift-6+x)
switchA> telnet 192.168.20.2
  Welcome to Multi-Protocol 2000 Series switch
switchC>ena
switchC#(press ctrl-shift-6+x)
switchA>where

NO.	Remote Addr	Remote Port	Local Addr	Local Port
1	192.168.20.1	23	192.168.20.180	20034

2	192.168.20.2	23	192.168.20.180	20035

switchA>disconnect 1

<Closing connection to 192.168.20.1> <y/n>y

Connection closed by remote host.

switchA>

After you enter **where** at switch A and the mounted outward connection of switch A is displayed, enter **disconnect 1**. You will be prompted whether the connection of switch B is closed. After you enter **Y**, the connection is closed.

2.1.7   switchkey

The following is a command to configure the terminal switch key on the line.

switchkey *key cmdalias server-name*

Parameter

Parameter	Description
key	Compound key can be the **ctrl** key plus any key from A to Z, except the letter **h**.
cmdalias	Alias of the **connect** command
server－name	Name of the remote host, which appears in the switchover prompt and the switchover menu

Default

None

Command mode

Line configuration mode

Instruction

The command is used to configure the terminal switchover key and the corresponding command alias, and the name of the remote host on the line.

Note:

1)   The parameter **cmdalias** must be applied at a correct command.

2)   The parameter **key** cannot be **ctrl-h**.

3)   The parameter **server-name** will appear at the switchover prompt and the switchover menu.

4)   The parameter **autocommand** cannot be configured at the line, or the terminal switchover function is invalid.

Example

switchA>switchkey ctrl-a cona ServerA

The previous command is to configure the switchover key **ctrl-a**. The alias of the used command is **cona**. You switch to Server A.

2.1.8   switchmsg

The following command is used to configure whether the prompt information about the terminal switchover is exported:

switchmsg *enable/disable*

Parameter

Parameter	Description
enable	Exports the terminal switchover prompt.
disable	Do not export the terminal switchover prompt.

Default

disable

Command mode

Line configuration mode

Instruction

The command can be used to decide whether the switchover prompt information is exported when the terminal is switched.

Example

switchA>switchmsg enable

When the terminal is switched, export the switchover prompt information.

2.1.9   sequence-char

The following is a command to configure the terminal switchover key on the line:

sequence-char *key char1 char2 char3 …*

Parameter

Parameter	Description
key	Compound key can be the **ctrl** key plus any key from A to Z, except the letter **h**.
char1 char2 char3 …	Screen character sequence relative to the specific terminal

Default

None

Command mode

Line configuration mode

Instruction

The command can be used to configure the switchover key and the corresponding terminal character sequence on the line.

Note:

1)   The **key** parameter can not be **ctrl-h**.

2)   The character sequence parameter is relative to the detailed terminal. You can find it by checking the terminal manual.

3)   The character sequence parameter must be a hex value and starts from 0x. Each character is differentiated by space.

Example

Switch_config_line# sequence-char ctrl-a 0x1b 0x21 0x38 0x51

Set the character sequence of the switchover key **ctrl-a** to **0x1b 0x21 0x38 0x5**.

For other commands about **alias** and **async**, refer to relative configuration explanation.

Application Example:

The switch is configured as follows:

```
…
…
…
interface Serial1/1
  physical-layer mode async
  no ip directed-broadcast
  async mode interactive
line tty 1
switchkey       CTRL-U        cona        ServerA
 sequence-char   CTRL-U               0x1b 0x21 0x38 0x51
 switchkey       CTRL-V        conb        ServerB
 sequence-char   CTRL-V               0x1b 0x21 0x39 0x51
 switchkey       CTRL-W        conc        ServerC
 sequence-char   CTRL-W         0x1b 0x21 0x31 0x30 0x51
 switchmsg enable
…
...
alias cona connect 192.168.20.1
alias conb connect 192.168.20.2
alias conc connect 192.168.20.3
```

When all the configurations are complete and the connection is established, open the terminal. The switchover menu automatically appears. After you press **CTRL-U**, the system automatically switches to server A and exports the prompt information about server A. After you press **CTRL-V**, the system automatically switches to server B on the new screen and exports the prompt information about server B. After you press **CTRL-W**, the system automatically switches to server C on the new screen and exports the prompt information about server C. If you press **CTRL-**, the switchover menu appears on the current screen and add the asterisk mark (*) behind the current server.

The following is a result after you press **CTRL-**:

```
=====================================
```
Terminal Switch Menu
1)	CTRL-U	ServerA	*
2)	CTRL-V	ServerB	
3)	CTRL-W	ServerC	

Note:

4) During multiple connection operations, if the system exits from one connection, the system will take the first connection as the current connection and the interface of the first host will appear. If the system has already exited from the first connection, it will take the second connection as the current connection and the interface of the second host will appear.

5) After all services are complete, you are recommended to directly shut down the terminal no matter how many connections are currently open.

6) Before other connections exit, you'd better not enable the system to exit from the first connection.

7) Try not to exit from a connection during operations. Switching connections is a better choice. After all operations are completer, shut down the terminal.

8) During terminal switchover, the functions to mount and resume the connection by pressing **ctrl-shift-6+x** are forbidden.

2.1.10 clear telnet

The following is a command format to clear the telnet session at the server:

clear telnet *no*

Parameter

Parameter	Description
no	Number of the telnet session that is displayed after the **show telnet** command is run

Default

None

Command mode

Management mode

Instruction

The command is used to clear the telnet session at the server.

Example

clear telnet 1

The telnet session whose sequence number is 1 is cleared at the server.

2.1.11 show telnet

The following is a command format to display the telnet session at the server:

show telnet

Parameter

None

Default

None

Command mode

All command modes except the user mode

Instruction

The command is used to display the telnet session at the server. The displayed information includes the sequence number, peer address, peer port, local address and local port.

Example

Switch# show telnet

If you run the previous command, the result is shown as follows:

NO.	Remote Addr	Remote Port	Local Addr	Local Port
1	192.168.20.220	1097	192.168.20.240	23
2	192.168.20.180	14034	192.168.20.240	23

2.1.12 debug telnet

The following is a format of the **debug** command for the telnet session:

debug telnet

Parameter

None

Default

None

Command mode

Management mode

Instruction

The command is used to open the switch of the telnet debug.

If the switch of the telnet debug is opened, the negotiation processes of all the incoming telnet sessions are printed on the window that the debug command invokes. The

debug telnet command is different from the **telnet debug** command. The former is to export the debug information of the telnet session connected to the server. The latter is to export the debug information of the telnet session that the client originates.

Example

debug telnet

The debug information of the telnet session that is connected to the server is displayed.

2.2   Terminal Configuration Command

The following are terminal configuration commands:

- attach-port
- autocommand
- clear line
- connect
- disconnect
- exec-timeout
- length
- line
- location
- login authentication
- monitor
- no debug all
- password
- printer enable
- printer start
- printer stop
- resume
- script activation
- script callback
- script connection
- script dialer
- script reset
- script startup
- sequence-char
- show debug
- show line
- show tty-status
- switchkey
- switchmsg

- terminal-type
- terminal monitor
- terminal width
- terminal length
- where
- width

2.2.1 attach-port

The following command is to bind the telnet listening port to the **line vty** number and enable the telnet connection at a specific port generates **vty** according to the designated sequence number.

[no] attach-port *PORT*

Parameter

Parameter	Description
port	Listening port of the telnet server (3001-3999)

Default

None

Command mode

Line configuration mode

Example

Bind listening port 3001 to line vty 2 3.

switch_config# line vty 2 3
switch_config_line#attach-port 3001

2.2.2 autocommand

It is used to set the automatically-run command when user logs in to the terminal. The connection is cut off after the command is executed.

autocommand *LINE*

no autocommand

Parameter

Parameter	Description
LINE	Command to be executed

Command mode

Line configuration mode

Example

switch_conf#line vty 1
switch_conf_line#autocommand pad 123456

After you successfully log in, the host whose X.121 address is 123456 will be automatically padded.

2.2.3   clear line

It is to clear the designated line.

clear line [*aux | tty | vty*] [*number*]

Parameter

Similar to the **line** command

Command mode

Management mode

Example

switch#clear line vty 0

2.2.4   connect

It is to connect the telnet server.

connect *server-ip-addr*/*server-host-name* {[/**port** *port*][/**source-interface** *interface*] [/**local** *local-ip-addr*]}

Parameter

Parameter	Description
server-ip-addr/server-host-name	IP address of the server or the host name of the server
port	Port number
interface	Name of the interface where the connection is originated
local-ip-addr	Local IP address where the connection is originated

Command mode

All configuration modes

Example

switch# connect 192.168.20.1

2.2.5   disconnect

It is used to delete the mounted telnet session.

disconnect *N*

Parameter

Parameter	Description
N	Number of the mounted telnet session

Command mode

All configuration modes

Example

switch#disconnect 1

2.2.6 exec-timeout

It is to set the maximum spare time for the terminal.

[**no**] **exec-timeout** [*time*]

Parameter

Parameter	Description
time	Spare time whose unit is second

Default

0 (No time-out limitation)

Command mode

Line configuration mode

Example

Set the spare time of the line to one hour.

switch_config_line#exec-timeout 3600

2.2.7 length

It is used to set the line number on the screen of the terminal.

[**no**] **length** [*value*]

Parameter

Parameter	Description
value	A value between 0 and 512 The value **0** means there is no pause.

Default

24

Command mode

Line configuration mode

2.2.8   line

It is used to enter the line configuration mode.

line [**aux | console | tty | vty**] [*number*]

Parameter

Parameter	Description
aux	Auxiliary line, which has only one number **0**
console	Monitoring line, which has only one number **0**
tty	Asynchronous line
vty	Virtual lines such as Telnet, PAD and Rlogin
number	Number in the line of the type

Command mode

Global configuration

Example

The following example shows how to enter the line configuration mode of VTY 0 to 10.

switch_config#line vty 0 10

2.2.9   location

It is used to recoded the description of the current line.

location [*LINE*]

no location

Parameter

Parameter	Description
LINE	Description of the current line

Command mode

Line configuration mode

2.2.10   login authentication

It is used to set line login authentication:

[**no**] **line login authentication** [**default** | *WORD*]

Parameter

Parameter	Description
default	Default authentication mode
WORD	Name of the authentication list

Command mode

Line configuration mode

Example

switch_conf_line#login authentication test

In the example, the authentication list of the line is set to **test**.

2.2.11   monitor

It is used to export the log and debugging information to the line:

[**no**] **monitor**

Parameter

None

Command mode

Line configuration mode

Example

switch_config_line#monitor

2.2.12   no debug all

It is used to shut down all debugging output of the current VTY:

no debug all

Parameter

None

Command mode

Management mode

Example

switch#no debug all

2.2.13　password

It is used to set the password for the terminal:

password {*password* | [encryption-type] *encrypted-password* }

no password

Parameter

Parameter	Description
password	Password configured on the line, which is entered in the plaintext form and whose maximum length is 30 bits.
[encryption-type] *encrypted-password*	**encryption-type** means the encryption type of the password. Currently, products only support two encryption modes: 0 and 7. The number **0** means the password is not encrypted and the plaintext of password is directly entered. It is the same as the way of directly entering the password. The number **7** means the password is encrypted through an algorithm defined by. You need to enter the encryption text for the encrypted password. The encryption text can be copied from the configuration files of other switches.

For password encryption, refer to the explanation of the commands **service *password-encryption*** and **enable password**.

Command mode

✧ Line configuration mode

Example

switch_conf#line vty 1
switch_conf_line#password test

The previous example shows the login password of VTY1 is set to **test**.

2.2.14　resume

It is used to resume the mounted telnet session:

resume *N*

Parameter

Parameter	Description
N	Number of the mounted telnet session

Command mode

All configuration modes

Example

switch#resume 1
s

2.2.15　switchkey

It is used to configure the terminal switchover key:

switchkey *key cmdalias server-name*

Parameter

Parameter	Description
key	Terminal switchover key, ranging from CTRL-A to CTRL-Z except CTRL-H
cmdalias	Alias of the command that is executed when terminal switchover is performed
server-name	Server name of each terminal's screen corresponds to

Command mode

Line configuration mode

Example

The following example shows how to connect to the **sco1** server by the **con_sco** command when the switchover is performed through pressing **ctrl-a**:

switch_config_line#switchkey ctrl-a con_sco sco1

2.2.16　sequence-char

It is used to configure the character sequence of terminal call-back when the terminal is switched:

sequence-char *key char1 char2 char3 …*

Parameter

Parameter	Description
key	Terminal switchover key
char1 char2 char3 …	Character sequence for call-back

Command mode

Line configuration mode

Example

The following example shows how to configure the character sequence of terminal call-back to **0x1b 0x21 0x38 0x51** when the terminal is switched.

switch_config_line#sequence-char ctrl-a 0x1b 0x21 0x38 0x51

2.2.17   show debug

It is used to display all debugging information of the current VTY:

show debug

Parameter

None

Command mode

Management mode or global configuration mode

Example

Switch# show debug
http authentication debug is on
http cli debug is on
http request debug is on
http response debug is on
http session debug is on
http erro debug is on
http file debug is on
TELNET:
Incoming Telnet debugging is on

2.2.18   show line

It is used to display the status of the current effective line:

show line {[**console** | **aux** / **tty** / **vty**] [*number*]}

Parameter

✧ If there is no parameter followed, the status of all effective lines will be displayed.

The definition of other parameters is similar to that of the **line** command.

Command mode

All configuration modes except the user mode

2.2.19   switchmsg

It is used to decide whether the prompt information is displayed when the terminal is switched:

switchmsg enable

switchmsg disable

Parameter

Parameter	Parameter
enable	Displays the prompt information when the terminal is switched.
disable	Does not display the prompt information when the terminal is switched.

Default

disable

Command mode

Line configuration mode

Example

The following example shows how to display the prompt information when the terminal is switched:

switch_config_line#switchmsg enable

2.2.20   terminal length

It is used to change the line number on the current terminal screen. The parameter can be obtained by the remote host. The rlogin protocol uses the parameter to notify the remote UNIX host. Run the **no terminal length** command to resume the default value:

terminal length *length*

no terminal length

Parameter

Parameter	Description
length	Line number displayed on each screen

Default

Pause when 24 lines are displayed on the screen.

Command mode

Global configuration

Instruction

The command is effective only to the current terminal. When the session is complete, the terminal attribute is invalid.

Example

switch#terminal length 40

Relative command

> **line**

2.2.21   terminal monitor

It is used to display the debugging output information and system faulty information at the current terminal. The negative form of the command is used to disable the monitoring:

> **terminal monitor**
>
> **no terminal monitor**

Parameter

> None

Default

> The system monitoring port (console) is open by default. Other terminals are closed by default.

Command mode

> Global configuration

Instruction

> The command is effective only to the current terminal. When the session is complete, the terminal attribute is invalid.

Example

> switch#terminal monitor

Relative command

> **line**
>
> **debug**

2.2.22   terminal width

In default settings, the switch is to export 80 characters in each line. If the default settings cannot meet your requirements, you can reset it. The parameter can be obtained by the remote host. Run the **terminal width** command to set the character number in each line. Run the **no terminal width** command to resume to the default value.

> **terminal width** *number*
>
> **no terminal width**

Parameter

Parameter	Description
number	Character number of each line

Default

80 characters in each line

Command mode

Global configuration

Instruction

The command is effective only to the current terminal. When the session is complete, the terminal attribute is invalid.

Example

switch#terminal width 40

Relative command

line

2.2.23   terminal-type

It is used to set the terminal type:

[**no**] **terminal-type** [*name*]

Parameter

Parameter	Description
name	Terminal name Terminal types currently supported are VT100, ANSI and VT100J.

Default

ANSI

Command mode

Line configuration mode

Chapter 3   Network Management Configuration Commands

3.1   SNMP Commands

The following are SNMP commands:

- snmp-server community
- snmp-server contact
- snmp-server host
- snmp-server location
- snmp-server packetsize
- snmp-server queue-length
- snmp-server trap-source
- snmp-server trap-timeout
- snmp-server view
- show snmp
- debug snmp

3.1.1   snmp-server community

Run the command **snmp-server community** in global configuration mode to permit accessing the community character string of SNMP. Use the negative form of the command to delete the designated community character string.

snmp-server community *string* [**view** *view-name*] [**ro | rw**] [*word*]

no snmp-server community *string*

Parameter

Parameter	Description
string	Community character string to access SNMP as the password does
view view-name	View name that is predefined (optional) The view defines the MIB objects effective to the community.
ro	Designates the read-only permission (optional). The authorized management station can only read MIB objects.
rw	Designates the read-write permission (optional). The authorized management station can read and modify MIB objects.
word	Designates the access list name of the SNMP agent which can be accessed through the community character string.

Default

The SNMP community character string can only read all objects.

Command mode

Global configuration

Instruction

If no parameter is followed, the configuration information of all community character strings are listed.

Example

The following example shows how to distribute the character string **comaccess** to the SNMP, how to permit the read-only access and how to designate the IP access list **allowed** to use the community character string:

snmp-server community comaccess ro allowed

The following example shows how to distribute the character string **mgr** to the SNMP, how to permit the read-write access to the objects in the **restricted** view:

snmp-server community mgr view restricted rw

In the following example, the community **comaccess** is deleted:

no snmp-server community comaccess

Relative command

access-list

snmp-server view

3.1.2   snmp-server contact

Run the command **snmp-server contact** in global configuration mode to set the **sysContact** information of the management node. Run the negative form of the command to delete the **sysContact** information.

snmp-server contact *text*

no snmp-server contact

Parameter

Parameter	Description
text	Character string of the **sysContact** information of the node

Default

The **sysContact** information of the node is not set.

Command mode

Global configuration

Instruction

It corresponds to the sysContact value of the MIB variable in the system group.

Example

The following is an example of the node contact:

snmp-server contact Dial_System_Operator_at_beeper_#_27345

3.1.3   snmp-server host

Run the command **snmp-server host** in global configuration mode to designate the receiver of SNMP trap operation. Run the command **no snmp-server host** to cancel the designated host.

snmp-server host *host community-string [trap-type]*

no snmp-server host *host*

Parameter

Parameter	Description
host	Host name or internet address
community-string	Password-like community string sent with the trap operation
trap-type	If no trap is designated, all traps will be sent to the host.
	Authentication: allowing to send the traps with wrong authentication
	Configure: allowing to send SNMP-configure traps
	Snmp: allowing to send all SNMP traps

Default

The command is invalid by default. The trap is not sent. If the command with keyword is not entered, all traps are sent by default.

Command mode

Global configuration

Instruction

If the **snmp-server host** command is not entered, the trap is not sent. To configure the switch to send SNMP traps, you need to run the **snmp-server host** command. If the command without the keyword **trap-type** is entered, all types of traps of the host are activated. If the command with the keyword **trap-type** is entered, you can designate multiple trap types in each host.

When you specify multiple **snmp-server host** commands at the same host, the SNMP trap information sent to the host will be filtered according to the character string and the trap type in the command. To the same host and the community character string, only one trap type can be configured.

The usability of the option *trap-type* depends on the switch type and the characteristics of the routing software supported by the switch.

Example

In the following example, the SNMP trap defined by RFC1157 to the host whose IP address is 10.20.30.40. The community character string is **comaccess**.

snmp-server host 10.20.30.40 comaccess snmp

In the following example, the switch uses the community character string public to send all types of traps to the host whose IP address is 10.20.30.40.

snmp-server host 10.20.30.40 public

In the following example, only **authentication** traps are valid and can be sent to host **bob**.

snmp-server host bob public authentication

Relative command

snmp-server queue-length

snmp-server trap-source

snmp-server trap-timeout

3.1.4   snmp-server location

Run the command **snmp-server location** in global configuration mode to set the character string of the node location. Run the negative form of the command to delete the location character string.

snmp-server location *text*

no snmp-server location

Parameter

Parameter	Description
text	Describes the character string of the node location.

Default

The character string of the node location is not set.

Command mode

Global configuration

Instruction

It corresponds to the value of **sysLocation** of the MIB variable in the **system** group.

Example

In the following example, the actual location of the switch is defined:

snmp-server location Building_3/Room_214

Relative command

snmp-server contact

3.1.5   snmp-server packetsize

Run the command **snmp-server packetsize** in global configuration mode to define the maximum SNMP packet size when the SNMP server receives the request or generates the response:

snmp-server packetsize *byte-count*

no snmp-server packetsize

Parameter

Parameter	Description
byte-count	Integer byte ranging between 484 and 17940 The default value is 3000 bytes.

Default

3000 bytes

Command mode

Global configuration

Instruction

It corresponds to the value of sysLocation of the MIB variable in the system group.

Example

In the following example, a filter is created for the packet with maximum length of 1024 bytes:

snmp-server location Building_3/Room_214

Relative command

snmp-server queue-length

3.1.6   snmp-server queue-length

Run the command **snmp-server queue-length** in global configuration mode to set the queue length for each trap host:

snmp-server queue-length *length*

Parameter

Parameter	Description
length	Trap event number that can be saved in the queue (1～1000)

Default

10 events

Command mode

Global configuration

Instruction

The command is used to define the queue length for each trap host. Once the trap message is successfully transmitted, the switch will clear the queue.

Example

The following example shows that a message queue that can capture four events is created.

snmp-server queue-length 4

Relative command

snmp-server packetsize

3.1.7　snmp-server trap-source

Run the command **snmp-server trap-source** in global configuration mode to designate a source address of an interface for all traps. Run **no snmp-server trap-source** to delete the interface with such a source address.

snmp-server trap-source *interface*

no snmp-server trap-source

Parameter

Parameter	Description
interface	Interface where the SNMP trap occurs It contains the interface type with specific platform syntax mode and the sequence number.

Default

No interface is designated.

Command mode

Global configuration

Instruction

When the SNMP server sends the SNMP trap, the SNMP trap has a trap address no matter from which interface it is sent out. If you want use the trap address to track the trap, you can use the command.

Example

The following example shows that the address of the Ethernet's 1/0 interface is designated as the source address of all traps.

snmp-server trap-source ethernet 1/0

The following example shows that the IP address of the Ethernet's 1/0 interface is designated as the source address of all traps.

snmp-server trap-source ethernet 1/0

Relative command

snmp-server queue-length

snmp-server host

3.1.8 snmp-server trap-timeout

Run the command **snmp-server trap-timeout** in global configuration mode to define the timeout value of resending the trap message.

snmp-server trap-timeout *seconds*

Parameter

Parameter	Description
seconds	An interval integer from 1 to 1000 (unit: second), which is set for resending the message

Default

30 seconds

Command mode

Global configuration

Instruction

Before the switch software sends the trap, it will look for the route of the destination address. If there is no route, the trap is stored in the resending queue. The command **server trap-timeout** decides the interval for resending the trap.

Example

The following example shows the trap message at the resending queue will be resent after an interval of 20 seconds:

snmp-server trap-timeout 20

Relative command

snmp-server host

snmp-server queue-length

3.1.9 snmp-server view

Run the command **snmp-server view** in global configuration mode to create or update an MIB view. Run the command **no snmp-server view** to delete a view of the SNMP server.

snmp-server view *view-name oid-tree* {*included | excluded*}

no snmp-server view *view-name*

Parameter

Parameter	Description
view-name	Updates or creates a logo of the view.
oid-tree	Object identifier of the ASN.1 sub-tree contained or declined by the view Identify the sub-tree, specify a character string containing numbers, such as 1.3.6.2.4 or a **system** sub-tree. The sub-tree name can be the name which can be found in the MIB tree.
included excluded	Type of the view The parameter **included** or **excluded** must be designated.

Default

None

Command mode

Global configuration

Instruction

If other SNMP commands need a view as a parameter, you can run the command to create a view to take as the parameter of these SNMP commands. In default settings, the view need not be defined. You can see all objects, which is similar to the **everything** view predefined by Cisco. You can use the command to define the objects that can seen from the view.

Example

The following example shows that the views of all objects in the MIB-II sub-tree are created:

snmp-server view mib2 mib-2 included

The following example shows that the views of all objects in the **system** group are created:

snmp-server view phred system included

The following example shows that the views of all objects in the **system** group are created, while all objects in sysServices.7 and in the No.1 interface of the interface group are excluded.

snmp-server view agon system included
snmp-server view agon system.7 excluded

Relative command

snmp-server community

3.1.10   snmp-server udp-port

To designate a port in global mode to be a destination port to which all traps are sent, run the following first command. To cancel this destination port, run the following second command.

snmp-server trap-source *interface*

no snmp-server trap-source

Parameter

Parameter	Description
udp-port	Stands for the ID of the destination port to which SNMP traps are sent, which cannot be a command port ID.

Default value

The default trap destination port is port 162.

Command mode

Global configuration mode

Instruction

When the SNMP traps are transmitted from the SNMP server, you can run this command to designate an ID for the special destination port.

Example

The following example shows how to designate all traps to be sent to port 1234 of a host.

snmp-server udp-port 1234

Related command

snmp**-server host**

3.1.11   snmp-server source-addr

Run the command **snmp-server source-addr** in global configuration mode to designate a source address for the SNMP message. Run the command **no snmp-server source-addr** to disable the designated function.

snmp-server source-addr *ipaddress*

no snmp-server source-addr

Parameter

Parameter	Description

ipaddress	Designates the source address where the SNMP generates the message. The parameter is the set IP address of the device.

Default

The interface is not designated.

Command mode

Global configuration

Instruction

The command is used to configure the source address of the SNMP message.

Example

The following example shows that the IP address of the Ethernet's 1/0 interface is designated as the source address of all SNMP messages.

snmp-server source-addr 192.168.213.15

Relative command

None

3.1.12   snmp-server group

Run the command **snmp-server group** in global configuration mode to create or update an SNMP group. Run the command **no snmp-server group** to delete a group.

snmp-server   group [*groupname* {**v1 | v2c |v3 [auth | noauth | priv**]}][**read** readview][**write** writeview] [**notify** notifyview] [**access** access-list]

Parameter

Parameter	Description
groupname	Name of the created or modified group
v1|v2|v3	SNMP protocol version number of the group
auth|noauth|priv	Lowest security level of users in the SNMPv3 group
readview	Access permission for GET operations, which is defined in the view form
writeview	Access permission for SET operations, which is defined in the view form
notifyview	Access permission when the trap message is sent, which is defined in the view form
access-list	IP access list that allows users in the group to get through

Default

Readview allows all leafs in the Internet sub-trees can be accessed.

Command mode

Global configuration

Instruction

The SNMP group is used to designate the access permission for users in the group.

Example

In the following example, an SNMP group is configured. The name of the SNMP group is set to **setter**. The SNMP version is version 3. The security level is authentication and encryption. The view of the **set** operations is **v-write**.

snmp-server group setter v3 priv write v-write

Relative command

snmp-server view

snmp-server user

3.1.13   snmp-server user

Run the command **snmp-server group** in global configuration mode to create or update an SNMP user. Run the command **no snmp-server group** to delete a user. When a remote IP address is specified, it means that a remote user is configured. When you configure a remote user, the engine ID of SNMP corresponding to the IP address of the management station must already exist. The format of the command is shown in the following:

snmp-server user *username groupname* **[remote** *ip-address* **[udp-port** *port*]] {v1 | v2c | v3 [encrypted] [auth {md5 | sha}** *auth-password* **]}[access** *access-list*]

Parameter

Parameter	Description
username	Name of the created or modified user
groupname	Group that users belong to
ip-address	IP address of the SNMP management station required when the remote user is created When the remote user is not specified, it stands for the local user.

port	UDP port of the SNMP management station where the remote user is located The default port is port 162.
auth-password	Authentication password of the user After the password is localized, it is used as the authentication and encryption key of SNMPv3.
access-list	IP access list that allows the user to get through

Default

The value of **portDefault** is 162, that is, it is the port in SNMP where the Trap message is received.

Command mode

Global configuration

Instruction

It is used to set the user name and password.

Example:

In the following example, an SNMP user is configured. Its name is set to **set-user**. It belongs to the **setter** group. The SNMP version is version 3. The security level is authentication and encryption. The password is 12345678. MD5 is used as the hash algorithm.

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

Relative command:

snmp-server view

snmp-server group

3.1.14 snmp-server engineID

Run the command **snmp-server engineID** in global configuration mode to configure an ID for the SNMP engine. Use the negative form of the command to delete an ID of the SNMP engine. When the remote IP address is specified, it means the ID of the SNMP engine need be configured. The following is the format of the command:

snmp-server engineID { remote *ip-address* **[udp-port** *port-number***] | local }** *engineid-string*

Parameter

Parameter	Description

ip-address	IP address of the SNMP management station where the remote engine is located, which need be created when the remote engine is created
port-number	UDP port number of the SNMP management station where the remote engine is located, which need be created when the remote engine is created The default value is 162.
engineid-string	Character string of the remote SNMP engine ID It must be a hex character string with no more than 32 characters.

Default

The value of **port-numberDefault** is 162, that is, the interface of SNMP where the Trap message is received.

Command mode

Global configuration

Instruction

It is used to set the ID for the remote or local SNMP engine. When the ID of the remote SNMP engine is deleted, no SNMP user or message-received host uses the IP address and the port number that the ID corresponds to.

Example

The following command shows that an SNMP engine ID is configured for the remote host 90.0.0.3:

snmp-server engineID remote 90.0.0.3 80000523015a000003

Relative command:

snmp-server host

snmp-server user

3.1.15 snmp-server encryption

TO display the configured SNMP community, the SHA encryption password and the MD5 encryption password, run **snmp-server encryption** in global mode. This command is a once-for-all command, which cannot be saved or canceled by its negative form.

snmp-server encryption

Parameter

None

Default value

The default settings is to display the SNMP community, the SHA encryption password and the MD5 encryption password in plain text.

Command mode:

Global configuration mode

Instruction

This command is used to display the SNMP community, the SHA encryption password and the MD5 encryption password in plain text.In this way, the security of the password is guaranteed.

Example

The following example shows how to show in the plain text the SNMP community, the SHA encryption password and the MD5 encryption password, which are set for host 90.0.0.3.

snmp-server encryption

Related command

snmp-server community

snmp-server user

3.1.16   show snmp

Run the command **show snmp** to monitor the SNMP input or output statistics, including the incorrect community character string, the number of faults and requests.

Run the command **show snmp host** to display information about the SNMP trap host.

Run the command **show snmp view** to display the information about SNMP views. The following is the format of the command:

show snmp [*host | view*]

Parameter

Parameter	Description
host	Displays information about the SNMP trap host.
view	Displays the information about SNMP views.

Default

None

Command mode

Management mode,Global configuration

Instruction

Run the command **show snmp** to monitor the SNMP input or output statistics.

Run the command **show snmp host** to display information about the SNMP trap host.

Run the command **show snmp view** to display the information about SNMP views.

Example

The following example shows that the SNMP input or output statistics is listed out:

#**show snmp**
37 SNMP packets input
0 Bad SNMP version errors
4 Unknown community name
0 Illegal operation for community name supplied
0 Snmp encoding errors
24 Number of requested variables
0 Number of altered variables
0 Get-request PDUs
28 Get-next PDUs
0 Set-request PDUs
78 SNMP packets output
0 Too big errors (Maximum packet size 1500)
0 No such name errors
0 Bad values errors
0 General errors
24 Get-response PDUs PDUs
13 SNMP trap PDUs

The fields for the SNMP Agent to send and receive the message statistics information are shown as follows:

Field	Meaning
Unknown community name	Community name that can not be recognized
Illegal operation for community name supplied	Incorrect operation
Encoding errors	Errors that occurs in encoding
Get-request PDUs	Get-request message
Get-next PDUs	Get-next message
Set-request PDUs	Set-request message
Too big errors	Response message is too big to be generated.
No such name errors	No specified instance exists.
Bad values errors	The value type is wrongly set.
General errors	Common errors
Get-response PDUs	Get-response message

Trap PDUs	SNMP trap message

In the following example, the information about the SNMP trap message is displayed:

#show snmp host
Notification host: 192.2.2.1   udp-port: 162   type: trap
user: public   security model: v1

In the following example, information about SNMP views is displayed:

#show snmp view
mib2   mib-2   -   included   permanent   active

Relative command

snmp-server host

snmp-server view

3.1.17   debug snmp

It is used to display the SNMP event, message sending and receiving, and errors:

debug snmp [*error | event | packet*]

Run the command **no debug snmp** to stop displaying information.

Parameter

Parameter	Description
error	Enables the debug switch of the SNMP errors.
event	Enables the debug switch of SNMP events.
packet	Enables the debug switch of SNMP incoming or outgoing message.

Command mode

Management mode

Instruction

After the switch of the SNMP debugging information is enabled, SNMP events and information about message sending and receiving are exported. The exported information helps to diagnose SNMP faults.

Example

The following example shows how to debug SNMP message receiving and sending:

switch#debug snmp packet
Received 49 bytes from 192.168.0.29:1433
0000: 30 82 00 2D   02 01 00 04   06 70 75 62   6C 69 63 A0   0..-.....public.
0016: 82 00 1E 02   02 7D 01 02   01 00 02 01   00 30 82 00   .....}.......0..

```
0032: 10 30 82 00   0C 06 08 2B   06 01 02 01   01 03 00 05    .0.....+........
0048: 00                                         .
Sending 52 bytes to 192.168.0.29:1433
0000: 30 82 00 30   02 01 00 04   06 70 75 62   6C 69 63 A2    0..0.....public.
0016: 82 00 21 02   02 7D 01 02   01 00 02 01   00 30 82 00    ..!..}.......0..
0032: 13 30 82 00   0F 06 08 2B   06 01 02 01   01 03 00 43    .0.....+.......C
0048: 03 00 F4 36                                ...6
Received 51 bytes from 1192.168.0.29:1434
0000: 30 82 00 2F   02 01 00 04   06 70 75 62   6C 69 63 A0    0../.....public.
0016: 82 00 20 02   02 6B 84 02   01 00 02 01   00 30 82 00    .. ..k.......0..
0032: 12 30 82 00   0E 06 0A 2B   06 01 02 01   02 02 01 02    .0.....+........
0048: 01 05 00                                   ...
Sending 62 bytes to 192.168.0.29:1434
0000: 30 82 00 3A   02 01 00 04   06 70 75 62   6C 69 63 A2    0..:.....public.
0016: 82 00 2B 02   02 6B 84 02   01 00 02 01   00 30 82 00    ..+..k.......0..
0032: 1D 30 82 00   19 06 0A 2B   06 01 02 01   02 02 01 02    .0.....+........
0048: 01 04 0B 45   74 68 65 72   6E 65 74 30   2F 31          ...Ethernet0/1
```

Field	Description
Received	SNM receives message.
192.168.0.29	Source IP address
1433	Port number of the source address
51 bytes	Length of the received message
30 82 00 2D 02 01 00 04 06 70 75 62 6C 69 63 A0 82 00 1E 02 02 7D 01 02 01 00 02 01 00 30 82 00 10 30 82 00 0C 06 08 2B 06 01 02 01 01 03 00 05 00	Message after being encoded by SNMP ASN
0..-.....public. .....}.......0.. .0.....+........ .	Presentation of the ASCII code which is used to receive message Content that is not in the scope of ASCII code is presented by the full stop.
sending	SNMP sends message.
192.168.0.29	Destination IP address
1433	Port number of the destination address
52 bytes	Length of the sent message
30 82 00 30 02 01 00 04 06 70 75 62 6C 69 63 A2 82 00 21 02 02 7D 01 02 01 00 02 01 00 30 82 00 13 30 82 00 0F 06 08 2B 06 01 02 01 01 03 00 43 03 00 F4 36	Message encoded by SNMP ASN
0..0.....public. ..!..}.......0.. .0.....+.......C	Presentation of the ASCII code which is used to receive message Content that is not in the scope

...6	of ASCII code is presented by the full stop.

The following example shows how to debug the SNMP event:

```
switch#debug snmp event
Received SNMP packet(s) from 192.2.2.51
  SNMP: GETNEXT request
   -- ip.ipReasmFails.0
  SNMP: Response
   >> ip.ipFragOKs.0 = 1
Received SNMP packet(s) from 192.2.2.51
  SNMP: GETNEXT request
   -- ip.ipFragOKs.0
  SNMP: Response
   >> ip.ipFragFails.0 = 0
Received SNMP packet(s) from 192.2.2.51
  SNMP: GETNEXT request
   -- ip.ipFragFails.0
  SNMP: Response
     >> ip.ipFragCreates.0 = 2
```

Field	Description
SNMP	SNMP is currently being debugged.
GETNEXT request	**getnext** request of SNMP
RESPONSE	SNMP response
--	Receiving message
>>	Sending message
ip.ipReasmFails.0	MIB OID that requires to be accessed
ip.ipFragOKs.0 = 1	Accessed MIB OID and the returned value

3.2   Configuring RMON Commands

The following are RMON configuration commands:

- rmon alarm
- rmon event
- rmon collection stat
- rmon collection history
- show rmon

3.2.1   rmon alarm

Command description

Run the following command to configure a rmon alarm item:

rmon   alarm *index variable interval* {absolute | delta} rising-threshold *value* [*eventnumber*] **falling-threshold** *value* [*eventnumber*] [owner *string*]

Parameter

Parameter	Description
variable	Objects that need be monitored Value range: oid of the monitored objects
interval	Interval for the sampling Value range: 1-4294967295 seconds
value	Alarm threshold Value range: -2147483648-2147483647
eventnumber	Index of the event that is triggered when the threshold is reached Value range: 1-65535
string	Holder description information Value range: 1-127 characters

Default

eventnumberDefault is not set.

Instruction

The command is configured in global configuration mode. It is used to monitor the value of the designated object. When the value exceeds the threshold, the specified event is triggered.

Example

In the following example, an alarm item is configured. The monitored object is **ifInOctets.2**. The sampling interval is 10. When the rising threshold value exceeds 15, event 1 is triggered. When the falling threshold value exceeds 25, event 2 is triggered.

rmon alarm 1 1.3.6.1.2.1.2.2.1.10.2 10 absolute rising-threshold 15 1 falling-threshold 25 2 owner switch

3.2.2   rmon event

Command description

It is used to configure an **rmon** event item:

rmon event *index* [description *des-string*] [log] [owner *owner-string*] [trap *community*]

Parameter

Parameter	Description
index	Index of the event item Value range: 1-65535
des-string	Character string of event description Value range: 1-127 characters
owner-string	Character string of event description

	Value range: 1-127 characters
community	Community name when the trap is generated Value range: 1-127 characters

Default

None

Instruction

It is used to configure an **rmon** event item for alarm usage.

Example

In the following example, an **rmon** event item is configured. The index is **6**. The description character string is **example**. When the event is triggered, items will be added to the log table and the trap will be generated by taking **public** as the community name.

rmon event 6 log trap public description example owner switch

3.2.3   rmon collection stat

Command description

rmon collection stat   *index* [*owner string*]

The previous command is used to configure the **rmon** statistics function

Parameter

Parameter	Description
index	Index of the statistics table Value range: 1-65535
string	Character string for the owner Value range: 1-127 characters

Default

None

Instruction

It is configured in interface mode and used for the statistics on the interface.

Example

In the following example, the statistics function is enabled on interface 8 of fast Ethernet.

int f 0/8
rmon collection stats 2 owner switch

3.2.4 rmon collection history

Command description

rmon collection history *index* [**buckets** *bucket-number*] [**interval** *second*] [**owner** *owner-name*]

The previous command is used to configure a history control item.

Parameter

Parameter	Description
index	Its value ranges from 1 to 65535.
bucket-number	Among the data collected in the history control table, the latest **bucket-number** items are saved. Value range: 1-65535
second	Interval, whose value ranges from 1 to 3600
owner-name	Character string of the owner Value range: 1-127 characters

Default

The value of **bucket-numberDefault** is 50. The value of **secondDefault** is 1800.

Instruction

It is configured in interface mode and used for adding an item to the history control table.

Example

In the following example, the history control item is added to interface 8 of fast Ethernet. The statistics data in the latest 20 intervals is saved. The interval is 20 seconds.

```
int f 0/8
rmon collection history 2 buckets 20 interval 10 owner switch
```

3.2.5 show rmon

Command description

show rmon [**alarm**] [**event**] [**statistics**] [**history**]

The previous command is used to display the **rmon** configuration.

Parameter

None

Default

None

Instruction

It is used to display the **rmon** configuration.

Example

In the following example, the rmon configuration is displayed.

show rmon

Chapter 4   Maintenance and Debugging Tool Commands

4.1   Network Testing Tool Commands

4.1.1   ping

It is used to test host accessibility and network connectivity. After the **ping** command is run, an ICMP request message is sent to the destination host, and then the destination host returns an ICMP response message.

ping [**-f**] [**-i** {source-ip-address | source-interface}] [**-j** host1 [host2 host3 …]]   [**–k** host1 [host2, host3 …]] [**-l** length] [**-n** number] [**-r** hops] [**-s** tos] [**-t** ttl] [**-v**] [**-w** *waittime*] **host**

Parameter

Parameter	Description
-f	Sets the DF digit (message is not segmented).
	If the message required to be sent is larger than the MTU of the path, the message will be dropped by the routing switch on the path and the routing switch will then return an ICMP error message to the source host. If network performance has problems, one node in the network may be configured to a small MTU. You can use the **–f** option to decide the smallest MTU on the path.
	Default value: No resetting
-i	Sets the source IP address of the message or the IP address of an interface.
	Default value: Main IP address of the message-sending interface
source-ip-address	Source IP address adopted by the message
source-interface	Message takes the IP address of the **source-interface** interface as the source address.
-j *host1* [*host2 host3…*]	Sets the relaxation source route.
	Default: Not set
-k *host1* [*host2 host3…*]	Sets the strict source route
	Default: Not set
-l *length*	Sets the length of ICMP data in the message.
	Default: 56 bytes
-n *number*	Sets the total number of messages.
	Default: 5 messages
-r *hops*	Records routes.
	Up to **hops** routes are recorded.
	Default: not record

-s *tos*	Sets IP TOS of the message to *tos*. Default: 0
-t *ttl*	Sets IP TTL of the message to **ttl**. Default: 255
-v	Detailed output Default: simple output
-w *waittime*	Time for each message to wait for response Default: 2 seconds
host	Destination host

Command mode

Management mode, global configuration mode and interface configuration mode

Instruction

The command supports that the destination address is the broadcast address or the multicast address. If the destination address is the broadcast address (255.255.255.255) or the multicast address, the ICMP request message is sent on all interfaces that support broadcast or multicast. The routing switch is to export the addresses of all response hosts. By pinging multicast address 224.0.0.1, you can obtain the information about all hosts in directly-connected network segment that support multicast transmission.

Press the **Q** key to stop the **ping** command.

Simple output is adopted by default.

Parameter	Description
!	A response message is received.
.	Response message is not received in the timeout time.
U	The message that the ICMP destination cannot be reached is received.
Q	The ICMP source control message is received.
R	The ICMP redirection message is received.
T	The ICMP timeout message is received.
P	The ICMP parameter problem message is received.

The statistics information is exported:

Parameter	Description
packets transmitted	Number of transmitted messages
packets received	Number of received response messages, excluding other ICMP messages
packet loss	Rate of messages that are not responded to
round-trip min/avg/max	Minimum/average/maximum time of a round trip (ms)

Example

```
switch#ping -l 10000 -n 30 192.168.20.125
PING 192.168.20.125 (192.168.20.125): 10000 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 192.168.20.125 ping statistics ---
30 packets transmitted, 30 packets received, 0% packet loss
round-trip min/avg/max = 50/64/110 ms
```

4.2 System Debugging Commands

4.3 Fault Diagnosis Commands

The chapter describes the commands used for fault diagnosis. All the following commands are used to detect the reason of the fault. You can use other commands to remove the fault, such as the **debug** command.

The following are fault diagnosis commands:

- logging
- logging buffered
- logging console
- logging facility
- logging monitor
- logging on
- logging trap
- service timestamps
- clear logging
- show break
- show controller
- show debug
- show logging

4.3.1 logging

It is used to record the log information to the **syslog** server.

logging *A.B.C.D*

no logging *A.B.C.D*

Parameter

Parameter	Description
A.B.C.D	IP address of the **syslog** server

Default:

The log information is not recorded to the server.

Command mode

Global configuration

Instruction

It is used to record the log information to the designated **syslog** server. It can be used for many times to designate multiple **syslog** servers.

Example

logging 192.168.1.1

Relative command

logging trap

4.3.2   logging buffered

It is used to record the log information to the memory of the switch.

logging buffered [*size | level | dump*]

no logging buffered

Parameter

Parameter	Description
size	Size of memory cache Value range: 4096-2147483647 Unit: byte
level	Information level of the log recorded to memory cache Refer to table 1.
dump	When the system has abnormality, the information in the current memory is currently recorded to the flash and the information is resumed after the system is restarted.

Default

The information is not recorded to the memory cache.

Command mode

Global configuration

Instruction

The command records the log information to the memory cache of the switch. The memory cache is circularly used. After the memory cache is fully occupied, the latter information will cover the previous information.

You can use the **show logging** command to display the log information recorded in the memory cache of the switch.

Do not use big memory for it causes the shortage of memory.

Table 1   Level of log recording

Prompt	Level	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Relative command

clear logging

show loggin

4.3.3   logging console

Run the command **logging console** to control the information volume displayed on the console.

Run the command **no logging console** to forbid the log information to be displayed on the console:

logging console *level*

no logging console

Parameter

Parameter	Description
level	Information level of the logs displayed on the console Refer to table 2.

Default

None

Command mode

Global configuration

Instruction

After the information level is specified, information of this level or the lower level will be displayed on the console.

Run the command **show logging** to display the currently configured level and the statistics information recorded in the log.

Table 2   Level of log recording

Prompt	Level	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Example

logging console alerts

Relative command

logging facility

show logging

4.3.4   logging facility

Run the command **logging facility** to configure to record specified error information. To restore to **local7**, run the command **no logging facility**.

logging facility *facility-type*

no logging facility

Parameter

Parameter	Description
facility-type	Facility type Refer to table 3.

Default

local7

Command mode

Global configuration

Instruction

Table 3 Facility type

Type	Description
auth	Authorization system
cron	Cron facility
daemon	System daemon
kern	Kernel
local0-7	Reserved for locally defined messages
lpr	Line printer system
mail	Mail system
news	USENET news
sys9	System use
sys10	System use
sys11	System use
sys12	System use
sys13	System use
sys14	System use
syslog	System log
user	User process
uucp	UNIX-to-UNIX copy system

Example

logging facility kern

Relative command

logging console

4.3.5 logging monitor

Run the command **logging monitor** to control the information volume displayed on the terminal line.

Run the command **no logging monitor** to forbid the log information to be displayed on the terminal line.

logging monitor *level*

no logging monitor

Parameter

Parameter	Description
level	Information level of the logs displayed on the terminal line Refer to table 4.

Default

debugging

Command mode

Global configuration

Instruction

Table 4   Level of log recording

Prompt	Level	Description	Syslog Definition
emergencies	0	System is unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Example

logging monitor errors

Relative command

terminal monitor

4.3.6   logging on

Run the command **logging on** to control the recording of error information.

Run the command **no logging on** to forbid all records.

logging on

no logging on

Parameter

None

Default

logging on

Command mode

Global configuration

Example

switch_config# **logging on**
switch_config# ^Z
switch#
Configured from console 0 by DEFAULT
switch# **ping 192.167.1.1**

switch#ping 192.167.1.1
PING 192.167.1.1 (192.167.1.1): 56 data bytes
!!!!!
--- 192.167.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0/4/10 ms
switch#IP: s=192.167.1.111 (local), d=192.167.1.1 (FastEthernet0/0), g=192.167.1.1, len=84, sending
IP: s=192.167.1.1 (FastEthernet0/0), d=192.167.1.111 (FastEthernet0/0), len=84,rcvd
IP: s=192.167.1.111 (local), d=192.167.1.1 (FastEthernet0/0), g=192.167.1.1, len=84, sending
IP: s=192.167.1.1 (FastEthernet0/0), d=192.167.1.111 (FastEthernet0/0), len=84,rcvd
IP: s=192.167.1.111 (local), d=192.167.1.1 (FastEthernet0/0), g=192.167.1.1, len=84, sending
IP: s=192.167.1.1 (FastEthernet0/0), d=192.167.1.111 (FastEthernet0/0), len=84,rcvd
IP: s=192.167.1.111 (local), d=192.167.1.1 (FastEthernet0/0), g=192.167.1.1, len=84, sending
IP: s=192.167.1.1 (FastEthernet0/0), d=192.167.1.111 (FastEthernet0/0), len=84,rcvd
IP: s=192.167.1.111 (local), d=192.167.1.1 (FastEthernet0/0), g=192.167.1.1, len=84, sending
IP: s=192.167.1.1 (FastEthernet0/0), d=192.167.1.111 (FastEthernet0/0), len=84,rcvd

switch_config# **no logging on**

switch_config# ^Z
switch#
switch# **ping** 192.167.1.1
PING 192.167.1.1 (192.167.1.1): 56 data bytes
!!!!!
--- 192.167.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0/4/10 ms

Relative command

logging

logging buffered

logging monitor

logging console

4.3.7   logging trap

Run the command **logging trap** to control the information volume recorded to the syslog server.

Run the command **no logging trap** to forbid the information to be recorded to the syslog server.

logging trap *level*

no logging trap

Parameter

Parameter	Description
level	Information level of the logs displayed on the syslog server Refer to table 5.

Default

Informational

Command mode

Global configuration

Instruction

Table 5   Level of log recording

Prompt	Level	Description	Syslog Definition
emergencies	0	System is unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Example

> logging 192.168.1.1
> logging trap notifications

Relative command

> **logging**

4.3.8　logging command

To open the function to record command execution, run **logging command**.After this function is opened, a log will be generated for each of all entered commands, in which the line to execute this command, the command line, the execution result, the login line and the login address will be recorded.

Parameter

> None

Default value

no logging command

Command mode

Global configuration mode

Example

Switch_config#logging command

Switch_config#Jul 11 15:26:56 %CMD-6-EXECUTE: `logging command ` return 0, switch(vty 0, 192.168.25.42).

Related command

> **logging**

4.3.9　service timestamps

Run the command **service timestamps** to configure the time stamp that is added when the system is debugged or records the log information.

> Run the command **no service timestamps** to cancel the time stamp that is added when the system is debugged or records the log information.

> **service timestamps** [log|debug] [*uptime| datetime*]
>
> **no service timestamps** [log|debug]

Parameter

Parameter	Description

log	Adds the time stamp before the log information.
debug	Adds the time stamp before the debug information.
uptime	Duration between the startup of the switch and the current time
datetime	Real-time clock time

Default

service timestamps log date

service timestamps debug date

Command mode

Global configuration

Instruction

The time stamp in the **uptime** form is displayed like HHHH:MM:SS, meaning the duration from the start-up of the switch to the current time.

The time stamp in the **date** form is displayed like YEAR-MON-DAY HH:MM:SS, meaning the real-time clock time.

Example

service timestamps debug uptime

4.3.10   clear logging

It is used to clear the log information recorded in the memory cache.

clear logging

Parameter

None

Command mode

Management mode

Relative command

logging buffered

show logging

4.3.11   show break

It is used to display the information about abnormal breakdown of the switch.

show break [*map-filename*]

Parameter

Parameter	Description
map-filename	Specifies the filename of the function mapping table.

Default

None

Command mode

Management mode

Instruction

It is used to display the information about abnormal breakdown of the switch, helping to find the cause of the abnormality.

Example

```
switch#sh break
Exception Type:1400-Data TLB error
BreakNum: 1 s date: 2000-1-1   time: 0:34:6
r0        r1        r2        r3        r4        r5        r6
00008538-01dbc970-0054ca18-00000003-80808080-fefefeff-01dbcca1-
r7        r8        r9        r10       r11       r12       r13
00000000-00009032-00000000-7fffff0-00008588-44444444-0054c190-
r14       r15       r16       r17       r18       r19       r20
000083f4-000083f4-00000000-00000000-00000000-00000000-00000000-
r21       r22       r23       r24       r25       r26       r27
00000000-0000000a-00000001-00000000-00000000-004d6ce8-01dbd15c-
r28       r29       r30       r31       spr8      spr9      ip
00000002-00467078-00010300-00000300-00000310-00008588-00000370-
Variables :
00008538-44444444-01dbd15c-01dbcaac-00000002-00000000-004d6ce8-
01dbca18-
 00008538 ---   do_chram_mem_sys_addr---bspcfg.o
 0001060c ---   subcmd---cmdparse.o---libcmd.a
 000083e4 ---   do_chram_mem_sys---bspcfg.o
 0000fb24 ---   lookupcmd---cmdparse.o---libcmd.a
 0000f05c ---   cmdparse---cmdparse.o---libcmd.a
 003e220c ---   vty---vty.o---libvty.a
 00499820 ---   pSOS_qcv_broadcast---ksppc.o---os\libsys.a
```

The whole displayed content can be divided into six parts:

1   RROR:file function.map not found

The prompt information means that the system has not been installed the software **function.map**, which does not affect the system running.

If the version of the software **function.map** is not consistent with that of the switch, the system prompts that the version is not consistent.

2   Exception Type—Abnormal hex code plus abnormal name

3   BreakNum

It is the current abnormal number. It means the number of abnormalities that the system has since it is powered on in the latest time. It is followed by the time when the abnormality occurs.

4 Content of the register

The common content of the register is listed out.

5 Variable area

The content in the stack is listed out.

6   Calling relationship of the number

If the **map** file is not installed on the system, only the function's address is displayed. If the **map** file is installed on the system, the corresponding function name, **.o** file name and **.a** file name are displayed.

The calling relationship is from bottom to top.

4.3.12   show debug

It is used to display all the enabled debugging options of the switch.

show debug

Parameter

None

Command mode

Management mode

Example

switch# show debug

Crypto Subsystem:
   Crypto Ipsec debugging is on
   Crypto Isakmp debugging is on
   Crypto Packet debugging is on

Relative command

debug

4.3.13   show logging

It is used to display the state of logging (syslog).

show logging

Parameter

None

Command mode

Management mode

Instruction

It is used to display the state of logging (syslog), including the login information about the console, monitor and syslog.

Example

switch# show logging

Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: level debugging, 12 messages logged
    Monitor logging: level debugging, 0 messages logged
    Buffer logging: level debugging, 4 messages logged
    Trap logging: level informations, 0 message lines logged

Log Buffer (4096 bytes):
2000-1-4 00:30:11 Configured from console 0 by DEFAULT
2000-1-4 00:30:28 User DEFAULT enter privilege mode from console 0, level = 15

Relative command

clear logging

Chapter 5   SSH Configuration Commands

5.1.1   ip sshd enable

Command description

ip sshd enable

no ip sshd enable

Parameter

None

Default

1024 bits

Instruction

It is used to generate the rsa encryption key and then monitor the connection to the ssh server. The process of generating encryption key is a process of consuming the calculation time. It takes one or two minutes.

Command mode

Global configuration mode

Example

In the following example, the SSH service is generated.

device_config#ip sshd enable

5.1.2   ip sshd timeout

Command description

ip sshd timout *time-length*

no ip timeout

Parameter

Parameter	Description
time-length	Maximum time from the establishment of connection to the authentication approval Value range: 60-65535

Default

180 seconds

Instruction

To prevent the illegal user from occupying the connection resources, the connections that are not approved will be shut down after the set duration is exceeded.

Command mode

Global configuration mode

Example

In the following example, the timeout time is set to 360 seconds:

device_config#ip sshd timeout 360

5.1.3   ip sshd auth-method

Command description

ip sshd auth-method *method*

no sshd auth-method

Parameter

Parameter	Description
method	Sets authentication method list.

Default

The **default** authentication method list is used.

Instrunction

The ssh server uses the authentication method list of the login type.

Command mode

Global configuration mode

Example

In the following example, an **auth-ssh** authentication method list is configured and it is applied to the ssh server:

device_config#aaa authentication login auth-ssh local
device_config#ip sshd auth-method auth-ssh

5.1.4   ip sshd access-class

Command description

ip sshd access-class *access-list*

no ip sshd access-class

Parameter

Parameter	Description
access-list	Standard IP access list

Default

No access control list

Instrunction

It is used to configure the access control list for the ssh server. Only the connections complying with the regulations in the access control list can be approved.

Command mode

Global configuration mode

Example

In the following example, an **ssh-accesslist** access control list is configured and applied in the ssh server:

device_config# ip access-list standard ssh-accesslist
device_config_std_nacl#deny 192.168.20.40
device_config#ip sshd access-class ssh-accesslist

5.1.5　ip sshd auth-retries

Command description

ip sshd auth-retries *times*

no ip sshd auth-retries

Parameter

Parameter	Description
times	Maximum re-authentication times Value range: 0-65535

Default

3 times

Instrunction

The connection will be shut down when the re-authentication times exceeds the set times.

Command mode

Global configuration mode

Example

In the following example, the maximum re-authentication times is set to five times:

device_config#ip sshd auth-retries 5

5.1.6   ip sshd clear

Command description

ip sshd clear *ID*

Parameter

Parameter	Description
ID	Number of the SSH connection to the local device Value range: 0-65535

Default

N/A

Instruction

It is used to mandatorily close the incoming ssh connection with the specified number. You can run the command **show ip sshd line** to check the current incoming connection's number.

Command mode

Global configuration mode

Example

In the following example, the No.0 incoming connection is mandatorily closed:

device_config#ip sshd clear 0

5.1.7   ssh

Command description

ssh –l *userid* **–d** *destIP* **[-c {des|3des|blowfish }] [-o** *numberofpasswdprompts***] [-p** *port***]**

Parameter

Parameter	Description
–l userid	User account on the server
–d destl	Destination IP address in the dotted decimal system
-o numberofpasswdprompts	Re-authentication times after the first authentication fails Actual re-authentication times is the set value plus the smallest value set

	on the server. Its default value is three times. Value range: 0-65535
-p port	Port number that the server monitors Its default value is 22. Value range: 0-65535
-c {des|3des|blowfis h}	Encryption algorithm used during communication The encryption algorithm is 3des by default.

Default

N/A

Instruction

The command is used to create a connection with the remote ssh server.

Command mode

Privileged mode

Example

In the following example, a connection with the ssh server whose IP address is 192.168.20.41 is created. The account is **zmz** and the encryption algorithm is **blowfish**:

device#ip ssh –l zmz –d 192.168.20.41 –c blowfish

5.1.8   show ssh

Command description

show ssh

Parameter

None

Default

N/A

Instrunction

It is used to display the sessions on the ssh server.

Command mode

Privileged mode

Example

In the following example, the sessions on the ssh server are displayed:

device#show ssh

5.1.9　show ip sshd

Command description

> **show ip sshd**

Parameter

> None

Default

> N/A

Instrunction

> It is used to display the current state of the ssh server.

Command mode

> Privileged mode

Example

> In the following example, the current state of the ssh server is displayed:
>
> device#show ip sshd

Chapter 6   Other Systematic Commands

6.1   higig-mode

Syntax

[no] higig-mode {higig+|higig2}

To set the higig mode, run the above-mentioned command.

Parameter

Parameter	Description
higig+|higig2	Chooses the higig+ mode or the higig2 mode.

Default value

The default settings is the higig+ mode.

Instruction

This command is configured in global configuration mode. The higig2 mode can support the MPLS communication between line cards.

Example

The following example shows how to set the higig2 mode.

higig-mode higig2