Basic Configuration Commands

Table of Contents

Chapter 1 **System Management Commands**

1.1 Configuring File Management Commands

File management commands include the following ones:

- copy
- delete
- dir
- download c0
- eraserom
- more
- upload c0
- download
- upload

1.1.1 copy

You can access the TFTP server to read the file from the router by running the **copy** command and write a file in the file system of the router to the TFTP server.

You also can read a file in the U disk on a router or a TFTP server and write a file in the file system of the TFTP server or router to the U disk

Copy {**tftp**<:filename> | **flash**<:filename>} {**flash** <:filename> | **tftp**<:filename>} <blksize>

Copy { **flash**<:filename> | **usb**<:filename>} {**usb** <:filename> | **flash**<:filename>}

Copy {**tftp**<:filename> | **usb**<:filename>} {**usb** <:filename> | **tftp**<:filename>} <blksize>

Parameter

Parameter	Description
tftp<:filename>	When it is used as the first parameter in the previous command sentences, it means to read a file on the TFTP server. When it is used as the second one, it means to write a file to the TFTP server. **Filename** indicates the corresponding file name. If the file name is not

	specified, you will be notified to enter a file name after running the **copy** command.
flash <:filename>	When it is used as the first parameter in the previous command sentences, it means to read a file in the flash of the router. When it is used as the second one, it means to write a file to the flash of the router. **Filename** indicates the corresponding file name. If the file name is not specified, you will be notified to enter a file name after running the **copy** command.
usb <:filename>	When it is used as the first parameter in the previous command sentences, it means to read a file on the U disk. When it is used as the second one, it means to write a file to the U disk. **Filename** indicates the corresponding file name. If the file name is not specified, you will be notified to enter a file name after running the **copy** command.
blksize	Specifies the block size in the TFTP transmission.

Default

None

Command mode

EXEC

Explanation

If you enter the question mark behind **flash:**, all the matched file names will be shown. 如：

After you enter the question mark behind **copy flash: s**, all the file names started with the **s** letter in the current directory are shown.

flash：startup-config flash：sample

You also can enter the all-path or relative path of the **usb** file behind **usb:**to specify the to-be-copied file.

If a router has only one USB card and a U disk on the USB card, the all-path of the **usb** file is **/usb0/path/filename**.

If a router has two USB cards and two U disks on the two USB cards, the U disk at the smaller-number slot is labeled as **usb0** and the other one is labled as **usb1**. The all-path of the **usb** file is like **/usb0/path/filename** or **/usb1/path/filename**.

Example

If you run **copy flash: startup-config tftp: config.txt 600**, the **startup-config** file will be copied from the flash to the TFTP server and named as config.txt. At the same time the size of the transmission block is specified as 600 bytes.

If you run copy flash:router.bin usb:/usb0/r.bin, the router.bin file in the flash will be copied to the U disk at USB0 and labeled as r.bin.

If you run copy tftp:router.bin usb:/usb1/r.bin 2.2.2.2 1024, the router.bin file in the TFTP server will be copied to the U disk at USB1 and labeled as r.bin.Meanwhile, the address of the TFTP server is specified as 2.2.2.2 and the size of the transmission block as 1024 bytes.

cd /usb0

copy flash:router.bin   usb:r.bin

The previous cd command is used to switch the current directory to a subdirectory under the /usb0 directory. The relative path is used to copy the router.bin file in the flash to the root directory of the U disk at usb0, and then the router.bin file is named as r.bin.

Related command

None

1.1.2   delete

It is used to delete a file.

delete   *file-name*

Parameter

Parameter	Description
file-name	File name with up to 20 characters

Default

If the file name is not entered, the **startup-config** file is deleted by default.

Command mode

Monitoring mode

Explanation

None

Related command

None

1.1.3   dir

It is used to display the file and the directory name.

dir file-name

Parameter

Parameter	Description
file-name	File name with up to 20 characters

Default

None

Command mode

Monitoring mode

Explanation

None

Related command

None

1.1.4   download c0

It is used to download the files from the console port in monitor state.

download c0 *filename*

Parameter

Parameter	Description
file-name	Name of the local file

Default

None

Command mode

Monitoring mode

Explanation

The command can be used to download files under the ZMODEM protocol.

Example

monitor#download c0 router.bin

Prompt: speed[9600]?115200

After **speed[9600]?115200** appears, the speed rate is modified to 115200. You then choose the to-be-transmitted file in the transmission menu of the super terminal (simulated terminal) after reconnection.

After the file transmission is over, the following information appears:

ZMODEM:successfully receive 36 blocks ,18370 bytes

Related command

None

1.1.5　eraserom

It is used to delete the updated BOOTROM version.

eraserom

Parameter

None

Default

None

Command mode

Monitoring mode

Explanation

None

Related command

None

1.1.6　more

It is used to display the file content.

more file-name

Parameter

Parameter	Description
file-name	File name with up to 20 characters

Default

None

Command mode

Monitoring mode

Explanation

All the files are composed of displaying characters, use the ASCII code to display them; otherwise, use the binary system to display them.

Related command

None

1.1.7 upload c0

It is used to upload the file in the flash to the host under the **zmodem** protocol.

upload c0 *filename*

Parameter

Parameter	Description
filename	File name in the local flash

Default

None

Command mode

Monitoring mode

Explanation

None

Example

After you enter the command, you are required to enter the speed rate of the port.

Router#upload c0 router.bin

Prompt: speed[9600]?115200

After **speed[9600]?115200** appears, the speed rate is modified to 115200. You then choose the to-be-received file in the reception menu of the super terminal (simulated terminal) after reconnection.

After the file transmission is over, the following information appears:

Zmodem send process completed.

Related command

None

1.1.8 download

It is used to copy the file from the host to the flash under the **zmodem** protocol.

download c0 *filename*

Parameter

Parameter	Description
filename	File name in the memory

Default

Identical with the filename in the host

Command mode

EXEC

Explanation

None

Example

After you enter the command, you are required to enter the speed rate of the port.

Router#download c0 router.bin

Prompt: speed[9600]?115200

After **speed[9600]?115200** appears, the speed rate is modified to 115200. You then choose the to-be-transmitted file in the transmission menu of the super terminal (simulated terminal) after reconnection.

After the file transmission is over, the following information appears:

Zmodem receive process completed.

Related command

None

1.1.9 upload

It is used to upload the file in the memory to the host under the **zmodem** protocol.

upload c0 *filename*

Parameter

Parameter	Description
filename	File name in the memory

Default

None

Command mode

EXEC

Explanation

None

Example

After you enter the command, you are required to enter the speed rate of the port.

Router#upload c0 router. Bin

Prompt: speed[9600]?115200

After **speed[9600]?115200** appears, the speed rate is modified to 115200. You then choose the to-be-received file in the reception menu of the super terminal (simulated terminal) after reconnection.

After the file transmission is over, the following information appears:

Zmodem send process completed

Related command

None

1.2   System Management Commands

Basic system management commands include:

- boot flash

- cd

- chram

- date

- md

- pwd

- rd

- rename

- reboot

- alias

- boot system flash

- help

- history

- job

- debug job

- jobd

- show alias

- show tech-support

1.2.1　boot flash

It is used in monitor mode to start up at the specified file manually.

boot flash *filename*

Parameter

Parameter	Description
filename	Specifies the file name

Default

None

Command mode

Monitoring mode

Explanation

After the system enters the monitor mode, the command is used to start up the system.

Example

monitor#boot flash router.bin

Related command

dir

1.2.2　cd

It is used in monitor mode to change the current directory.

cd　directory|..

Parameter

Parameter	Description
directory	Directory name with up to 20 characters
..	Upper-level directory

Default

None

Command mode

Monitoring mode

Explanation

None

Example

monitor#cd my_dir

Related command

pwd

1.2.3 chram

It is used to change the memory data.

chram mem_addr value

Parameter

Parameter	Description
mem_addr	Memory address in the hex system, ranging from 0 to 0 x01FFFF00.
value	Memory data in the hex system

Default

None

Command mode

Monitoring mode

Explanation

The command is a debugging command and you are not recommended to use it.

Example

None

Related command

None

1.2.4   date

It is used to set the absolute systematic time.

Parameter

None

Default

None

Command mode

EXEC or global configuration mode

Explanation

Routers need to reset the systematic time after powering off, the command, hence, is used to set the time for these routers. If time is not right, you should replace the battery.

Example

config#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 command

None

1.2.5　md

It is used to create a directory.

md　directory

Parameter

Parameter	Description
directory	Directory name with up to 20 characters

Default

None

Command mode

Monitoring mode

Explanation

None

Related command

None

1.2.6　pwd

It is used to display the current directory.

Parameter

None

Default

None

Command mode

Monitoring mode

Explanation

None

Related command

None

1.2.7 rd

It is used to delete a directory.

rd directory

Parameter

Parameter	Description
directory	Directory name with up to 20 characters

Default

None

Command mode

Monitoring mode

Explanation

The system will prompt you whether the directory exists or not. If the directory does not exist, the system will prompt that the directory does not exist.

Related command

None

1.2.8 rename

It is used to change the file name.

rename old_file_name new_file_name

Parameter

Parameter	Description

old_file_name	Original file name
new_file_name	New file name

Default

None

Command mode

Monitoring mode

Explanation

None

Related command

None

1.2.9　reboot

It is used to restart the router.

Parameter

None

Default

None

Command mode

Monitoring mode

Explanation

None

Related command

None

1.2.10 alias

It is used to set the alias of the command. The "no" form of the command is used to delete the alias of the command.

[no] alias [alias_name command_line**]**

Parameter

Parameter	Description
alias_name	Alias of the command, which is used to replace the command line
command_line	Command line which is replaced by the alias of the command

Default

None

Command mode

Configuration mode

Explanation

If you complex command lines are frequently used, you can use the command to specify the command alias.

Example

Router_config#alias c copy tftp:router.bin flash:router.bin 192.2.2.1

Related command

show alias

1.2.11 boot system flash

It is used to specify the mirroring file executed when the system is started. The "no" form of the command is used to delete the previous configuration.

boot system flash *filename*

no boot system flash *filename*

Parameter

Parameter	Description

filename	Specified file name with up to 20 characters

Default

None

Command mode

Global configuration mode

Explanation

If the command is not configured, the system will run the first systematic mirroring file in the file system in the flash. If multiple commands are configured, the system will run the mirroring files in order. If a mirroring file does not exist or has the checksum error, the next mirroring file will be run. If all mirroring files fail to be run, the system enters the monitor mode.

Example

config#boot system flash router.bin

Related command

None

1.2.12   help

It is used to display the help system of the router.

help

Parameter

None

Default

None

Command mode

EXEC

Explanation

None

Example

After you run the command, the help system of the router is displayed.

Router# 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?'.)

Related command

None

1.2.13   history

It is used to browse the used commands. The "no" form of the command is used to delete the previously used commands.

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

Parameter

Parameter	Description
+ <count>	**Displays 20 historical commands from beginning to end.**
- <count>	**Displays 20 historical commands from end to beginning.**

Default

If there are less than 20 historical commands, all commands will be displayed; if there are more than 20 historical commands, the recent 20 historical commands will be displayed from beginning to end.

Command mode

Any mode

Explanation

Routers of modular series can save up to 20 historical commands. You can use the up/down arrow key to find these commands or edit them.

Example

In the following examples, recent five historical commands are displayed from end to beginning.

Router#history - 5

config

int e1/1

no ip addr

ip addr 192.2.2.49 255.255.255.0

exit

Related command

None

1.2.14   job

It is used to define a job and set the schedule of the job. The "no" form of the command is used to cancel the defined job.

[no] job   {[interval *fireinterval* | one-shot] |sleep *sleeptime* |stop *jobname*}

Parameter

Parameter	Description
exec jobname	Performs a job immediately.
jobname definaton	Defines a job.
restart jobname	Restarts a job.
schedule jobname	Sets a job if a schedule is performed.
at firsttime	Sets the first execution interval of a job after **jobd** is started.
interval fireinterval	Sets the interval between two job executions
one-shot	Sets a job to be performed once

sleep sleeptime	Sets the sleep time.
stop jobname	Stops the scheduled job.

Default

None

Command mode

Global configuration mode

Explanation

Job here stands for a segment of script, defining the to-be-run command combination, the time to perform the job and the interval of the operation.

Example

The following example shows that jobs on all ports are defined to be shutdown.

job shutall "int s1/0;shut;int s1/1;shut;int s1/2;shut;int s1/3;shut"

The following example shows that jobs on all ports are defined to be **no shutdown**.

job noshutall "int s1/0; no shut;int s1/1;no shut;int s01/2;no shut;int s1/3;no shut"

The following example shows that all ports perform the **shutdown** operation and the **no shutdown** operation.

job schedule shutall at 100 interval 60

job schedule noshutall at 130 interval 60

After 100 seconds of jobd startup, **shutal**l a job and the job will be restarted every 60 seconds; After 130 seconds of the router startup, **noshutall shutall** the job and the job will be restarted every 60 seconds.）

To execute the order of shutall or noshutall, define and schedule like the following:

job reshut "job exec shutall；job exec noshutall"

job schedule reshut at 100 interval 30

If error occurs when shutall is operated, run the following command (paused by default):

job shutall on-error next

To run **noshutall**, do the following: (the job cannot be recursively called)

job shutall on-error exec noshutall

The following example shows that a job is paused.

job stop shutall

The following example shows that a paused job is restarted.

job restart shutall

Related command

jobd show

job debug

job

1.2.15   debug job

It is used to trace the execution of a job.

Parameter

None

Command mode

EXEC

Explanation

After the job debugging information is opened, the execution and schedule of the job is exported.

Example

config#debug job

JOB：<showver> fired

JOB：job <showver>, cmd "show ver" is parsing

Related command：

job

jobd

show job

1.2.16　jobd

It is used to start up the protection process for executing the job. The "no" form of the command is used to terminate the protection process of the job.

[no] jobd

Parameter

None

Default

None

Command mode

Global configuration mode

Explanation

The execution of the job need be scheduled and executed by **jobd**. The execution time of the job takes the startup time of **jobd** as the basis. Press **q**, **Q** or **Ctrl+Shift+6** to terminate **jobd**.

Example

The following example shows how **jobd** is started:

Router_config# jobd

Job daemon started. No commands can be entered.End with q,Q,or Ctrl+Shift+6

Related command

debug job

job

show job

1.2.17   show alias

It is used to display all aliases or specified aliases.

Show alias [<*alias name*>]

Parameter

Parameter	Description
alias name	Alias of a command

Default

All aliases are displayed according to the formula "alias name=command line".

Command mode

EXEC mode or configuration mode

Explanation

None

Example

In the following example, all aliases in the current system are displayed:

Router_config# show alias

hualab=date

router=snmp

Related command

alias

1.2.18   show tech – support

It is used to display some important information about the system.

show tech – support

Parameter

None

Default

None

Command mode

EXEC mode or configuration mode

Explanation

The command is used to display some important information about the system, which is required by technical support.

1.3　HTTP Configuration Commands

HTTP configuration commands include:

- ip http access-class

- ip http port

- ip http server

1.3.1　ip http access-class

It is used to receive the specified HTTP request successfully.

ip http access-class *string*

no ip http access

Parameter

Parameter	Description
string	Name of the specified standard access control list (ACL)

Command mode

Global configuration mode

Explanation

The specified ACL must be set before the command is used.

The "no" form of the command is used to cancel the limitation to the HTTP request.

Example

router_config# ip access-list standard http-acl

router_config_std_nacl# permit 192.2.2.37 255.255.255.0

router_config_std_nacl# exit

router_config# ip http access-class http-acl

Related command

ip http server

ip http port

1.3.2   ip http port

It is used to specify the number of the HTTP port.

ip http port *number*

Parameter

Parameter	Description
number	Port number of the HTTP service

Default

Port 80 is taken by the browser as the default port number of the HTTP service.

Command mode

Global configuration mode

Explanation

After the command is run, if the http service is enabled, shut down the original listening port and then use the specified port (the specified port is available) to receive the request of the http service; if the http service is not enabled, the command has no effect on the http service request temporarily.

Example

The following example shows the number of the http port is changed from 80 to 90.

router_config# ip http server

router_config# ip http port 90

Related command

ip http access-class

ip http server

1.3.3   ip http server

It is used to enable the http service.

ip http server

no ip http server

Parameter

None

Command mode

Global configuration mode

Explanation

You can use the command to specify a port of the router to accept the http request, handle the request and to return the result to the browser.

Example

router_config# ip http server

Related command

ip http access-class

ip http port

Chapter 2   **Terminal Service Configuration Commands**

2.1   Telnet Configuration Commands

Telnet configuration commands include:

- telnet

- ip telnet

- ctrl-shift-6+x

- where

- disconnect

- resume

- switchkey

- switchmsg

- sequence-char

- clear telnet

- show telnet

- debug telnet

2.1.1   telnet

The command line for establishing the telnet session is shown in the following:

telnet *server-ip-addr/server-host-name* [**/port** *port*][**/source-interface** *interface*] [**/local** *local-ip-addr*] [**/debug**][**echo/noecho**] [**/script** *scriptname*] [**/ts-block** | **/ts-discard**] [**/info** *information*] [**/source-port** *sourceport*]

Parameter

Parameter	Description
server-ip-addr	Dotted-decimal IP address of the remote server
server-host-name	Host name of the remote server, which need be configured by the **ip host** command
port	Port of the telnet service provided by the remote server
interface	Local interface which triggers the telnet connection

local-ip-addr	Local IP address which triggers the telnet connection
/debug	Opens the debug switch at the client and prints the negotiation process during the connection.
echo/noecho	Opens and shuts down the local echo. The echo is not enabled by default.
scriptname	Name of the script which is used for automatic logging
/ts-block	Sets to block the local telnet connection when it is at the background.
/ts-discard	Sets the telnet message to be dropped when the local telnet connection is at the background.
/info	Sets related printing information before the telnet connection.
/source-port	Sets the local port for the telnet connection
/router-id	Authenticates the router ID.

Default

The default value of the port is 23, while the interface has no default value.

Command mode

EXEC

Explanation

You can use the following command line for remote login.

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

In this case, the application program will directly send the request for creating a telnet link to port 23 of the remote server. The adopted local IP address is the one nearest to the peer which is found by the routing table.

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

The application program sends the request for creating a telnet link to the peer port.

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

The application program takes the IP address on the interface as the local address.

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

The application program enables the **debug** switch and exports the connection negotiation information on the client.

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

The application program enables/disables the local echo. In general, the local echo is disabled. The echo process is performed by the server. Only when the server does not echo is the switch of the local echo enabled.

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

The automatic login command for running the script need be configured by the **ip telnet script** command.

In some print-screen applications, corresponding **routeras** software is not installed on the server. When the local telnet connection is at the background and is set with the parameter **/ts-block** or **/ts-discard**, if there is data from the server, the router can temporarily save 4000-bytes data for the telnet connection. As for the later data, the router will take the following two strategies:

If the **/ts-block** parameter is set, the server will be blocked from transmitting the data to the local computer until the telnet connection is at the front workstation.

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

In this case, the application program will print the configuration information out and then sends the request for creating telnet link to the remote server.

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

In this case, the application program sends a request for creating telnet link to port 23 of the remote server. The used local TCP port is the configured source port.

The commands and parameters above can be used together.

During the session between remote server and client, you can press **Q** to exit the session. If you does not exit the session manually, the session will be over after 10 seconds.

Example

Suppose you telnet the remote server whose IP address is 192.168.20.124 and the telnet service ports of the server are port 23 and port 2323. There are two local ports **e1/1(192.168.20.240)** and **s1/0(202.96.124.240)**. You can use the following command lines for remote login:

telnet 192.168.20.124 /port 2323

After you perform the previous command line, a telnet connection will be established between port 2323 of host 192.168.20.124 and host 192.168.20.240. The local IP address seen on the peer is 192.168.20.240.

telnet 192.168.20.124 /source-interface s1/0

After you perform the previous command line, a telnet connection will be established between port 23 of host 192.168.20.124 and host 192.168.20.240. The local IP address seen on the peer is 202.96.124.240.

telnet 192.168.20.124 /local 192.168.20.240

After you perform the previous command line, a telnet connection will be established between port 23 of host 192.168.20.124 and host 192.168.20.240. The local IP address seen on the peer is 192.168.20.240.

telnet 192.168.20.124 /debug

After you perform the previous command line, information about the negotiation process of the telnet connection with the peer port 23 is printed out.

telnet 192.168.20.124 /echo

The local echo switch is opened. If the echo also occurs on the server, all entered information will be echoed twice.

telnet 192.168.20.124 /script s1

The s1 login script will be used for automatic login.

telnet 192.168.20.124 /info adminadmin

After you run the previous command line, the information "adminadmin" will be first printed out.

telnet 192.168.20.124 /source-port 601

After you perform the previous command line, a telnet connection will be established between port 23 and local machine. The local tcp port is port 601.

telnet 192.168.20.124 /router-id /p 10000

A telnet connection will be established between port 1000 and local machine. The router ID authentication will be performed afterwards. You need configure corresponding router ID authentication on the peer.

2.1.2 ip telnet

The command lines for establishing the telnet session is shown in the following:

ip telnet source-interface *interface*

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

ip telnet server-port *server-port*

Parameter

Parameter	Description
interface	Local interface which triggers the telnet connection
accesslist	Name of the ACL which limits the source address when the local machine receives the connection
start-port	Start port number for specifying the listening port area
end-port	End port number for specifying the listening port area
scriptname	Name of the login script
user_prompt	Prompt information about the user name sent back by the telnet server
user_answer	Response information about user name provided by the client
pwd_prompt	Prompt information about the user password sent back by the

	telnet server
pwd_answer	Response information about password provided by the client

Default

None

Command mode

Global configuration mode

Explanation

You can run the following command to configure the local interface for triggering the telnet connection.

ip telnet source-interface *interface*

In this case, all the coming telnet connections will use the interface. The command has the similar function as the **telnet source-interface** *interface* command, but the command has not followed by the **interface** parameter. After the interface is configured and the telnet command has the **interface** parameter followed, take the followed interface as the standard.

You can use the following command to configure the name of the ACL which limits the local machine to receive the telnet connection.

ip telnet access-class *accesslist*

In this case, the server will check the ACL before it receives all telnet connections.

You can run the following command to configure the ports except default port (23) to receive the telnet connection.

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

Note: If the end port number is not specified, the port listening must be performed on a certain port. The number of specified listening ports cannot be larger than 16 and the port number ranges between 3001 and 3999.

You can run the following command to configure the telnet login script.

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

Note:

During script configuration, username prompt and answer, password prompt and answer must be completely matched. The prompt information is case sensitive. The prompt information must be in the inverted comma (''). If error occurs in the configuration, the automatic logon cannot go on.

Note:

The previous four commands can use the "no" form of these commands to cancel the configuration.

You can run the following command to correct the telnet listening port.

ip telnet server-port *serverport*

Note:

You can run the command to modify the telnet listening port to any port except port 23.

Note:

1) When you run this command to modify the listening port, all telnet connections on the original listening port will be deleted.

2) Run the corresponding command to resume the telnet listening port to port 23.

3) Run corresponding "no" form of these commands to disable the telnet listening function, that is, the router cannot serve as a telnet server after you run the "no" form commands.

Example

1) ip telnet source-interface s1/0

In this case, all the coming telnet connections will use interface s1/0.

2) ip telnet access-class abc

In this case, the following received telnet connections will be checked by the **abc** ACL.

3) ip telnet listen-port 3001 3010

Except port 23, all ports between port 3001 and port 3010 can receive the telnet connection.

4) ip telnet script s1 'login:' router 'Password:' test

The s1 logon script is configured. The username prompt is **login** and the answer is **router**. The password prompt is **password** and the answer is **test**.

2.1.3 ctrl-shift-6+x (mounting the current telnet connection)

Run the following command to mount the current telnet connection.

ctrl-shift-6+x

Parameter

None

Default

None

Command mode

Any time in the current telnet session

Explanation

You can use the shortcut key to mount the currently outgoing telnet connection at the client.

Example

RouterA>telnet 192.168.20.1

Welcome to Multi-Protocol 1700 Series Router

RouterB>ena

RouterB#(按 ctrl-shift-6+x)

RouterA>

If you press **ctrl-shift-6+x** during the current telnet session which connects router B, the connection of router B is mounted and the system gets back to the current state of router A.

2.1.4 where

It is used to check the currently mounted outgoing telnet session at the client.

where

Parameter

None

Default

None

Command mode

Global configuration mode

Explanation

You can run the command at the client to check the currently mounted outgoing telnet session. The displayed information includes the serial number, peer address, peer port, local address and local port.

Note:

The **where** command and the **show telnet** command are different. The former is used at the client and can display the outgoing telnet connection, while the latter is used at the server and can display the incoming telnet connection.

Example

RouterA>telnet 192.168.20.1

   Welcome to Multi-Protocol 1700 Series Router

RouterB>ena

RouterB#(按 ctrl-shift-6+x)

RouterA> telnet 192.168.20.2

   Welcome to Multi-Protocol 1700 Series Router

RouterC>ena

RouterC#(按 ctrl-shift-6+x)

RouterA>where

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

If you run where on router A, the information about the mounted outgoing connection of router A is displayed.

2.1.5   resume

It is used to resume the currently mounted outgoing telnet session at the client.

resume *no*

Parameter

Parameter	Description

No	Serial number of the currently-mounted telnet session which is observed after the **where** command is run

Default

None

Command mode

Global configuration mode

Explanation

You can run the command at the client to resume the currently mounted outgoing telnet session.

Example

RouterA>telnet 192.168.20.1

Welcome to   Multi-Protocol 1700 Series Router

RouterB>ena

RouterB#(press ctrl-shift-6+x)

RouterA> telnet 192.168.20.2

Welcome to Multi-Protocol 1700 Series Router

RouterC>ena

RouterC#(press ctrl-shift-

6+x) RouterA>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

RouterA>Resume 1

[Resuming connection 1 to 192.168.20.73 . . .]

(enter)

RouterB#

After you run **where** at router A and the mounted outgoing connections on router A are displayed, enter **resume 1**. Connection 1 is resumed. After you press **Enter**, the command prompt appears on router B.

2.1.6   disconnect

It is used to delete the currently mounted outgoing telnet session at the client.

disconnect *no*

Parameter

Parameter	Description
No	Serial number of the currently-mounted telnet session which is observed after the **where** command is run

Default

None

Command mode

Global configuration mode

Explanation

You can run the command at the client to delete the currently-mounted outgoing telnet session.

Note:

The **disconnect** command and the **clear telnet** command are different. The former is used at the client and can delete the outgoing telnet connection, while the latter is used at the server and can delete the incoming telnet connection.

Example

RouterA>telnet 192.168.20.1

   Welcome to Multi-Protocol 1700 Series Router

RouterB>ena

RouterB#(Press ctrl-shift-6+x)

RouterA> telnet 192.168.20.2

   Welcome to Multi-Protocol 1700 Series Router

RouterC>ena

RouterC#(Press ctrl-shift-6+x)

RouterA>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

RouterA>disconnect 1

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

Connection closed by remote host.

RouterA>

After you run **where** at router A and the mounted outgoing connections on router A are displayed, enter **disconnect 1**. You are notified whether the connection of router B is closed. After you press **Y**, the connection is cut off.

2.1.7   switchkey

The following command is used to configure the terminal switchover key on the line.

switchkey key cmdalias server-name

Parameter

Parameter	Description
Key	The composite key is formed of the **ctrl** key plus any letter key except the **H** key.
cmdalias	Alias of the **connect** command
Server－name	Name of the remote host, which appears in the shift prompt information and the shift menu.

Default

None

Command mode

Line configuration mode

Explanation

You can run the command in line configuration mode to configure the terminal shift key, the alias of the corresponding command and the name of the remote host.

Note:

1) The **cmdalias** parameter must be pointed to a correct **connect** command.

2) Ctrl-h cannot be the key parameter.

3) The server-name parameter will appear in the shift prompt information and the shift menu.

4) autocommand cannot be configured on the line, or the terminal shift function is out of function.

Example

RouterA>switchkey ctrl-a cona ServerA

The shift key is set to **ctrl-a** and the command alias is set to **cona**. The server which is switched to is server A.

2.1.8   switchmsg

The following command is used to configure whether the terminal shift information is exported or not.

switchmsg enable/disable

Parameter

Parameter	Description
Enable	Exports the prompt information about terminal shift.
Disable	Forbids to export the prompt information about terminal shift.

Default

disable

Command mode

Line configuration mode

Explanation

You can use the command during terminal shift configuration to decide whether to export the prompt information about terminal shift.

Example

RouterA>switchmsg enable

When the terminal is shifted, the prompt information appears.

2.1.9   sequence-char

The following command is used to configure the terminal switchover key on the line.

sequence-char key char1 char2 char3 …

Parameter

Parameter	Description
Key	The composite key is formed of the **ctrl** key plus any letter key except the **H** key.
char1 char2 char3 …	Character sequence about the specific terminal

Default

None

Command mode

Line configuration mode

Explanation

You can use this command to configure the terminal shift key and the character sequence of the corresponding terminal on the line.

Note:

Ctrl-h cannot be the key parameter.

The character sequence is related with the detailed terminal. The terminal manual can be found on the terminal manuscript.

The character sequence must be in the hex system and starts with 0x. Each character are separated by pressing the space key.

Example

RouterA>sequence-char ctrl-a 0x1b 0x21 0x38 0x51

The character sequence of the **ctrl-a** shift key is set to **0x1b 0x21 0x38 0x5**.

For other **alias** and **async** commands, see relative configuration explanation.

Application example

The configuration of the router is 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

After all configuration and the connections are done, open the terminal. The shift menu automatically appears. In this case, you press the composite key **Ctrl-U**, the system is automatically shifted to server A. The prompt information of the current host, server A, is exported automatically.
After you enter **Ctrl-V**, the system is automatically shifted to server B and the prompt information of the current host, server B, is exported automatically.
After you enter **Ctrl-W**, the system is automatically shifted to server C and the prompt information of the current host, server C, is exported automatically. No matter when you enter **ctrl-**, the current screen displays the shift menu and the "*" symbol is added behind the current server.

The following information is displayed after you press **ctrl-**.

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

Terminal Switch Menu

1)   CTRL-U   ServerA   *

2)   CTRL-V   ServerB

3)   CTRL-W   ServerC

Note: During the operation of multiple connections, if you enable the system to exit from one connection, the system will take the first connection as the current connection and the interface of the first host is shown on the screen. If the first connection has been exited, the second connection will be taken as the current connection and the interface of the second host is shown on the screen.

After all services are completed, the recommended exit method is to directly shut down the terminal no matter how many connections are opened currently.

Before other connections are not exited, you'd better not enable the system to exit the first connection.

You are strongly suggested to switch a connection to another not just to disable a connection. After all operations are done, you can shut down the terminal.

During terminal switchover, the function to mount or resume the connection through the **ctrl-shift-6+x** command is disabled.

2.1.10   clear telnet

Run the following command to remove the telnet session on the server.

clear telnet *no*

Parameter

Parameter	Description
No	Serial number of the telnet session displayed by the **show telnet** command

Default

None

Command mode

EXEC

Explanation

You can run the command to remove the telnet session on the server.

Example

1. clear telnet 1

The telnet session (192.168.20.220:1097) whose serial number is 1 is deleted.

2.1.11 show telnet

Run the following command to display the telnet session on the server.

show telnet

Parameter

None

Default

None

Command mode

All modes except the user mode

Explanation

You can run the command to remove the telnet session on the server. The displayed information includes the serial number, peer address, peer port, local address and local port.

Example

1. show telnet

After the previous command is run, the following information is shown:

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 command is used to debug the telnet session:

debug telnet

Parameter

None

Default

None

Command mode

EXEC

Explanation

You can run the command to open the debugging switch of the telnet session.

After you run the command, the negotiation processes of all the incoming telnet sessions are shown on the debugging output window. The **debug telnet** command is different from the **telnet [/debug]** command. The former is used to export the debugging information about the incoming connections on the server, while the latter is used to export the debugging information about the telnet sessions trigger by the client.

Example

debug telnet

The switch of the debugging server which the telnet session connects is opened.

2.2   Rlogin Configuration Commands

The **rlogin** command is used to create the rlogin session between remote servers. In general, the **rlogin** command is used for remote login between the local machine and the Unix system. Because the operating system of the peer is already known, the option negotiation does not need. The rlogin command is mainly used for authentication based on the IP address of the host and the username of the remote server. The major difference between **rlogin** and **telnet** lies in that the **rlogin** command prevents user from entering the password every time through proper configuration on the server.

2.2.1   rlogin

The command line for establishing the rlogin session is shown in the following:

rlogin   server-ip-addr   [**-l**   Username]

Parameter

Parameter	Description
server-ip-addr	Dotted-decimal IP address of the remote server
Username	User name of the remote server, which is up to 30 characters

Default

None

Command mode

Global configuration mode

Explanation

You can run one of the following commands for remote login.

- **rlogin** *server-ip-addr*

  The application program queries you the remote user name and tries to create a connection with the remote terminal.

- **rlogin** server-ip-addr **-l** Username

  In this case, the application program directly tries to create a remote connection.

During the session between remote server and client, you can press one of the following composite keys.

- Ctrl-S: Preventing the client from the output of the remote terminal

- Ctrl-Q: Resuming the output of the remote terminal

Note:

When you press the composite key **Ctrl-S** or **Ctrl-Q**, the corresponding cooperation from the server is required.

You can enable the system to exit from a session by adding the continuous sequence "~" and ".".

Press the composite key **ctrl+shift+6** to exit from the session.

Example

Suppose you use the **rlogin** command to log on to the server 192.168.20.124 and the username on the server is **guest**, you can one of the following commands to perform the remote login:

rlogin 192.168.20.124

In this case, the username for logging on to the remote server is required. After the username is obtained, the connection with the remote server starts to be created. The following is an example:

router# rlogin 192.168.20.124

username: guest

Try to connect server .

The shadow font is entered.

rlogin 192.168.20.124 –l guest

In this case, the r**login** command is used to directly try to establish the connection with the remote server.

2.3   Terminal Configuration Commands

Terminal configuration commands include:

- 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

2.3.1   attach-port

The following command is used to bind the listening telnet port to the **line vty** number, enabling the telnet connection on a specific port to generate vty according to the specified sequence order.

[no] attach-port *PORT*

Parameter

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

Default

None

Command mode

Line configuration mode

Example

The following example shows that the listening port, 3001, is bound to line vty 23.

Router_config# line vty 2 3

Router_config_line#attach-port 3001

2.3.2 autocommand

It is used to set the auto-run command when the user logs on to the terminal. After the command is run, the connection is disconnected.

autocommand *LINE*

no autocommand

Parameter

Parameter	Description
LINE	Command which will be run

Command mode

Line configuration mode

Example

Router_conf#line vty 1

Router_conf_line#autocommand pad 123456

After successful login, the system pads that the address of X.121 is host 123456.

2.3.3 clear line

It is used to remove the specified line.

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

Parameter

Same as the **line** command

Command mode

EXEC

Example

Router#clear line vty 0

2.3.4 connect

It is used to connect the telnet server.

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

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 triggered
local-ip-addr	Local IP address where the connection is triggered
/ts-block	Sets to block the local telnet connection when it is at the background.
/ts-discard	Sets the telnet message to be dropped when the local telnet connection is at the background.

Command mode

All configuration modes

Example

Router#connect 192.168.20.1

Explanation

For the parameters **/ts-block** and **/ts-discard**, see the **telnet** command.

2.3.5 disconnect

It is used to cancel the mounted telnet session.

disconnect *N*

Parameter

Parameter	Description
N	Number of the mounted telnet session

Command mode

All configuration modes

Example

Router#disconnect 1

2.3.6 exec-timeout

It is used to set the maximum free time of the terminal.

[no] exec-timeout [*time*]

Parameter

Parameter	Description
time	Free time whose unit is second

Default

0

Command mode

Line configuration mode

Example

The following example shows the free time of a line is set to 3600 seconds (one hour).

Router_config_line#exec-timeout 3600

2.3.7 length

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

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

Parameter

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

Default

24

Command mode

Line configuration mode

2.3.8　line

It is used to enter the line configuration mode.

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

Parameter

Parameter	Description
**aux	console	tty	vty**	All are the line types. **AUX** stands for the auxiliary line; **console** stands for the monitoring line; **tty** for asynchronous line and **vty** for the virtue lines such as Telnet, PAD and Rlogin.
number	Number of the line of the typeFor console and aux, only the number **0** is used for numbering.

Command mode

Global configuration mode

Example

The following example shows that the configuration states of No. 0 line to No.10 line after the system enters VTY.

Router_config#line vty 0 10

2.3.9　location

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

location [*LINE*]

no location

Parameter

Parameter	Description
LINE	Description about the current line

Command mode

Line configuration mode

2.3.10   login authentication

It is used to set the authentication parameter about line login.

[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

Router_conf_line#login authentication test

The authentication list of the line is set to **test**.

2.3.11   monitor

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

[no] monitor

Parameter

None

Command mode

Line configuration mode

Example

Router_config_line#monitor

2.3.12 no debug all

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

no debug all

Parameter

None

Command mode

EXEC

Example

Router#no debug all

2.3.13 password

It is used to set the terminal password.

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

no password

default password

Parameter

Parameter	Description
Password	Password configured on the line It is entered in a way of the plain text and its length can be over 30 digits.
[encryption-type] encrypted-password	**encryption-type** means the type of password encryption. Currently only two types, 0 and 7, are supported. **0** means that the data is not encrypted. The plain text of the password is directly entered for the parameter **encrypted-password**, which has the same result as the password is directly entered without adding the encryption-type. **7** means that an algorithm defined is used for encryption. For the **encrypted-password** parameter, the encrypted password text need be entered, which can be copied from the configuration file of other routers.

For any problem about the password, see the description of the commands **service password-encryption** and **enable password**.

Command mode

Line configuration mode

Example

Router_conf#line vty 1

Router_conf_line#password test

In this example, the login password of VTY1 is set to **test**.

Explanation

The parameter **no password** means that the password is not required. After you configure the line authentication mode under **aaa**, directly log on to the line or enter the EXEC mode.

Default password meas to resume the default configuration, that is, no password exists. After you configure the line authentication mode under **aaa**, you cannot log on to the line or enter the EXEC mode.

2.3.14   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

Router#resume 1

2.3.15   printer enable

Open or shut down the direct-through printer.

printer enable[*disable*]

Parameter

Parameter	Description
enable	Opens the direct-through printer on the line.
disable	Closes the direct-through printer on the line.

Default

disable

Command mode

Line configuration mode

Example

Open the direct-through printer on line tty 1.

Router_config# line vty 1

Router_config_line#printer enable

2.3.16   printer start

Configure the character sequence for starting printing.

[no] printer start *char1 char2 char3 …*

Parameter

Parameter	Description
char1 char2 char3 …	Character sequence in the hex system for printing, which starts with 0x and is separated with space
no	Resumes the default value of the printing character sequence, 0x1b 0x5b 0x35 0x69

Default

0x1b 0x5b 0x35 0x69

Command mode

Line configuration mode

Example

Configure the printing character sequence on line tty 1.

Router_config# line vty 1

Router_config_line#printer start 0x1b 0x5b 0x30 0x69

2.3.17   printer stop

Configure the character sequence for ending printing.

[**no**] **printer stop** *char1 char2 char3 …*

Parameter

Parameter	Description
char1 char2 char3 …	Character sequence in the hex system for ending printing, which starts with 0x and is separated with space
no	Resumes the default value of the character sequence of ending printing, 0x1b 0x5b 0x34 0x69

Default

0x1b 0x5b 0x34 0x69

Command mode

Line configuration mode

Example

Configure the character sequence for ending printing on line tty 1.

Router_config# line vty 1

Router_config_line#printer stop 0x1b 0x5b 0x31 0x69

2.3.18   script activation

Configure the activation script of the line.

script activation *WORD*

Parameter

Parameter	Description
WORD	Name of the script

Command mode

Line configuration mode

Example

Set the activation script of the line to **script1**.

Router_config_line#script activation script1

2.3.19　script callback

Configure the script for dial-back.

script callback *WORD*

Parameter

Parameter	Description
WORD	Name of the script

Command mode

Line configuration mode

Example

Set the activation script of the line to **script1**.

Router_config_line#script callback script1

2.3.20　script connection

Configure the script for creating connection.

script connection *WORD*

Parameter

Parameter	Description
WORD	Name of the script

Command mode

Line configuration mode

Example

Configure the script for creating connection to **script1**.

Router_config_line#script connection script1

2.3.21 script dialer

Configure the script for dial-out.

script dialer *WORD*

Parameter

Parameter	Description
WORD	Name of the script

Command mode

Line configuration mode

Example

In the following example, the script for dial-out is configured.

Router_config_line#script dialer script1

2.3.22 switchkey

Configure the terminal shift key.

switchkey key cmdalias *server-name*

Parameter

Parameter	Description
key	Terminal shift key (ctrl-a—ctrl-z, except ctrl-h)
cmdalias	Alias of the execution command when the terminal is shifted
server-name	Name of the server corresponded by each terminal screen

Command mode

Line configuration mode

Example

In the following example, the **sco1** server is connected by the **con_sco** command after you use **ctrl-a** for switchover.

Router_config_line#switchkey ctrl-a con_sco sco1

2.3.23　script reset

It is used to configure the script for port resetting.

script reset *WORD*

Parameter

Parameter	Description
WORD	Name of the script

Command mode

Line configuration mode

Example

In the following example, the script for port resetting is set to **script1**.

Router_config_line#script reset script1

2.3.24　script startup

It is used to configure the startup script.

script startup *WORD*

Parameter

Parameter	Description
WORD	Name of the script

Command mode

Line configuration mode

Example

In the following example, the startup script is set to **script1**.

Router_config_line#script startup script1

2.3.25   s equence-char

It is used to configure the character sequence for writing back to the terminal when the terminal is shifted.

sequence-char key *char1 char2 char3 …*

Parameter

Parameter	Description
key	Terminal shift key
char1 char2 char3 …	Write-back character sequence

Command mode

Line configuration mode

Example

In the following example, the write-back character sequence is set to **0x1b 0x21 0x38 0x51** when **ctrl-a** is used for switchover.

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

2.3.26   show debug

It is used to display all current debugging information opened by VTY.

show debug

Parameter

None

Command mode

EXEC or global configuration mode

Example

Router#show debug

Generic IP:

IP packet debugging is on

Frame Relay:

Lmi debugging is on

2.3.27 show line

It is used to display the currently effective line state.

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

Parameter

If there is no parameter followed, all currently effective line states are displayed.

The definitions of other parameters are in line with that of the **line** command.

Command mode

All modes except the user mode

2.3.28 show tty-status

It is used to display the configuration state of the port corresponded by TTY.

show tty-status *N*

Parameter

Parameter	Description
N	Sequence number of the line TTY

Default

None

Command mode

All modes except the user mode**Example**

The configuration state of the port corresponded by TTY1 is displayed in the following example.

Router_config# show tty-status 1

2.3.29   switchmsg

It is used to configure whether the prompt information is displayed at terminal switchover.

switchmsg *enable*

switchmsg *disable*

Parameter

Parameter	Description
enable	Displays the prompt information at the switchover of the terminal.
disable	Forbids to display the prompt information at the switchover of the terminal.

Default

disable

Command mode

Line configuration mode

Example

The prompt information is displayed at the switchover of the terminal.

Router_config_line#switchmsg enable

2.3.30   terminal length

It is used to modify the number of lines displayed on the current terminal, which can be obtained by the remote host. The **rlogin** protocol uses the parameter to notify the UNIX host. You can run **no terminal length** to resume the default value.

terminal length *length*

no terminal length

Parameter

Parameter	Description
length	Number of lines displayed on each screen

Default

The lines pauses to be displayed after 24 lines are displayed.

Command mode

Global configuration mode

Explanation

It is valid for the current terminal. After the session triggered by the command is complete, the terminal attributes are gone.

Example

router#terminal length 40

Related command

line

2.3.31   terminal monitor

To display the debugging output information or systematic error information on the current terminal, run **terminal monitor**. You can run **no terminal monitor** to shut down the monitoring function.

terminal monitor

no terminal monitor

Parameter

None

Default

The console port is opened by default, while other terminals are shut down by default.

Command mode

Global configuration mode

Explanation

It is valid for the current terminal. After the session triggered by the command is complete, the terminal attributes are gone.

Example

router#terminal monitor

Related command

line

debug

2.3.32   terminal width

The router exports 80 characters each line by default. If the terminal width cannot satisfy the demands of the terminal, you can reset it. The parameter can be obtained by the remote host. You can run **terminal width** to set the number of characters of each line. You can run **no terminal length** to resume the default value.

terminal width *number*

no terminal width

Parameter

Parameter	Description
number	Number of characters in each line

Default

80 characters each line

Command mode

Global configuration mode

Explanation

It is valid for the current terminal. After the session triggered by the command is complete, the terminal attributes are gone.

Example

router#terminal width 40

Related command

line

2.3.33 terminal-type

It is used to set the terminal type.

[no] terminal-type [*name*]

Parameter

Parameter	Description
name	Terminal nameThe terminal types supported currently include VT100, ANSI and VT100J.

Default

ANSI

Command mode

Line configuration mode

2.3.34 where

It is used to check the currently mounted outgoing telnet session at the client.

where

Parameter

None

Command mode

All configuration modes

Example

Router#where

2.3.35 width

It is used to set the terminal width of the line.

[**no**] **width** [*value*]

Parameter

Parameter	Description
value	Value between 0 and 5120 表示不折行。

Default

80

Command mode

Line configuration mode

2.3.36   debug line

It is used to export the debugging information about the line.

[**no**] **debug line** *line [lineno]*

Parameter

Parameter	Description
line	Line type: aux/console/tty/vty/tty2console
lineno	Sequence number of the line

Default

The debugging is shut down.

Command mode

EXEC

Explanation

If you run **debug line aux/console/vty/tty2console**, the debugging information of the corresponding line is printed on the console port. If you run **debug line tty** *lineno,* the **tty lineno** debugging information is printed on VTY.

Chapter 3   **Network Management Configuration Commands**

3.1   HTTP Configuration Commands

Telnet configuration commands include:

- 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

It is used to set the character string of the community SNMP access. You can run the "no" form of the command to delete the specified group character string.

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

no snmp-server community *string*

Parameter

Parameter	Description
string	Character string of the community SNMP access, similar to the password
view *view-name*	Name of the view previously defined, which is an optional parameter The view defines the MIB object which is valid to the community.
ro	An optional parameter, which specifies the read-only permission The authorized management workstation can only read the MIB object.

rw	An optional parameter, which specifies the read-write permission The authorized management workstation can read and modify the MIB object.
word	An optional parameter, which specifies the IP ACL name for accessing the SNMP agent using the community character string

Default

The character string of SNMP community has the read-only permission to all objects by default.

Command mode

Global configuration mode

Explanation

If no parameter follows, the configuration information about the community character string is listed.

Example

The following example shows that the comaccess character string is distributed to the SNMP, the read-only permission is allowed and the community character string of the IP ACL is specified.

snmp-server community comaccess ro allowed

The following example shows the **mgr** character string is distributed to the SNMP and the objects in the **restricted** view are allowed.

snmp-server community mgr view restricted rw

The following example shows the **comaccess** community is deleted.

no snmp-server community comaccess

Related command

access-list

snmp-server view

3.1.2   snmp-server contact

It is used in global configuration mode to set the contact (**sysContact**) about the management node. You can use the "no" form of the command to delete the **sysContact** parameter configuration.

snmp-server contact *text*

no snmp-server contact

Parameter

Parameter	Description
text	Character string about the contact

Default

The contact information about the node is not set.

Command mode

Global configuration mode

Explanation

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

Example

The following example shows the information about the contact of the node.

snmp-server contact Dial_System_Operator_at_beeper_#_27345

Related command

You can use the main index or the online information of the index to look up related documents.

3.1.3   snmp-server host

It is used in global configuration mode to specify the receiver of the SNMP trap operation. You can run the "no" form of the command to delete the specified 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	Community character string sent together with the trap operation, which is similar to the password
trap-type	An optional parameter

	If no trap is specified, all traps are sent to the host.
authentication	Allows to send the trap about the authentication error.
configure	Allows to send the **SNMP-configure** trap.
snmp	Allows to send all SNMP traps.

Default

The command is invalid by default. No trap will be sent. If a command without any keyword is run, all types of traps will be sent by default.

Command mode

Global configuration mode

Explanation

If the **snmp-server host** command is not run, the trap will not be sent. To configure the router to send the SNMP trap, you must run the **snmp-server host** command. If the command without the **trap-type** keyword is entered, all trap types about the host are activated. If the command with the **trap-type** keyword is entered, the trap type relative with the keyword is activated. You can specify many trap types for each host.

If you specify multiple **snmp-server host** commands for a same host, the router will filter the SNMP trap information according to the community character string and the trap type. You can only configure one trap type for a same host and a community character string.

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

Example

The following example shows that the SNMP trap defined by RFC1157 is sent to the host whose IP address is 10.20.30.40. The community character string is defined as **comaccess**.

snmp-server host 10.20.30.40 comaccess snmp

The following example shows how to enable the router to send all types of traps to host 10.20.30.40 using the community character string **public**.

snmp-server host 10.20.30.40 public

The following example shows that the effective **authentication** trap will be sent to host **bob**.

snmp-server host bob public authentication

Related command

snmp-server queue-length

snmp-server trap-source

snmp-server trap-timeout

3.1.4   snmp-server location

It is used in global configuration mode to set the character string for the location of the node. You can run the "no" form of the command to delete the location character string.

snmp-server location *text*

no snmp-server location

Parameter

Parameter	Description
text	Character string describing the node's location

Default

The character string of the node's location is not set.

Command mode

Global configuration mode

Explanation

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

Example

In the following command, the actual location of the router is defined.

snmp-server location Building_3/Room_214

Related command

snmp-server contact

3.1.5   snmp-server packetsize

It is used in global configuration mode to define the maximum size of the SNMP packet when the SNMP server receives requests or generates response.**snmp-server packetsize** *byte-count*。

no snmp-server packetsize

Parameter

Parameter	Description
byte-count	Integer byte from 484 to 17940Its default value is 3000 bytes.

Default

3000 bytes

Command mode

Global configuration mode

Explanation

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

Example

The following example shows that a filter with a maximum packet of 1024 bytes is created.

snmp-server location Building_3/Room_214

Related command

snmp-server queue-length

3.1.6   snmp-server queue-length

It is used in global configuration mode to set the length for the message queue of each trap host.

snmp-server queue-length *length*

Parameter

Parameter	Description

length	Number of trap events that can be saved in the queue

Default

Ten events

Command mode

Global configuration mode

Explanation

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

Example

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

snmp-server queue-length 4

Related command

snmp-server packetsize

3.1.7   snmp-server trap-source

It is used in global configuration mode to specify an interface as the source address of all traps. You can run the "no" form of the command to cancel such an interface.

snmp-server trap-source *interface*

no snmp-server trap-source

Parameter

Parameter	Description
interface	An interface where the SNMP trap generatesParameters include the interface type and serial number of the syntax mode for a specific platform.

Default

Do not specify the interface.

Command mode

Global configuration mode

Explanation

After the SNMP server sends the SNMP trap out, it has a trap address no matter from which interface it is sent out. If you want to use the trap address for tracking, run the command.

Example

The following example shows that the address of interface 1/0 is specified as the source address of all traps.

snmp-server trap-source ethernet 1/0

The following example shows that the IP address of interface 1/0 is specified as the source address of all traps.

snmp-server trap-source ethernet 1/0

Related command

snmp-server queue-length

snmp-server host

3.1.8 snmp-server trap-timeout

It is used in global configuration mode to define the timeout value for resending the trap information.

snmp-server trap-timeout *seconds*

Parameter

Parameter	Description
seconds	An interval for message resending, which is an integer between 1 and 1000 Its unit is second.

Default

30 seconds

Command mode

Global configuration mode

Explanation

Before the router tries to send the trap, it can be used to find the route of the destination address. If there is no route, the trap will be saved in the re-sent queue. This command decides the interval of message resending.

Example

The following example shows an interval of 20 seconds is set and the trap message will be resent from the re-sent queue.

snmp-server trap-timeout 20

Related command

snmp-server host

snmp-server queue-length

3.1.9   snmp-server view

It is used in global configuration mode to create or update the MIB view. You can run the "no" form of the command to cancel 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	Tag of the view that is updated or created
oid-tree	Object identifier of the **ASN.1** sub-tree which is included or rejected in the viewIdentifier sub-tree can specify a character string including numbers, for example, 1.3.6.2.4 or a sub-tree name **system**. Sub-tree names are names that can be found in all MIB trees.
included excluded	Type of the viewIt must be set to **included** or **excluded**.

Default

None

Command mode

Global configuration mode

Explanation

If other SNMP commands need a view to be their parameter, you can use the command to create a view for these SNMP commands. By default, the view need not be defined. You can see all the objects (similar to the **everything** view predefined by Cisco). You can use the command to define all objects that can be seen from the view.

Example

The following example shows how to create a view in the MIB-II sub-tree where all objects can be seen.

snmp-server view mib2 mib-2 included

The following example shows how to create a view in the **system** group where all objects can be seen.

snmp-server view phred system included

The following example shows a view where all objects in the **system** group can be seen is created. The view, however, excludes all objects in system 7 (sysService.7) and interface 1.

snmp-server view agon system included

snmp-server view agon system.7 excluded

Related command

snmp-server community

3.1.10   show snmp

The **show snmp** command is used to monitor the input and output SNMP statistics, including the character string items of the illegal community, error and number of the request variables.

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

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

show snmp [host | view]

Parameter

Parameter	Description

host	Displays the information about the SNMP trap host.
view	Displays the information about the SNMP view.

Default

None

Command mode

EXEC or global configuration mode

Explanation

To list out the output/input SNMP statistics, run the **show snmp** command.

To display the information about the SNMP trap host, run **show snmp host**.

To display the information about the SNMP view, run **show snmp view**.

Example

The input/output SNMP statistics is listed in the following:

#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 domains of the statistics information received or transmitted by the SNMP agent are shown in the following table:

Domain	Meaning
Unknown community name	Community name that cannot be identified
Illegal operation for community name supplied	Incorrect operation
Encoding errors	Incorrect encoding
Get-request PDUs	Get-request message
Get-next PDUs	Get-next message
Set-request PDUs	Set-request message
Too big errors	The response message is too big to be generated.
No such name errors	The specified instance does not exist.
Bad values errors	The value is incorrectly 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 host is shown.

#show snmp host

Notification host: 192.2.2.1   udp-port: 162   type: trap

user: public   security model: v1

The following example shows that the SNMP view is displayed:

#show snmp view

mib2   mib-2   -   included   permanent   active

Related command

snmp-server host

snmp-server view

3.1.11   debug snmp

It is used to display the SNMP event, message reception and transmission and error information.

debug snmp [error | event | packet]

Run **no debug snmp** to stop displaying relative information.

Parameter

Parameter	Description
error	Enables the debugging switch of the incorrect SNMP information.
event	Enables the debugging switch of the SNMP event.
packet	Enables the debugging switch of the input/output SNMP message.

Command mode

EXEC

Explanation

After the SNMP debugging switch is enabled, the SNMP event, message transmission and reception and error information are exported, which helps you to check the SNMP fault.

Example

The following example shows the procedure of receiving and transmitting the SNMP message:

Router#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

Domain	Description
Received	SNMP receiving the message.
192.168.0.29	Source IP address
1433	Port number of the source address
51 bytes	Length for receiving the 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 encoded by SNMP ASN
0..-.....public. .....}.......0.. .0.....+........ .	ASCII code presentation of message receivingThe content which is not in the range of the ASCII code is presented with dots.
sending	SNMP transmitting message
192.168.0.29	Destination IP address
1433	Port number of the destination address
52 bytes	Length for transmitting the 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 ...6	ASCII code presentation of message transmittingThe content which is not in the range of the ASCII code is presented with dots.

The following is an example of the debugging of the SNMP event:

Router#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

Domain	Description
SNMP	The currently debugged protocol is the SNMP protocol.
GETNEXT request	SNMP getnext request
RESPONSE	SNMP response
--	Receiving message
>>	Transmitting message
ip.ipReasmFails.0	MIB OID which is required to be accessed
ip.ipFragOKs.0 = 1	Accessed MIB OID and the response value

3.2　RMON Configuration Commands

HTTP configuration commands include:

- rmon alarm

- rmon event

- rmon collection stat

- rmon collection history

- show rmon

3.2.1 rmon alarm

Description

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

It is used to configure an **rmon** alarm item.

Parameter

Parameter	Description	Value Range
variable	Object which will be monitored	OID of the detected object
interval	Sampling interval	1~4294967295 seconds
value	Alarm threshold	-2147483648~2147483647
eventnumber	Index of the event which is triggered after the threshold is reached	1~65535
string	Description about the owner	Length of the character string:1~127

Default

The **eventnumber** parameter is not set.

Note:

The command is configured in global configuration mode, used to monitor the value of the specified object and triggers the specified event when the value reaches the threshold.

Example

In the following example, an rmon alarm item is configured and the monitored object is set to **ifInOctets.2**. The sampling interval is set to 10. If the value **15** is exceeded, event 1 is triggered. If the threshold is falling by 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 admin

3.2.2 rmon event

Description

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

It is used to configure an **rmon** event.

Parameter

Parameter	Description	Value Range
index	Index of the event list	1-65535
des-string	Character string of event description	1~127
owner-string	Character string of the owner	1~127
community	Community name when the trap is generated	1~127

Default

None

Note:

The command is used to configure an **rmon** event for alarm.

Example

In the following example, an **rmon** event is set; the index is set to **6** and the description string is set to **example**. If the event is triggered, items will be added to the log and the trap is generated with the community name **public**.

rmon event 6 log trap public description example owner admin

3.2.3   rmon collection stat

Description

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

It is used to configure the rmon statistics function.

Parameter

Parameter	Description	Value Range
index	Index of the event list	1~65535
string	Character string of the owner	1~127

Default

None

Note:

It is configured in interface configuration mode and used to enable the statistics function of the interface.

Example

The following example shows that the command is used to enable the statistics function of interface 8.

int f 0/8

rmon collection stats 2 owner admin

3.2.4   rmon collection history

Description

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

It is used to configure an history control list

Parameter

Parameter	Description	Value Range
index	Index	1-65535
bucket-number	Among all data collected in the history control list, the recent **bucket-number** items need be saved.	1~65535
second	Interval	1~3600
owner-name	Character string of the owner	1~127

Default

The value of the **bucket-number** parameter is 50 and the value of the **second** parameter is 1800.

Note:

The command is configured in interface configuration mode and used to add an item to the history control list.

Example

In the following example, a history control list is added to interface 8 of fast Ethernet; the statistics data during recent 20 intervals are saved and each interval is 20 seconds.

int f 0/8

rmon collection history 2 buckets 20 interval 10 owner admin

3.2.5   show rmon

Description

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

It is used to configure the rmon configuration.

Parameter

None

Default

None

Note:

The rmon configuration is displayed.

3.3   HTTP Configuration Commands

- pdp enable
- pdp holdtime
- pdp timer
- pdp run
- show pdp traffic
- Show pdp neighbor

3.3.1   pdp enable

Description

pdp enable

no pdp enable

It is used to start up PDP on the interface.

Parameter

None

Default

The PDP is not started on the interface.

Note:

PDP is not started in global configuration mode or interface configuration mode. The command is valid only when PDP is started in global configuration mode.

Example

The following example shows how to start up PDP on the interface.

int e1/1

pdp enable

3.3.2   pdp holdtime

Description

pdp holdtime *second*

no pdp holdtimes

It is used to configure the time for PDP saving the neighbor information.

Parameter

Parameter	Description	Value Range
seconds	Preservation time	10-255

Default

180

Note:

None

Example

The value of **holdtime** is set to **90s**.

pdp holdtime 90

3.3.3   pdp run

Description

It is used to start up the PDP function on the router.

pdp run

no pdp run

Parameter

None

Default

None

Example

You can run the following commands to start up or shut down the PDP function.

pdp run

no pdp run

3.3.4   pdp timer

Description

It is used to configure the transmission frequency of the PDP message.

pdp timer *seconds*

no pdp timer

Parameter

Parameter	Description	Value Range
seconds	Interval for data transmission	5-254

Default

   60 seconds

Note:

   The shorter the time is, the higher the update frequency of the neighbor information.

Example

   The following example shows how to set the interval of data transmission to 30 seconds.

   pdp 30

3.3.5   show pdp traffic

Description

   It is used to display the statistics information about transmission and reception of the PDP data.

   show pdp traffic

Parameter

   None

Default

   None

Note:

   None

Example

   router#sho pdp traffic

      Packets output: 0, Input: 0

      Hdr syntax: 0, Chksum error: 0

      No memory: 0, Invalid packet: 0

3.3.6   show pdp neighbor

Description

It is used to display the information about the neighbor.

show pdp neighbor [detail]

Parameter

None

Default

None

Note:

None

Example

show pdp neighbor

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

S - Switch, H - Host, I - IGMP, r - Repeater

Device-ID	Local-Intf	Hldtme	Port-ID	Platform	Capability
2610	Fas0/0	154	Eth0/0	cisco 2610	R T
c25	Fas0/0	149	Eth0	cisco 2509	R
GK-C36	Fas0/0	123	Fas1/0	cisco 3640	R T
cMR	Fas0/0	167	Fas0/0	cisco 2621	R T

show pdp neighbor detail

Device ID: 2610

Entry address(es): IP address: 192.168.20.204

Platform: cisco 2610, Capabilities: Router Trans-Bridge

Interface: FastEthernet0/0, Port ID(outgoing port): Ethernet0/0

Holdtime : 123 sec

Version :

Cisco Internetwork Operating System Software

IOS (tm) C2600 Software (C2600-IS-M), Version 12.2(7), RELEASE SOFTWARE (fc1)

Copyright (c) 1986-2002 by cisco Systems, Inc.

Compiled Tue 15-Jan-02 23:58 by pwade

advertisement version:2

Duplex: half(00)

Device ID: c25

Entry address(es): IP address: 192.168.20.115

Platform: cisco 2509, Capabilities: Router

Interface: FastEthernet0/0, Port ID(outgoing port): Ethernet0

Holdtime : 178 sec

Version :

Cisco Internetwork Operating System Software

IOS (tm) 2500 Software (C2500-I-L), Version 11.2(4), RELEASE SOFTWARE (fc1)

Copyright (c) 1986-1997 by cisco Systems, Inc.

Compiled Mon 10-Feb-97 12:28 by ajchopra

Device ID: GK-C36

Entry address(es): IP address: 192.168.20.156

Platform: cisco 3640, Capabilities: Router Trans-Bridge

Interface: FastEthernet0/0, Port ID(outgoing port): FastEthernet1/0

Holdtime : 152 sec

Version :

Cisco Internetwork Operating System Software

IOS (tm) 3600 Software (C3640-A3JS56I-M), Version 12.1(3a)T1, RELEASE SOFTWARE (fc1)

Copyright (c) 1986-2000 by cisco Systems, Inc.

Compiled Sat 29-Jul-00 03:21 by ccai

advertisement version:2

Duplex: half(00)

Device ID: cMR

Entry address(es): IP address: 192.168.20.22

Platform: cisco 2621, Capabilities: Router Trans-Bridge

Interface: FastEthernet0/0, Port ID(outgoing port): FastEthernet0/0

Holdtime: 136 sec

Version :

Cisco Internetwork Operating System Software

IOS (tm) C2600 Software (C2600-A3JK9S-M), Version 12.2(10a), RELEASE SOFTWARE (fc1)

Copyright (c) 1986-2002 by cisco Systems, Inc.

Compiled Tue 21-May-02 12:50 by pwade

advertisement version:2

Duplex: half(00)

Chapter 4 **Maintenance and Debugging Commands**

4.1 Network Testing Command

Network testing command includes:

- ping

4.1.1 ping

It is used in monitoring mode to test whether the host can be reached and whether the network can be connected, by transmitting the ICMP request message to the to-be-tested peer and then waiting for the ICMP response message from the peer.

ping ip-address

Parameter

Parameter	Description
ip-address	Destination IP address

Default

None

Command mode

Monitoring mode

Explanation

After the command is run, four pieces of 48-byte message will be sent to the destination host. Two seconds later, timeout occurs if no response message is received.

Example

monitor#ping 192.168.0.100

Reply from 192.168.0.100 : data=48, time=10ms, ttl=128

Reply from 192.168.0.100 : data=48, time=10ms, ttl=128

Reply from 192.168.0.100 : data=48, time=10ms, ttl=128

Reply from 192.168.0.100 : data=48, time=10ms, ttl=128

4 packets sent, 4 packets received

round-trip min/avg/max = 0/2/10 ms

Related command

ip address

4.2   Trouble Diagnosis Commands

Trouble diagnosis commands include:

- 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

4.2.1   logging

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

logging *A.B.C.D* [vrf *vrfname*]

no logging *A.B.C.D* [vrf *vrfname*]

Parameter

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

Default

It is not recorded on the server.

Command mode

Global configuration mode

Explanation

It is used to record the log information on the **syslog** server. The command can be used many times to specify multiple syslog servers.

Example

logging 192.168.1.1

logging 192.168.1.1 vrf aaa

Related command

logging trap

4.2.2 logging buffered

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

logging buffered [size | level | dump]

no logging buffered

Parameter

Parameter	Description
size	Size of the memory cache, ranging from 4096 bytes to 2147483647 bytes
level	Log information level recorded to the memory cache
dump	When systematic trouble occurs, the information in the current memory will be temporarily saved to the flash. The system will be resumed after re-startup.

Default

It is not recorded to the memory cache.

Command mode

Global configuration mode

Explanation

The command is used to record the log information to the memory cache of the router. Because the memory cache is used in recycle, new information will replace old information after the memory cache is fully filled.

To display the log information recorded in the memory cache of the router, run **show logging**.

Do not use too much memory because the memory is insufficient.

Table 4-1 Level of the log record

	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

Related command

clear logging

show loggin

4.2.3　logging console

To control the information volume displayed in the console port, run **logging console**.

To forbid displaying the log information on the console port, run **no logging console**.

logging console *level*

no logging console

Parameter

Parameter	Description
level	Level of log information displayed on the console port

Default

None

Command mode

Global configuration mode

Explanation

After a level is specified, the log information of this level or under the level will be displayed on the console port. You can run **show logging** to display the current level and statistics of the log.

Table 4-2 Level of log record

	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

Related command

logging facility

show logging

4.2.4   logging facility

To configure which kind of error information will be recorded, run **logging facility**. To resume **local7**, run **no logging facility**.

logging facility *facility-type*

no logging facility

Parameter

Parameter	Description
facility-type	Type of the facility

Default

local7

Command mode

Global configuration mode

Explanation

Table 4-3 Type of facility

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

Related command

logging console

4.2.5 logging monitor

To control the information volume displayed on the terminal line, run **logging monitor**.

To forbid displaying the log information on the terminal line, run **no logging monitor**.

logging monitor *level*

no logging monitor

Parameter

Parameter	Description
level	Level of log information displayed on the terminal line

Default

debugging

Command mode

Global configuration mode

Explanation

Table 4-4 Level of log record

	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 monitor errors

Related command

terminal monitor

4.2.6   logging on

To control the record of error information, run **logging on**.

To disable all records, run **no logging on**.

logging on

no logging on

Parameter

None

Default

logging on

Command mode

Global configuration mode

Example

Router_config# **logging on**

Router_config# ^Z

Router#

Configured from console 0 by DEFAULT

Router# ping 192.167.1.1

Router#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

Router#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

Router_config# no logging on

Router_config# ^Z

Router#

Router# 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

Related command

logging

logging buffered

logging monitor

logging console

4.2.7　logging trap

To control the information volume recorded to the syslog server, run **logging trap**.

To forbid recording information to the syslog server, run **no logging trap**.

logging trap *level*

no logging trap

Parameter

Parameter	Description
level	Level of log information displayed on the terminal line

Default

Informational

Command mode

Global configuration mode

Explanation

Table 4-5 Level of log record

	Level	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate	LOG_ALERT

		action needed	
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

Related command

logging

4.2.8 service timestamps

To configure the time stamp which is added during debugging or log recording, run **service timestamps**.

To disable the time stamp which is added during debugging or log recording, run **service timestamps**.

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 debugging information.
uptime	Format of the time stamp: from startup time to current time
datetime	Real-time clock in the time stamp format

Default

service timestamps log date

service timestamps debug date

Command mode

Global configuration mode

Explanation

The time stamp in the uptime format is displayed as HHHH:MM:SS, indicating the period from the startup to the current time.

The time stamp in the uptime format is displayed as YEAR-MON-DAY HH:MM:SS, indicating the real time.

Example

service timestamps debug uptime

4.2.9　clear logging

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

clear logging

Parameter

None

Command mode

EXEC

Related command

logging buffered

show logging

4.2.10　show break

It is used to display the information about the abnormal interruption of the router.

show break [*map-filename*]

Parameter

Parameter	Description
map-filename	Specifies the file name for the function mapping table.

Default

None

Command mode

EXEC

Explanation

The **show break** command is used to display the captured information about abnormal interruption of the router. The reason of the fault, hence, will be found.

Example

Router#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 |

00000000-00009032-00000000-7ffffff0-00008588-44444444-0054c190-

| 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 displayed content is formed of six parts:

ERROR:file function.map not found

The previous error shows that the **function.map** software is not installed, which does not affect the function of the system.

If the version the **function.map** software is different from that on the router, the system shows that the version is not the same.

Exception type—abnormal hex encoding + abnormal name

BreakNum

BreakNum means the number of the current abnormality. It shows the number of the abnormities occurred after the system is started. It is followed by the time when the abnormity occurred.

Content of the register

The content of the register is listed in the following:

Variable area

The content in the stack is listed.

Number invocation

If the **map** file is not loaded on the system, only the address of the function is displayed. If the **map** file is loaded, the corresponding function name such as the **.o** file or the **.a** file will also be displayed.

The invocation of the number is from bottom to top.

4.2.11   show controller

To display the information about the controller of the router's interface, run the **show controller** command.

show controller [*interface*]

Parameter

Parameter	Description

interface	Specifies the name of the interface.

Default

None

Command mode

EXEC

Explanation

The show controller command is used to the state and its configuration information of the controller on the specified interface. When trouble occurs, you can find the reason of the trouble by analyzing relative data.

Example

Router#show controller s1/0

Interface Serial1/0

Hardware is PowerQUICC MPC860T

SCC Registers:

  General [GSMR]=0x68034:0x22, Protocol-specific [PSMR]=0x3000

  Events [SCCE]=0, Mask [SCCM]=0xcf, Status [SCCS]=0x3

  Transmit on Demand [TODR]=0, Data Async [DSR]=0x7e7e

Interrupt Registers:

  [CICR]=00e49f80 [CIPR]=4000c006 [CIMR]=48000000, [CISR]=00000000

Command register [CR]=0x6c0

SICR=0900002c, BRG=00000000:00010288:00000000:00000000 (aux=0)

Statistics: scc4, port3

  int 751229 bad_first 0 too_long 0 drop 0

  tx_count 1 bk_count 0 h_Q 81 s_Q 0

Port A [PADIR]=0000 [PAPAR]=53c3 [PAODR]=0000 [PADAT]=fefe

Port B [PBDIR]=00021001 [PBPAR]=00001020 [PBODR]=0000 [PBDAT]=0001e3be

Port C [PCDIR]=0000 [PCPAR]=0008 [PCSO]=0438 [PCDAT]=0fe7 [PCINT]=0008

Receive Ring

        rmd(fff02320): status=9000 length=0000 address=01155f58

        rmd(fff02328): status=9000 length=0000 address=01156c90

        rmd(fff02330): status=9000 length=0000 address=01156b18

        rmd(fff02338): status=9000 length=0000 address=011569a0

        rmd(fff02340): status=9000 length=0000 address=01156828

        rmd(fff02348): status=9000 length=0000 address=011566b0

        rmd(fff02350): status=9000 length=0000 address=01156538

        rmd(fff02358): status=b000 length=0000 address=01156f80

Transmit Ring

        tmd(fff02360): status=0000 length=0000 address=00000000

        tmd(fff02368): status=0000 length=0000 address=00000000

        tmd(fff02370): status=0000 length=0000 address=00000000

        tmd(fff02378): status=0000 length=0000 address=00000000

        tmd(fff02380): status=0000 length=0000 address=00000000

        tmd(fff02388): status=9000 length=0051 address=01156df4

        tmd(fff02390): status=0000 length=0000 address=00000000

        tmd(fff02398): status=2000 length=0000 address=00000000

SCC GENERAL PARAMETER RAM (at 0xfff03f00)

Rx BD Base [RBASE]=0x2320,   Fn Code [RFCR]=0x15

Tx BD Base [TBASE]=0x2360,   Fn Code [TFCR]=0x15

Max Rx Buff Len [MRBLR]=252

Current Rx(2) State [RSTATE]=0x9000,   BD Ptr [RBPTR]=0x1156b18

Current Tx(5) State [TSTATE]=0x9000,   BD Ptr [TBPTR]=0x1156df4

SCC UART PARAMETER RAM (at 0xfff03f30)

Maximum idle characters 1

Break Character 1

Received Parity Error 58445

Received Frame Error 65261

Received Noise Error 39256

Number of break conditions 22595

Last Received Break length 1524

uart1 63220 uart2 1

Transmit Out of sequence 0

cc[0] = 4011 cc[1] = 4013 cc[2] = 8000 cc[3] = 4011

cc[4] = 4013 cc[5] = 8000 cc[6] = 9c80 cc[7] = 7051

rccm = c0ff rccr = bf28 rlbc = a6fe

RxBufSiz 254 flow 1

flag=00000120, size=00000008, X=11, Xoff=13

DCR_B3#

The displayed content is formed of the following parts:

  Name and type of the controller

      The name is MPC860 and the type is SCC.

  Running state of the controller

      Information about interruption, error and reset
      Length of the queue

  Configuration parameters of the controller:

      Parameter of the register's content
      Partial parameters of the controller
      Parameter about the physical protocol

  State of receiving and transmitting BD

      The length, state and index of the BD are listed.
      Location and state of the currently-received or -transmitted BD

4.2.12   show debug

To display all opened invocation options of the router, run **show debug**.

show debug

  Parameter

  None

Command mode

EXEC

Example

Router# show debug

Crypto Subsystem:

Crypto Ipsec debugging is on

Crypto Isakmp debugging is on

Crypto Packet debugging is on

Related command

debug

4.2.13 show logging

To display the state of logging (syslog), run **show logging**.

show logging

Parameter

None

Command mode

EXEC

Explanation

After you run **show logging**, the state of logging is displayed, including the logging information about the console port, monitor and syslog.

Example

Router# 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

Related 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|blowfish}	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