Basic Configuration

Table of Contents

Chapter 1   System management

1.1   File configueration of management

1.1.1   management of files system

Name of the file in FLASH can have 20 characters at most, and you do not need to pay attention to whether need " capital".

1.1.2   Command of files system

"Black" part of all instructions is key word, others are parameters. Part of [ ] is optional.

Command	Description
format	You can format files system, delete all data.
dir [file name]	show names of file and catalog . part in [ ] means that display files whose name begins with [ ]. The format of displaying file is follow: Index number file name \<FILE> length of file creating time
delete filename	Delete a file, if it is not exist, it will prompt "this file does not exist".

1.1.3   update software

User can use this instruction to download router system software from local or remote sever to update your software or get the special version you have customed. (like data encryption).

There are two ways to update softwares in system monitor state.

1. By TFTP Negotiation

monitor#copy tftp<*:filename*> flash <*:filename*> [ip_addr]

This instruction is used to copy files from tftp server to system flash, after entering instruction, there will be a prompt to let user input remote server name and remote file name.

parameter explain

parameter	Description
tftp<:filename>	read files from tftp server. Filename shows the corresponding file name, if not , after executing "copy", there will be a prompt to let user input file name.

flash <:filename>	write files to router flash. Filename shows the corresponding file name, if not , after executing "copy", there will be a prompt to let user input file name.
ip_addr	Tftp IP address of server. If not, after executing "copy", there will be a prompt to let user input file name.

example:

read "main.bin"file from server, write to router" "router.bin"

monitor#copy tftp flash:router.bin

prompt: Remote-server ip address[]?192.168.0.116

prompt: Name of remote file to read[]?main.bin

TFTP:successfully receive 36 blocks ,18370 bytes

monitor#

2. By serial communication negotiation zmodem

if you want to update software, adopt"download".enter"download?",you can get some help.

monitor#download   c0   <local_filename>

This instruction is used to copy files to system flash by serial communication negotiation, after entering instruction, there will be a prompt to let user input interface speed.

Parameter explains

Parameter	Description
Local_filename	Which is the file name used to save to flash, user must input file name.

Example

The terminal program can adopt Hyper Terminal in WINDOWS 95, NT 4.0 or terminal emulate program in Windows 3.X.

monitor#download c0 router.bin

 prompt : speed[9600]?115200

Then, change speed to 115200, after reconnecting , choose" send file" on transportation menu in Hyper Terminal(terminal emulate) .then, a dialogue window will appear, as below photo:
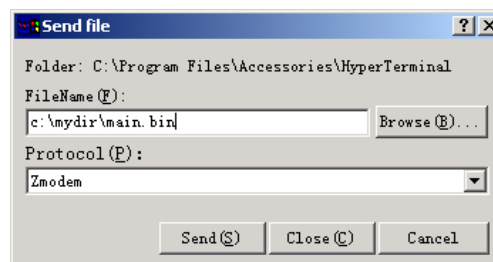
Figuer 1-1 dialogue window of "send file"

Enter full path of main.bin (provide by our company) in file name input frame, choose "Zmodem", press "send" button to send files.

After file transportation , there will appear information as follows:

ZMODEM:successfully receive 36 blocks ,18370 bytes

monitor#

It shows that you have successfully upgrade your software.

1.1.4   upgrade configurations

The configurations of router save as file, the file name is startup-config, User can use instructions like software upgrading to upgrade configurations.

1. By TFTP negotiation

monitor#copy tftp flash:startup-config

2. B．by serial interface communication negotiation

monitor#download   c0   flash:startup-config

1.2   Basic system management

1.2.1   configure ethernet IP address

monitor#ip address <ip_addr> <net_mask>

This instruction is used to configure Ethernet IP address, default is 192.168.0.1,

Network mask is 255.255.255.0

Parameter explain

Parameter	Description
ip_addr	Ethernet IP adderss
net_mask	Ethernet network mark

Example

monitor#ip address 192.168.1.1 255.255.255.0

1.2.2   configure default router

monitor#ip route default <ip_addr>

This instruction is used to configure default router, it can configure only one default router.

Parameter explain

Parameter	Description
ip_addr	IP address of gateway.

Example

monitor#ip route default 192.168.1.1

1.2.3   Use "ping" to test network connecting state

monitor#ping   <ip_address>

This instruction is used to test network connecting state.

Parameter explain

Parameter	Description
ip_address	target IP address

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

startup from a file by hand

monitor#boot flash <local_filename>

This instruction is used to startup some router software in FLASH, There are maybe many router softwares in FLASH.

Parameter explain

Parameter	Description
local_filename	File name saved to FLASH, user must input file name.

Example

monitor#boot flash router.bin

1.3   HTTP Configueration

This chapter explains how to configure   http in router.

1.3.1　Enable http service

Default http service is closed.

use the following command　under global configuration mode will enable http service :

Command	Function
ip http server	Enable http service

1.3.2　Change http service port number

Default http service monitor port is 80.

Use the following command under global configuration mode to change http service port number:

Command	Function
ip http port number	Change http service port number

1.3.3　Configure http service access password

HTTP uses enable password as an access password. To authenticate http access, you must configure enable password. Use the following commands under global configuration mode to configure enable password:

Command	Function
enable password {0|7} line	Configure enable password.

1.3.4　Appoint access control list for http service

To control the access from host to http service, users may appoint access control list to http service. Use the following command under global configurtion mode to appoint access control list to http service:

Command	Function
ip http access-class string	Appoint access control list for http service.

1.3.5　Access and use web client interface

This section explains how to access web client interface and how to execute commands with web interface.

1. Preparation before access

    (1)　make sure the version of the browser on the pc is 5.0 or above.if "Web console"is used ,you must install Java2 v1.4.1 plug.(you can get the plug　from http://java.sun.com/products/plugin/index.htmlor from my compony).

    (2)　make sure a directory named "html" exists in router root. If not, establish the directory.

(3) copy the documents offered by network management team to the html directory in router. These files include: WEBR.jar, jh.jar, homepage.html, default.html, not_supported.html, and Redirect.class.

(4) enable http service under configuration mode in the router. Specific commands is : "ip http server". For details about configuration, refer to "http configuration command directory".

2. Access router homepage

Follow the steps below to access router homepage.

(1) Enter **Error! Hyperlink reference not valid.** in the url window of web browser.

(2) If the router is configured with enable password, the browser will prompt to input password. Fill in enable password and press enter (user name is not necessary).
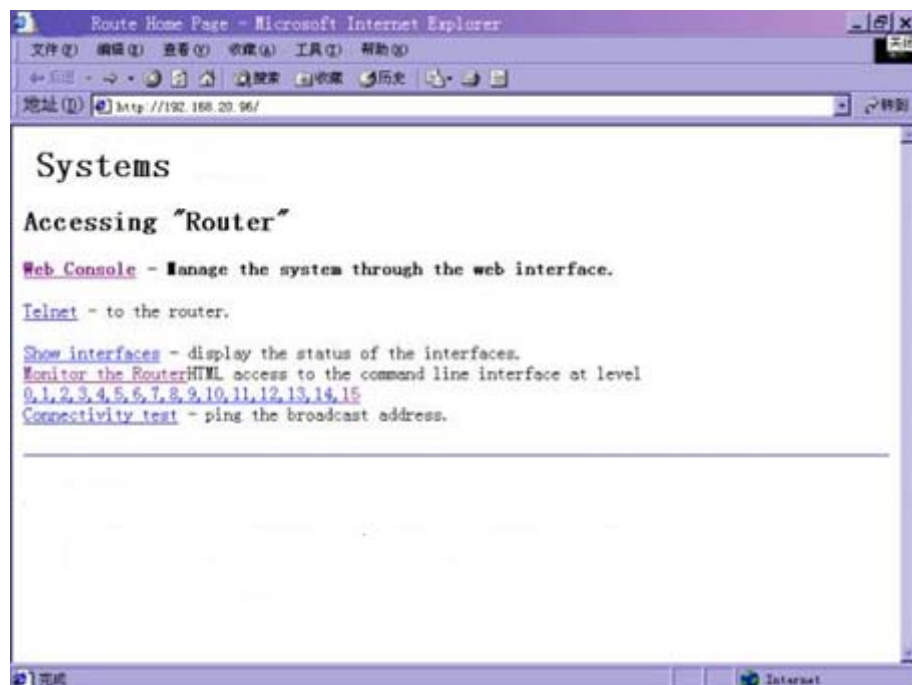
Figuer 1-2 The browser of router homepage

3. Link to Homepage

- web console

  Click on the Web Console. Enter into waitting interface. When the system configuration (such as IE 5.0 or later, JAVA 1.3 or later) meets system requirements, system enters EMS (Equipment Management System) client interface after setup. For detail, refer to "Execute commands with web console interface".

- telnet

  Click the link to enable system default telnet client tools. Request for telnet service on No. 23 tcp port.

● Show interface

Click the link to output the result of executing the command—"show interface." For detail, refer to "Execute command with web browser".

● Monitor the Router

Click the link to display command interface under privilege mode. Click the following hyperlink to enter the corresponding command input interface under supervisor mode. For detail, refer to "Execute command with web browser".

● Connectivity test

Click the link, the router will execute "ping 255.255.255.255" and display the executable result.

● Help resource

4. Execute command with web browser user interface

On the router homepage, click the hyperlink with title number is 0 to 15 and enter the corresponding privilege configuration mode. There is a command area on the page. Users may input command following the instructions on the command line. The page also display command list hyperlink. By clicking the hyperlink to execute corresponding command.

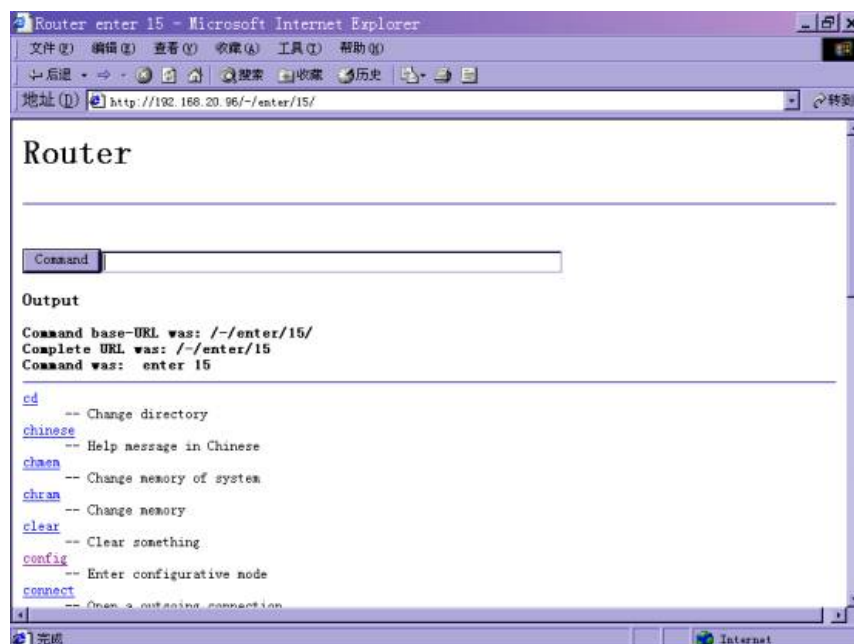

Figuer 1-3 the router homepage of command

5. Input command with hyperlink

To input command with hyperlink, scroll the screen to find the command hypertext and click the hypertext you want. If the hypertext is a complete command, command will be executed. If the command requires more parameters, it will display another hyperlink table. Click on the command link on the second hyperlink table.

If the command input is to display some information such as "show arp" command, web browser windows will display output information.

If the command input requires a "variable", it will display a table for you to input "variable".

6. Use command area to enter command

input command with command area is similar to input command with terminal. Use the syntax described in command index to input commands. To know items under a certain command, users may enter "?" to inquire.

For example, enter "show ?" under command area. The parameter list of "show" command is displayed. The parameters are displayed by hyperlink. To enter these parameters, you can click on the hyperlinks or input commands and parameters in the command area.

7. Enter commands with url window

Users may execute commands with url window of web browser.

Executing command with url window should use the following syntax:

http://router_ip/-/[enter/level/][command-mode/][command]

Parameter	Description
Router_ip	Ip address of the router
enter/*level*	(optional)Privilege for accessing
mode	(optional)The mode under which the command is executed, such as config. If not specified in url, the default is supervisor mode.
command	(optional)the command needed to be executed. Use "/" to replace the space in the command line syntax. If command is not specified in url, it will display a hyperlink list table page including all possible command under current mode.

For example, to execute "show arp" privilege mode command in router with ip address is 192.168.20.96, users need to enter the following character string in url window:

http://192.168.20.96/-/show/arp

After executing the command, web browser will display the arp cache list on the router.

The difference between entering command in url window and command area is that the former uses "/" to replace space in the command syntax.
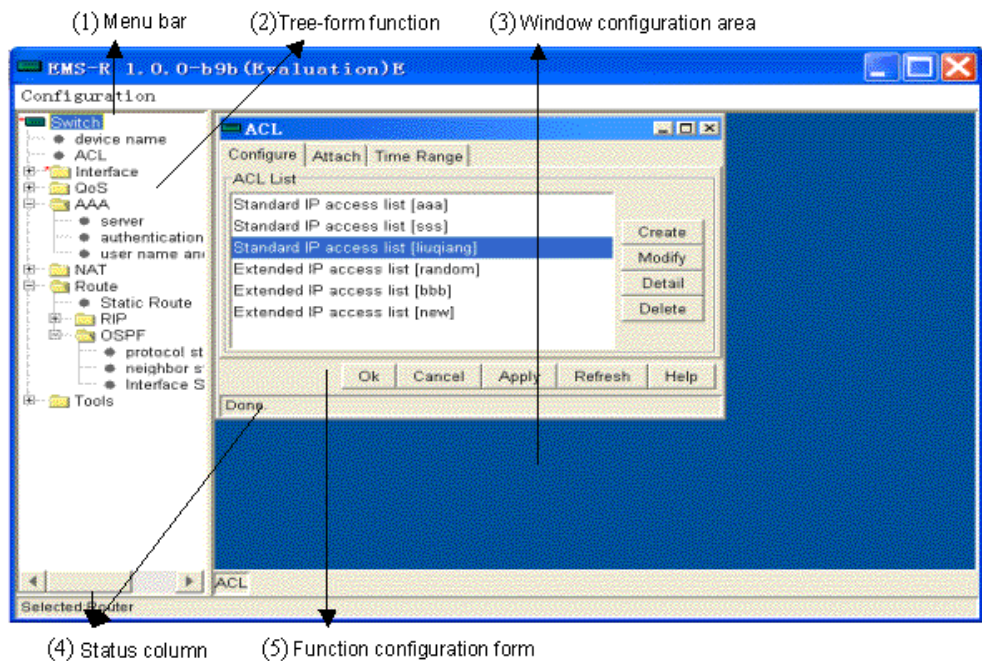
1.3.6   Execute command with web console interface

1. Preparation before access

make sure the pc running browser has installed Java2 v1.4.1 plug.(you can get the plug from http://java.sun.com/products/plugin/index.htmlor from my compony).

2. Client interface

When you use EMS, you may see the following components on the client main interface.

Figuer 1-4 Client interface

- Menu bar (1): On the upper side of the main interface.It contains basic operations.

- Tree-form function area (2) and Window configuration area (3),they are in the center of the main interface. the Tree-form function area is on the left side and Window configuration area is on the right side. The Window configuration area display function configuration form (figure 5). Tree-form function area (2) has many different functions. When you click on a node, the Window configuration area (3) displays the corresponding function configuration form.and the bottom of Window configuration area (3) displays the currently active form.

  In EMS, configuration task are working in function configuration form.

- Status column (4): In the bottom of the main interface and the bottom of function configuration menu(5). When you select a node on the tree, the bottom of the main interface will prompt "selected: ####" ;When you click on the node to enable function configuration form, the bottom of the configuration form will prompt "processing, please wait…", When the form finishes enable, the status column will prompt "done",which means the form can be configured then..

- Function configuration form (5): When buttons and other components are in gray color, they are disabled. The button "OK" is used to accept the current configuration and close the window. "Close" is used to cancel the current configuration and close the window. "Help" is used to display related use help. "Refresh" is used to display the latest data. "Apply" is used to make the configuration work while keeping the form unchanged. When you make wrong configurations, the system will prompt accordingly. Shown as follows (the figure is prompt window of different interface style).

1.3.7 Function configuration example

1. Configure expanded access list
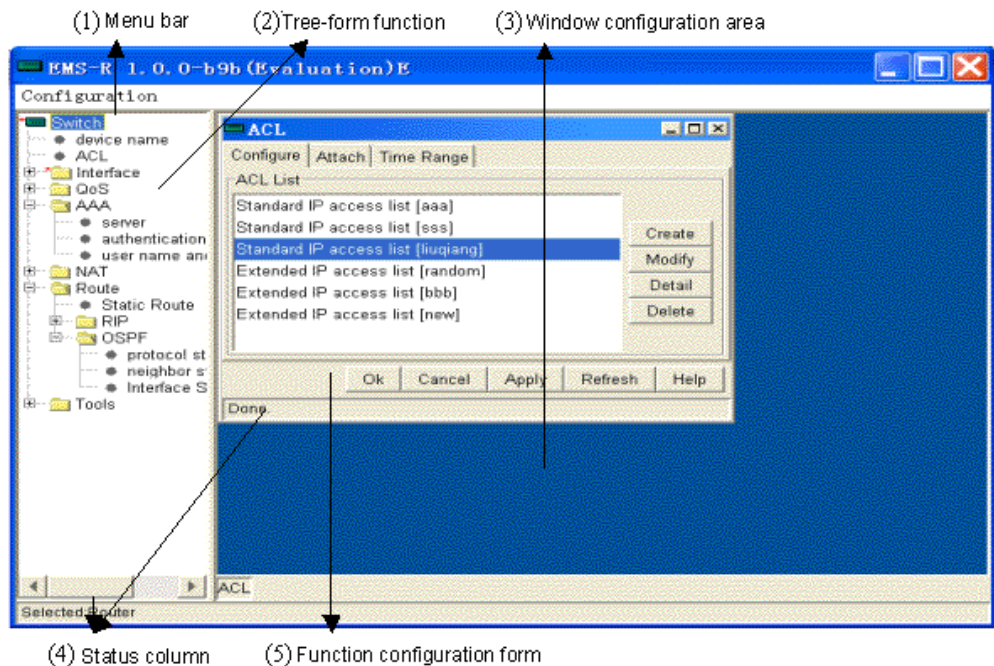
Figuer 1-5 Configure expanded access list

(1)   Click on the ACL node on the Function tree and ACL window will display. The access list of current router will display in the configuration page.

(2)   Modify an item in the access list: "Extended IP access list [random]". Select and click the "Modify" button.   "Modify ACL" window displays.

(3)   Click "↑" or "↓" button to adjust the order in "random" members, modify members. Select "permit ip any any", enters "Extended IP" sub-window.

(4)   Modify attribute area based on needs, such as set the sender's address to "192.168.33.1", the sender mask to"255.255.255.0".

(5) Click the "OK" button under the window to accept modifications. Click "Cancel" to cancel modifications.

2. Configure authentication server group in AAA
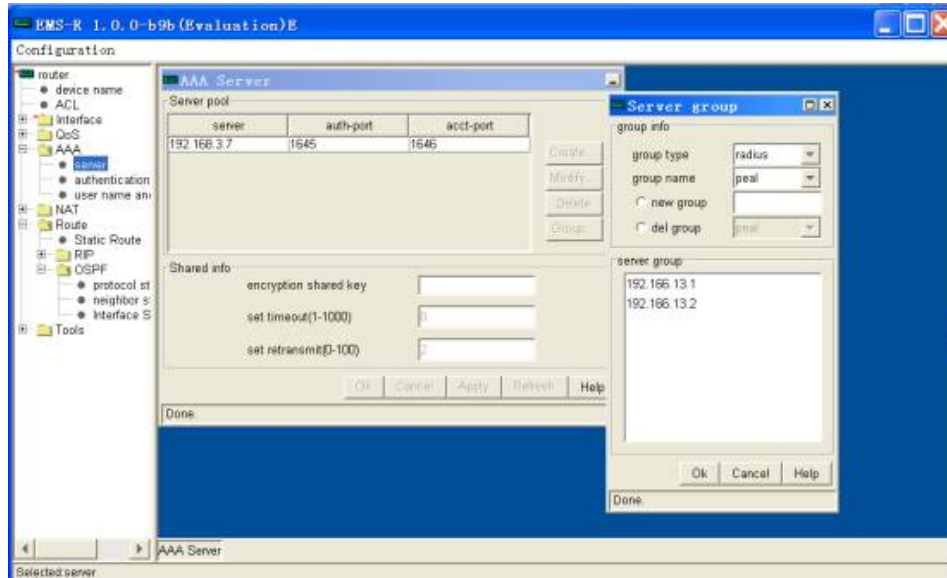
Figuer 1-6 Configure authentication server group in AAA

(1) Click node "AAA > Server" on the function tree. "Server pool" displays the current radius server list. "Shared info" is the shared attribute of radius server.

(2) Modify the item"192.168.3.7" in the list. Select the item and click the button "Group" and "Server group" sub-window displays. The selected group member are displayed under "Server group".

(3) Select server group based on needs. Such as select server group type to "radius", select server group name to"peal".

(4) Click the "OK" button under the window to accept modifications. Click "Cancel" to cancel modifications.

3. Save configuration

If you want to retain the current configuration next time you boot up, click click the item on the menu: Configuration > Save Configuration.

4. Exit

Close the brower or click the item on the menu: Configuration > Exit.

Chapter 2   Terminal Configuration

2.1   VTY configuration description

Router use line command to set terminal parameters simply and neatly; such as width and height, configuration courses are adapted to users' custom.

This chapter will introduce how to configure the VTY(virtual terminal)on the Router. Details about commands for configuring the VTY, please refer to   "VTY configuration commands".

2.2   Configuration tasks

Router has four kinds of cables: console ,aux, asynchronous and virtual terminal .The different routers have different numbers. User can refer to software and hardware configuration references below   to properly configure equipment:

Cable	Interface	Description	Rules of line code
CON(CTY)	console	use to login the router to configure	Code= 0
AUX	assistant	RS-232 DTE interface, an asynchronous interface to backup,can not be used as a second console	Code=65，if the slot number<=4, otherwise Code="slot number "multiple 16 +1
TTY	asynchronism	Asynchronous interface, often used in the dial sessions of SLIP,PPP	Incept number is 1. Serial number differs from different console. Range is maximum asynchronism interfaces supported by a router. For instance ， there are 16 asynchronism module on slot 1,null on slot 2,8 synchronization module. So,a1/0 line 1， a1/15 is corresponding to line 16，s3/0 is corresponding to line 17，s3/7 is corresponding to line 24。
VTY	Virtual-asynchronism	Use to link to sync ports of routers, such as Telnet,X.25 PAD 、 HTTP and Rlogin on Ethernet & serial interface	64 numbers begins from maximum TTY cable number +1

relationship between line and interface:

- asynchronism interface and TTY line

- synchronization interface and VTY line

asynchronism interface and TTY asynchronism interface are corresponding to physical interminal line[TTY].   When asynchronism interface does not enclapsulation protocols, it can be connected to intermial.

synchronization interface and VTY line: Virtual interminal line provide accessing to a router by synchronization interface. VTY line is not corresponding to synchronization interface as TTY line to asynchronism interface. This is because VTY line is dynamic created on router,while TTY line is a static physical port. When a user try to link to router by VTY line, he is tring to connect a virtual interface. There are several virtual interfaces to each synchronization interface.

For example, several Telnet connect to one interface(Ethernet or serial interfaces).

You need to do following steps to configure VTY:

- enter the configuration mode

- configure the terminal parameters

Refer to "Examples of VTY configuration" to know more about VTY configurations.

2.3   monitor and maintain

Users can use "show line"command   to check the configuration of VTY.

2.4   Examples of configuration

2.4.1   Example of TTY configuration

The commands configure the line width and lines of screen on terminal on tty1-tty10.If user login from this interface ,the prompt "more" will appear every 40 lines, and a newline will be displayed after 132 charaters;

config#line tty 1 10
config_line#width 132
config_line#length 40
Configure s1/0 to TTY interface:
config_s1/0#physical-layer mode async
config_s1/0#async mode interactive

Such a configuration use back to back cable to connect s1/0 directly. If you want to telnet with modem, you should configure line dial before you the command "async mode interactive".

2.4.2   Example of VTY configuration

The following configuration will cancel the VTY limitation to lines of each screen and will not prompt the "more".

config#line vty 0 63
config_line#length 0

Chapter 3 Network Management Configuration

3.1 Configuring SNMP

Details about instructions of this chapter ,refer to "SNMP instructions".

3.1.1 Overview

SNMP system include three parts:

- SNMP management end

- SNMP AGENT

- management information base

SNMP is a protocol for the application layer. It provides message format Which are transferred between network management end and AGENT.

The SNMP network management end is a part of network management system(NMS,such as the Works).Because the AGENT and MIB are on the Router, it's necessary to define the relationship between the network management end and   the AGENT if users want to configure the SNMP of the Router.

SNMP AGENT include MIB variables, SNMP management end can retrieve and and change these variables values. SNMP management end can get variables values from AGENT or save variables values to AGENT.   AGENT collects data from MIB. MIB is an information base of network data and devices parameter.The agent responds to the request of the network management end for reading or setting data. The agent can send the trap forwardly to the management end . Trap is a kind of alarm message which will give an alarm to the management end in some network condition .Trap can point out the incorrect user authentication, reset, link status(up or down),TCP link closing, link losing with neighbor Routers or other important   events.

1. SNMP   inform

Router can send inform to the management end when special event happens. For an example, agent router may send a message to the management end when it meets an error.

SNMP inform can be sent as trap or inform request. The receiver does not respond to the trap ,and the transmitter doesn't judge whether the trap is received, so the trap is not credible.

On the contrast , when receiving inform request, the management end responds with SNMP response PDU. The management end won't give any response if it does not receive a inform request, and if the transmitter doesn't receive any answer ,it will send the inform request again. So ,the inform will reach tageted destination more possible.

The inform requests consume more resources of the Router and network for their credibilities. The traps will be rejected once they are been sent. On the contrast, inform request must be saved in the memeory until receiving the response or the request is time out. And the trap will be sent only once while the inform request can be send for several times. Resend add network communication and aggravate network traffic. So ,the trap and inform request provide a balance between credibilities and resources of network.

If it is necessary for the SNMP management end to receive each inform ,the inform request should be used. If care for the network traffic or memory of the Router ,and it is not necessary to receive each inform, trap can be used.

Router only support trap now , but it provides the extension of using inform request.

2. SNMP version

SNMP versions supported by Routers are :

- SNMPv1—a simple network management protocol, a absolute internet standard, defined in RFC1157.

- SNMPv2C-- SNMPv2 Administrative Framework based on team, an test internet protocol, defined in RFC1901

SNMP versions supported by Our company:

- SNMPv3 。

SNMPv1 use safety format based on team. It can access agent MIB'S management end team.

It's necessary to set the SNMP agent to the version supported by the management station. AGENT can communicate with serveral management ends.

3. supported MIB

SNMP of Routers support all MIB variables (described in RFC1213) and SNMP traps (described in RFC1215).

Router provides a private MIB extension for each system.

3.1.2   Configuration lists

- create and modify accessing control for SNMP group

- set manager contact ways and location of this router

- define maximam length of SNMP agent data packet

- monitor SNMP status

- configure SNMP traps

3.1.3   Configuration tasks

1. create or modify access control for SNMP team

The SNMP team character string can define relationship between the SNMP management end and AGENT. Team character string is similar to the password which is used to access the Router AGENT. Users can designate one or more characters associated with team character string below(optional):

the IP address access list of SNMP management end permitting to use team character string to acquire the authority for accessing the AGENT .

Define the MIB tree of all the leaf nodes which have the authority for accessing the designated team.

Appoint the read-write authority of the MIB object that has the access authority

The commands used to configure the team character string in the overall configuration mode are given below:

Command	Function
snmp-server community string [view view-name] [ro	rw] [word]	Define team access character string

Users can configure one or more team character strings and can use "no snmp-server community"command to delete the default team character strings.

The example of configuring the team character string ,refer to the chapter" SNMP commands".

2. Configure the way to contact the Router manager and location of the Router.

"sysContact" and "sysLocation "are both the management variables of MIB system group. They define the sign of the node(Router) manager and his location. Those information can be accessed by configuration files. Users can use one or more commands below in the overall configuration mode :

Command	Function
snmp-server contact text	set the node manager string
snmp-server location text	Set the node location string

3. Define the maximum length of the SNMP agent data packet:

The SNMP agents set the maximum length of data packet when receiving request or sending response. Users can use one or more commands below in the overall configuration mode :

Command	Function
snmp-server packetsize byte-count	set the maximum length of data packet

4. monitor SNMP status

Users can use one or more commands below in the overall configuration mode to monitor the SNMP input/output statistics, including forbidden team string and the number of errors and request variables.

Command	Function
show snmp	Monitor SNMP status

5. configure SNMP trap

Users can use the following commands to configure the Router's sending the SNMP Traps(the second task is optional):

●   configure the Router to send SNMP traps

Users can use one or more commands below in the overall configuration mode to configure the Router to send SNMP traps to a host:

Command	Function
snmp-server host host community-string [trap-type]	Designate the receiver of the traps

The SNMP agents will startup automatically after our company has powered on , and all kinds of the traps will be activated. Users can use"snmp-server host" command to designate a host to receive appointed types of traps.

Some traps need to be controlled by other commands. For example, if users want to send SNMP traps when interface is up or down, user should use "snmp trap link-status"command to activate the link traps in the interface configuration mode ,and use "no snmp trap link –stat" command to shut off these traps.

To receive the traps ,the host must be configured with "snmp-server host"command.

●   alter the running parameters of the traps

It is an optional item, and it can designate the source interface generating the traps and the length of message(data packet)queue or the value of retransmission interal for every host.

Users can use optional commands below to alter trap running parameters in the overall configuration mode :

Command	Function
snmp-server trap-source *interface*	designate the source interface. and the source IP add
snmp-server queue-length *length*	set the length of message queue for each host. Default value is 10
snmp-server trap-timeout *seconds*	Define the retransmission frequency of traps in retransmission queue. default value is 30 seconds

3.1.4   Configuration Examples

1. Example 1

snmp-server community public RO

snmp-server community private RW

snmp-server host 192.168.10.2 public

We configure two team strings-"public" and "private"."Public" has the authority of reading all the MIB variables . While "private" has the Authority of reading and writing all the MIB variables.

Users can use "public"to read the MIB variables of the Router and use"private"to read the MIB variables of the Router and use "private"to write some wirtiable variables.

It designate the Router to use "public" to send traps to "192.16.20.2" when the Router need to send traps also.. For example ,when some interface is down, the Router will send a linkdown trap to "192.168.20.2".

2. Example 2

snmp-server community public view sysmib RO

snmp-server community private RW nativehost

snmp-server contact router@company.com.cn

snmp-server host 192.168.10.2 public snmp

snmp-server location 405-room

snmp-server view sysmib system included

ip access-list standard nativehost

permit 192.168.10.2 255.255.255.255

In this example, "public"only has the authority Of reading the MIB variables in system group of the Router. It only permit the host whose IP address is 192.168.10.2 to use"private" to read or write MIB variables of router.

Only send snmp trap to the host"192.168.10.2" and do not send authentication or configure traps.

The contact way should be configure to router@company.com.cn, and location should be configured to 405-room,that is to say, "sysContact" in MIB is router@company.com.cn and "sysLocation"in MIB is 405-room.

3.2   Configuring RMON

This chapter explains how to configure rMon on router.

3.2.1   Configuration lists

- Configure RMon Warning on a router

- Configure RMon Event on a router

● Configure RMon Statistics on a router

● Configure RMon History on a router

● Display RMon configuration of a router

3.2.2 Configuration tasks

1. Configure rMon Warning on a router

Users may configure rMon with command line or SNMP network management. If you want to make configurations with SNMP network management, you have to configure SNMP to the router in advance. After finishing the warning configuration, the device can monitor some statistics. To configure rMon Warning, follow the steps below:

Command	Function
configure	Enter Global Configuration Mode
rmon alarm index variable interval {absolute | delta} rising-threshold value [eventnumber] falling-threshold value [eventnumber] [owner string]	To add an rMon Warning item "index" ranges from 1 to 65535, which is the item index "variable" is an MIB object, which is under monitored. A variable must be a valid MIB object and only 2 types of MIB objects, "INTEGER.Counter.Gauge" or "TimeTicks", can be inspected "interval" is the intermission for sampling (in seconds) with available value from 1 to 4294967295 Use "absolute" to inspect the value obtained by MIB objects, and use "delta" to inspect the variations between values "value" is a "threshold value" for alerting a warning, and the corresponding "eventnumber" (optional) is the event index when the threshold value is reached An "owner string" is the descriptive information of the warning
exit	Back to Supervisor Mode
write	Save the configurations

After finishing one warning item, the device will obtain the "oid" specified by "variable" every "interval second". System will make comparison between the obtained value and the previous one according to the type of warning (absolute or delta). If the obtained value is higher than the previous value and higher than the "threshold value" specified by "rising-threshold", an event with an index as "eventnumber" will be launched. (No event will be launched if the value of "eventnumber" is zero or there is no event that has "eventnumber" as its index.) The above situation happens in descending values as well. If the "oid" specified by "variable", this warning item status will be set to "invalid". If users configure the Warning item of the same index with "alarmcommand" more than once, only the latest parameter is valid. Please use "no rmon alarm indexcommanddelete" as the warning item for "index".

2. Configure RMon Event on a router

To configure the rMon Event, follow the steps below:

Command	Function
configure	Enter Global Configuration Mode
rmon event index [description string] [log] [owner string] [trap community]	To add a rMon Event item "index" ranges from 1 to 65535, which is the item index "description" is descriptive information for the event "log" will add a piece of information in log table when the event is launched. "trap" means when an event is launched, a trap also takes place; "community" is the name of the group An "owner string" is the descriptive information of the event
exit	Back to Supervisor Mode
write	Save the configurations

After configuring an rMon event, when an rMon warning is launched, replace "eventLastTimeSent" with "sysUpTime" in this event table. If the event has been configured a long attribute, add a piece of information in the log table. If a "trap" attribute is configured, launch a trap with "community". If users configure the same Event item of the same index with "rmon eventcommand" more than once, only the latest parameter is valid. Use "no rmon event indexcommanddelete" as an event item index.

3. Configure RMon Statistics on a router

RMon Statistics is used for inspecting statistics obtained from each device. To configure rMon Statistics, follow the steps:

Command	Function
configure	Enter Global Configuration Mode
interface iftype ifid	To enter Interface Configuration Mode iftype is a type of interface ifid is an interface id
rmon collection stat index [owner string]	To enable Statistics on the interface "index" is the statistics item index An "owner string" is the descriptive information of the statistic
exit	Back to Global Configuration Mode
exit	Back to Supervisor Mode
write	Save the configurations

If users configure the Event item of the same index with "rmon collection statcommand" more than once, only the latest parameter is valid. Use "no rmon collection stats indexcommanddelete" as a statistics item index.

4. Configure RMon History on a router

RMon History is used for collecting statistics from one interface in different time period. To configure rMon History, follow the steps:

Command	Function
configure	enter global configuration mode

interface iftype ifid	enter interface configuration mode
	
	    iftype is the type of interface
	
	    ifid is the id of interface

rmon collection history index [buckets bucket-number] [interval second] [owner owner-name]	To enable Statistics on the interface.
	
	    "index" is the history item index
	
	    Keep the latest "bucket-number" item in the collected history record. Users may visit Ethernet History Record to obtain the statistics. Default number of records is 50.
	
	    "second" is the interval between obtaining statistics. Default value is 1800 seconds (30 minutes)
	
	    An "owner string" is the descriptive information of the History table.

exit	Back to Global Configuration Mode
exit	Back to Supervisor Mode
write	Save configuration

After adding one History item, the device will obtain the statistics from the specified interface every specified seconds according to "second" and add the result to Ethernet History Record as an item. If users configure the "History" item of the same index with "rmon collection history indexcommand" more than once, only the latest parameter is valid. Notice that if you use "no rmon history indexcommanddelete" as History item index, a great "bucket-number" and short "interval second" will occupy too much system resource.

5. Display rMon configuration of a router

Display rMon configuration of a router with "showcommand":

Command	Function

show rmon [alarm] [event] [statistics] [history]	To display rMon configuration information
	
	    "alarm" is the Warning item configuration
	
	    "event" is Event item configuration. Log items resulted from launching an event are also displayed.
	
	    "statistics" is that when Statistics item configuration is displayed, statistics collected from the interface are also diaplayed.

	"history" represents that when a History item configuration is displayed, statistics collected between the intervals are also displayed.

3.3 Configuring PDP

3.3.1 Overview

This chapter will introduce how to configure PDP of a router.

PDP is a two-layer protocol specially for detecting network equipments, is used to discover all neighbors of a known equipment in network management program. Users can know type and agent address of SNMP of neighbor equipment through using PDP. The network management program can query the neighboring devices for information about the topology services by SNMP.

Though the PDP of Routers can discover the neighboring devices , it can not Use SNMP to query neighboring devices. So, We can only be the edge of network, or ,it will not get the full network topology.

PDP on a router can configure to all SANP (such as Ethernet, HDLC, frame relay,PPP).

3.3.2 Configuration lists

- Default PDP configuration on a router

- Set PDP clock and holdtime

- Enable PDP on a router

- Enable PDP on a router's interface

- Monitor and manage PDP

3.3.3 Configuration tasks

1. Default PDP configuration on a router

function	default
PDP overall configuration mode	down
PDP interface configuration mode	down
PDPclock(transmit frequency)	60 seconds
PDP hold time	180 seconds

2. Set PDP clock and holdtime

Users can use following commands to set PDP transmit frequency and holdtime in overall configuration mode:

Command	Function
pdp timer s*econds*	Set PDP transmit frequency
pdp holdtime *seconds*	Set PDP holdtime

3. Enable PDP on a router

If in default ,PDP is down, user can start PDP through using following command in overall configuration mode:

Command	Function
pdp run	Start PDP on a router

4. Enable PDP on a router's interface

If in default, PDP is down, after starting PDP on a router, users can use following commands to start PDP in interface configuration mode:

Command	Function
pdp enable	start PDP on a router's interface

5. Monitor and manage PDP

Users can use following commands to monitor PDP:

Command	Function
show pdp traffic	display the count of PDP tansmitted and received by the Router
show pdp neighbor [detail]	Display neighbors of the router discovered by PDP

3.3.4　Examples of PDP configuration

1. enablel PDP

Router_config# **pdp run**
Router_config# **int f0/0**
Router_config_f0/0#**pdp enable**

2. Set PDP clock and holdtime

Router_config# **pdp timer 30**
Router_config# **pdp holdtime 90**

3. Monitor PDP information

router# show pdp neighbors
Capability Codes:R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H -
Host, I - IGMP, r - Repeater
Device ID Local IntrfceHoldtmeCapabilityPlatform Port ID
joeEth 0 133 4500 Eth 0
samEth 0 152 R AS5200 Eth 0