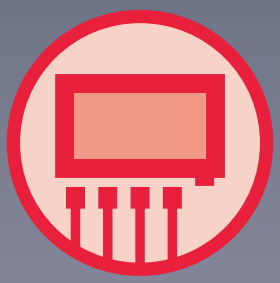
Signamax Security Router

Model: 065-1530



Active

Configuration Guide

Revision A1

SIGNAMAX™
CONNECTIVITY SYSTEMS

Table of Contents

Router Concepts

This chapter explains concepts of InfoExpress IOS system in Signamax router series such as InfoExpress system mode, configuration environment and CLI.

Configuration Modes

Signamax routers provide users with four configuration modes:

Configuration using the command shell via console interface

Configuration via LINE interface of 56/336 modem module

Configuration via telnet remote log in a router

Configuration via SNMP network management system

The configuration mode - configuration via SNMP network management system - provides users with English interface to monitor network status and collect system statistical information.

The manual also explains router configuration mode via interface console. The other two modes, which configure the router via LINE interface in 56/336modem and telnet remote login, are similar.

The configuration via SNMP refers to the router network management system specifications.

Command Line Mode

InfoExpress IOS of Signamax router series provides a special subsystem dealing with commands for management and execution of system commands called shell. Following are the shell functions:

System command registration

User edit of system configuration commands

Syntax parsing of commands input by users (via interface console or telnet link)

System command execution

When a user configures router via command shell, the system provides many run modes for command execution. Each command mode supports the special InfoExpress IOS configuring command. This protects system hierarchy and ensures protection against unauthorized access to the system.

The shell subsystem provides the following modes for running configuring commands. Each different mode relates with a different system prompt informing users about their operating mode. The modes are:

Common user mode (user EXEC)

Privileged user mode (privileged EXEC)

Global configuration mode (global configuration)

Interface configuration mode (interface configuration)

Route configuration mode (route configuration)

File system configuration mode (file system configuration)

Access list configuration mode (access list configuration)

Voice-port configuration mode (voice-port configuration)

Dial-peer configuration mode (dial-peer configuring)

Encryption transform configuration mode (crypto transform-set configuration)

Encryption mapping configuration mode (crypto map configuration)

IKE policy configuration mode (isakmp configuration)

Pub key chain configuration mode (pubkey-chain configuration)

Pub key configuration mode (pubkey configuration)

DHCP configuration mode (DHCP configuration)

The following table lists methods of entering different command modes and how to switch between modes. The InfoExpress system modes and switch methods between modes are:

Mode	Entering mode	System prompt	Exiting	Function
Common user mode	Login	router>	Execute command exit to exit	Alters terminal configuration Executes the basic testing Displays system information
Privileged user mode	Execute command enable in the common user mode	router#	Execute command disable to come back to the user mode Execute command configure to enter the global configuration mode	Configures executing parameters of the router
Global configuration mode	Execute command configure in privileged user mode and specify related keyword at the same time	Router(config)#	Execute command exit to come back to the privileged user mode Execute command interface to enter the interface configuration mode	Configures global parameters needed for the router running
Interface Configuration mode	Execute command interface in global	router(config-if-xxx[number])#	Execute command exit to come back to the privileged user mode	Config u r

	configuration mode (and designate related interface at the same time)			es interface of the router in the node, incl

				u d i n g Ethernet interface, serial interface, ISDN Configures the interface IP phone; Configures the interface E1
Routing configuration mode	Execute related route configuring command in global configuration mode	router(config-static)# router(config—rip)# router(config-ospf)# router(config-irmp)#	Execute command exit to return to the privileged user mode	Configures IP routing protocol in the mode, including Static routing, RIP dynamic routing, IRMP configuration mode
File system configuration mode	In global configuration mode, a user enters this mode via command filesystem	router (config-fs)#	Execute command exit to return to the privileged user mode	Finishes file system management of the router Upgrades the router software
Access list configuration mode	In global configuration mode, a user enters the mode via command ip access-list, and designates related keys and parameters	router(config-std-nacl)# router(config-ext-nacl)#	Execute command exit to return to the global configuration mode	Configures access list of the firewall, including standard access list, extended access list
Voice-port configuration mode	In global configuration mode, a user enters the mode via command voice-port, and designates related parameters	router(config-voice-port)#	Execute command exit to come back to the global configuration mode	Configures voice-port

The dial-peer configuration mode	In global configuration mode, a user enters the mode via command dial-peer, and designates keys and parameters	router(config-dial-peer)#	Execute command exit to come back to the global configuration mode	Configures VoIP Configures POTS
The encryption transform configuration mode	In global configuration mode, a user enters the mode via command crypto IPsec transform-set, and designates related parameters	router(cfg-crypto-trans)#	Execute command exit to come back to the global configuration mode	Configures the encryption transform set
The encryption mapping configuration mode	In global configuration mode, a user enters the mode via command crypto map, and designates related keys and parameters	router(cfg-crypto-map)#	Execute command exit to come back to the global configuration mode	Configures the encryption mapping items
The IKE policy Configuration mode	In global configuration mode, a user enters the mode via command crypto isakmp, and designates related keys and parameters	router(config-isakmp)#	Execute command exit to come back to the global configuration mode	Configures IKE policy
The public key chain configuration mode	In global configuration mode, a user enters the mode via command crypto key pubkey-chain rsa	router(config-pubkey-chain)#	Execute command exit to return to the global configuration mode	Configures RSA public key to be used
Public key configuration mode	In config-pubkey-chain mode, a user enters the mode via command named-key or addressed-key and designates related keys and parameters	router(config-pubkey-key)#	Execute command exit to return to the config-pubkey-chain mode	Configures public key

DHCP Configuration mode	In the global configuration mode, a user enters the mode via command router(config)#ip dhcp pool, and designates keywords and parameters	router(dhcp-config)#	Execute command exit to return to the global configuration mode	Configures DHCP

The word router is the default system name of a router when it leaves the factory. Users rename the system name by executing the command hostname in the global configuration mode. The change goes into effect immediately.

Configuration Environment

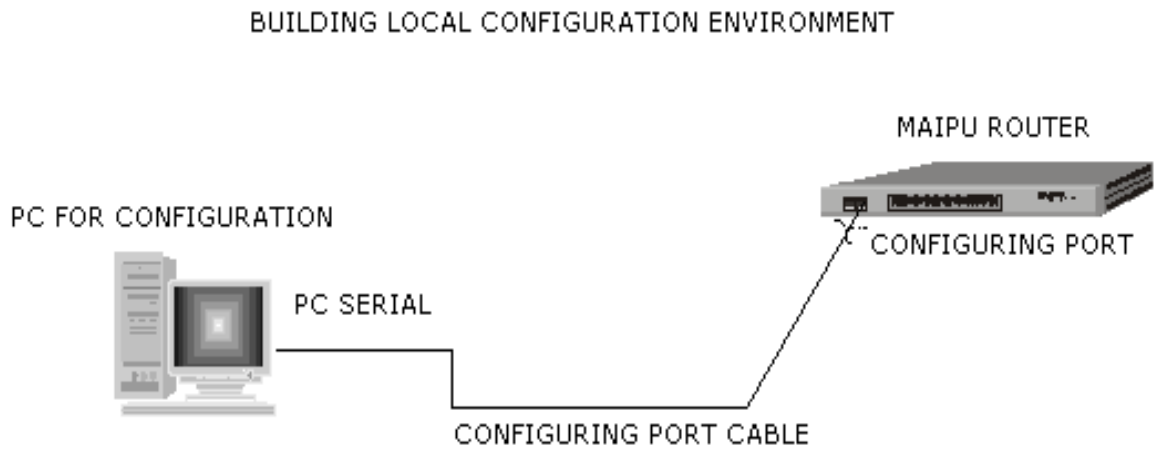
Users use the command line provided by a router in four different ways.

Configuring Router via Console

Following are steps to connect with a terminal and configure the router via port console:

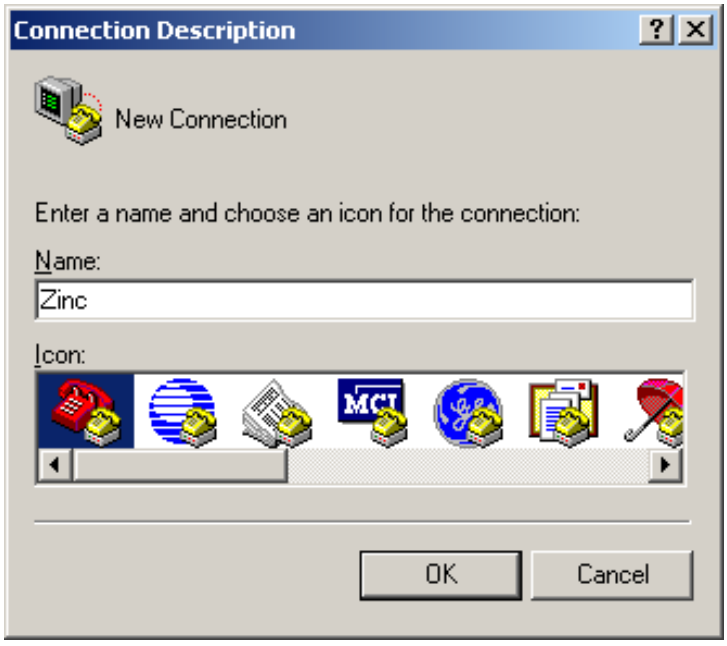
The terminal can be a standard one with RS-232 serial port or a common PC. When configuring from remote-end, users need two more modems.

After ensuring shutdown of the router or terminal, connect RS-232 serial port of the terminal with the router console port.



Creating connection:
Choose a name for the connection – Signamax or choose other name.

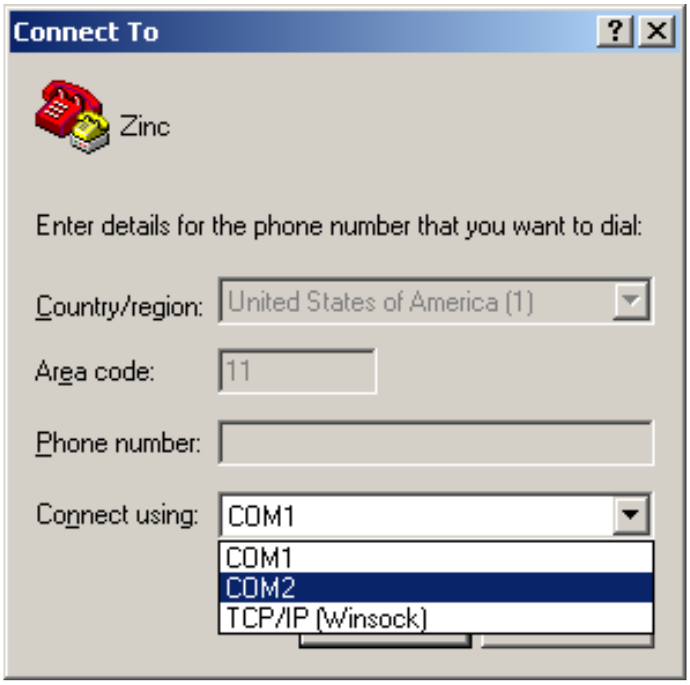
Choosing Windows icon for created connection:



Power up the terminal, configuring communication parameters of the terminal: 9600bps baud rate, 8 data bits, no parity, 1 stop bit, and no flow control. Choose VT100 as the type of terminal.

If the PC is running Win95/98/2000/NT Operating System, use the Hyper Terminal program and set serial port parameters of HyperTerminal program according to above parameters.

The following example explains the HyperTerminal program running in Windows NT:



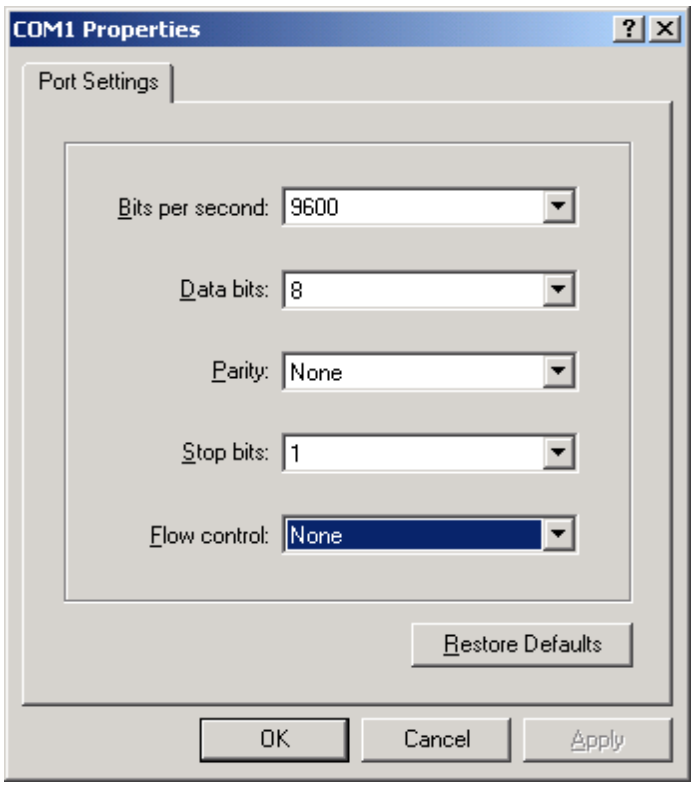
Choosing serial communication port:

Configuring parameters of the serial communication port:

Baud ratio (bits per second) - 9600bps
Data bits - 8
Parity - no
Stop bit - 1
Flow control - None

Choosing serial communication port:
This example explains configuration communication parameters of HyperTerminal program:

Choose COM1 or COM2 according to the serial port connected.



Configuring parameters of the serial communication port:

Power on the router and press Enter key. A prompt "router>" displays on the terminal, allowing router configuration.

Configuring via 56/336 Modem Module LINE Port

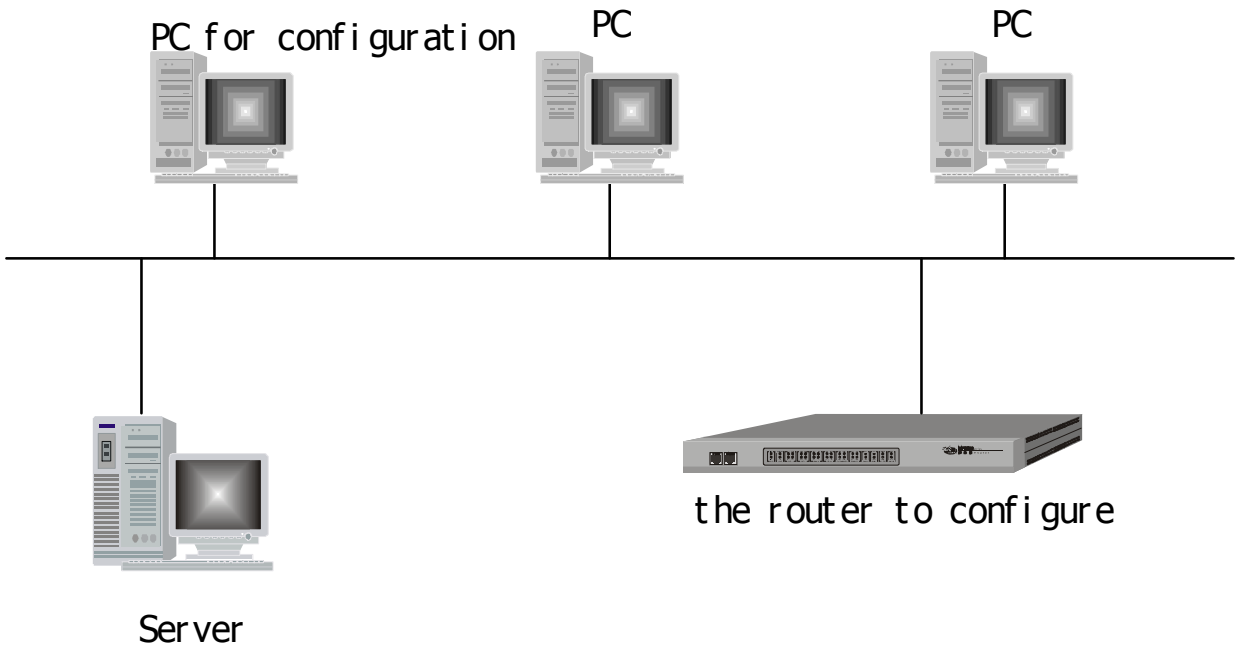
If the 56/336modem module is configured in the router, the DIP dial-up switch of the module is used to configure the port LINE working mode. The following table explains usage of DIP switch:

Choosing mode	Configuring DIP switch		Interpretation
	1	2	
56/336MODEM mode	OFF	OFF	LINE port used as interface of inside 56/336MODEM
Console port mode	ON	OFF	LINE port used as CONSOLE port and router can be configured via remote dial-up login

Configuring Router via Telnet

If the IP address of each interface on the router is configured correctly, then Telnet can be used to log in the router via LAN or WAN, and the router can be configured.

Configuring via LAN:

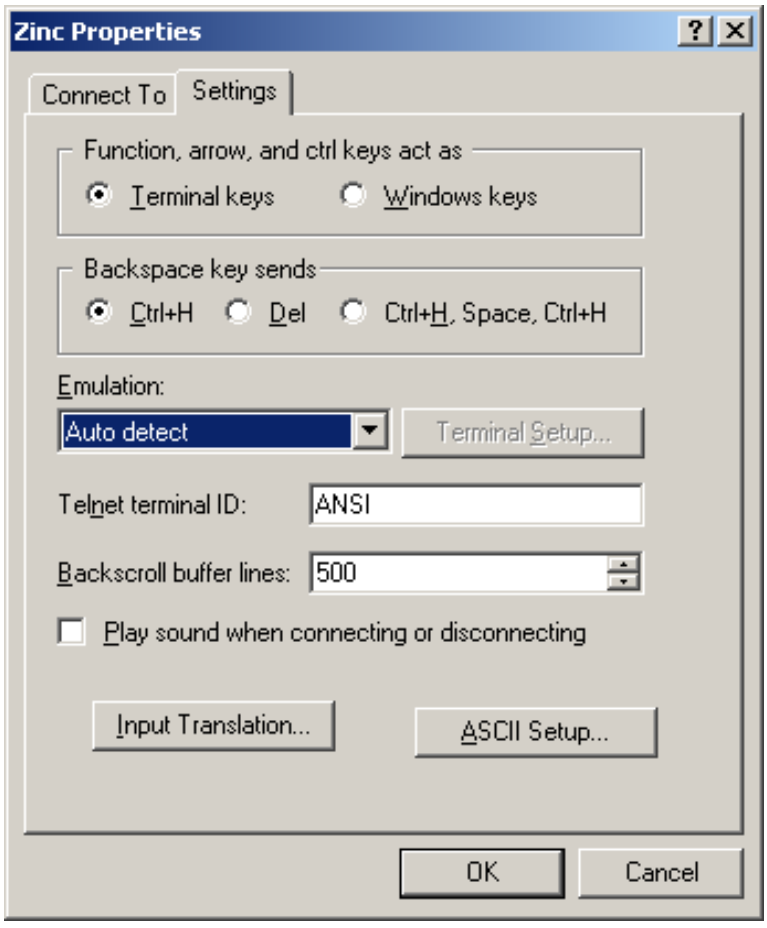


Connect the computer network interface with router Ethernet port on LAN

Run the Telnet client application program on a computer in LAN

Configure default mode (preference) of the Telnet terminal

Contents of the configuration should be set as:
terminal ->default mode -> simulation option select VT100/ANSI.



During configuration of Telnet client program, the option "local response (each display)" should be canceled or it displays contents input by the user adversely effecting the command edit function of shell subsystem.

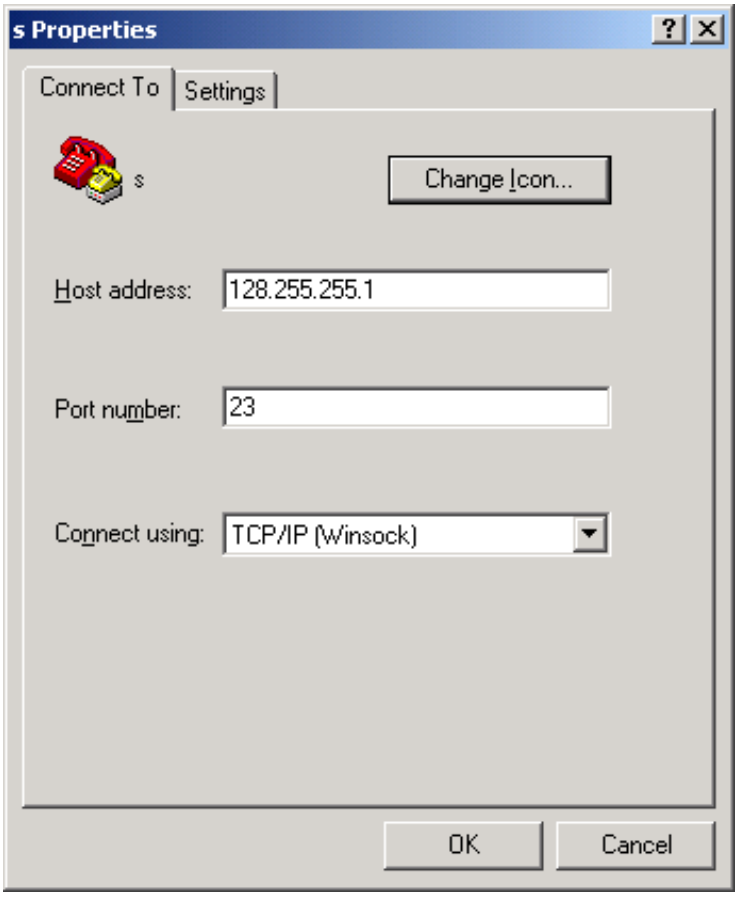
Type in router IP address and establish Telnet connection to the router.

Set Host Name as router IP address: 128.255.255.1

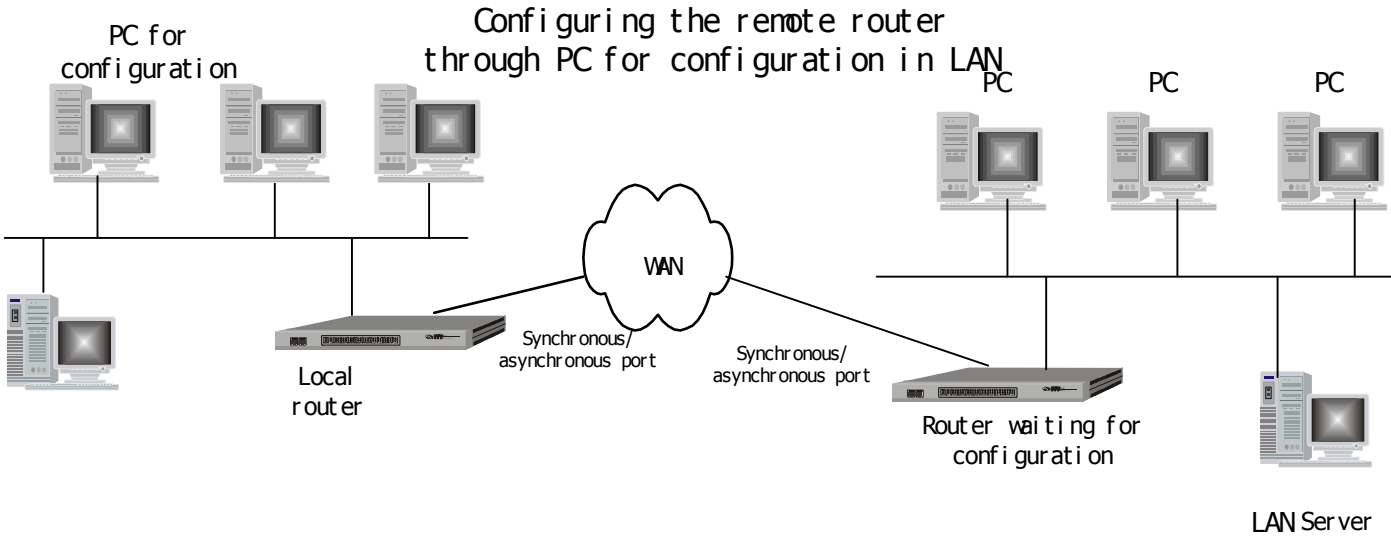
Configure port as Telnet (23)

Configure terminal type as TCP/IP (Winsock)

The other operations are the same as configuration via console interface.

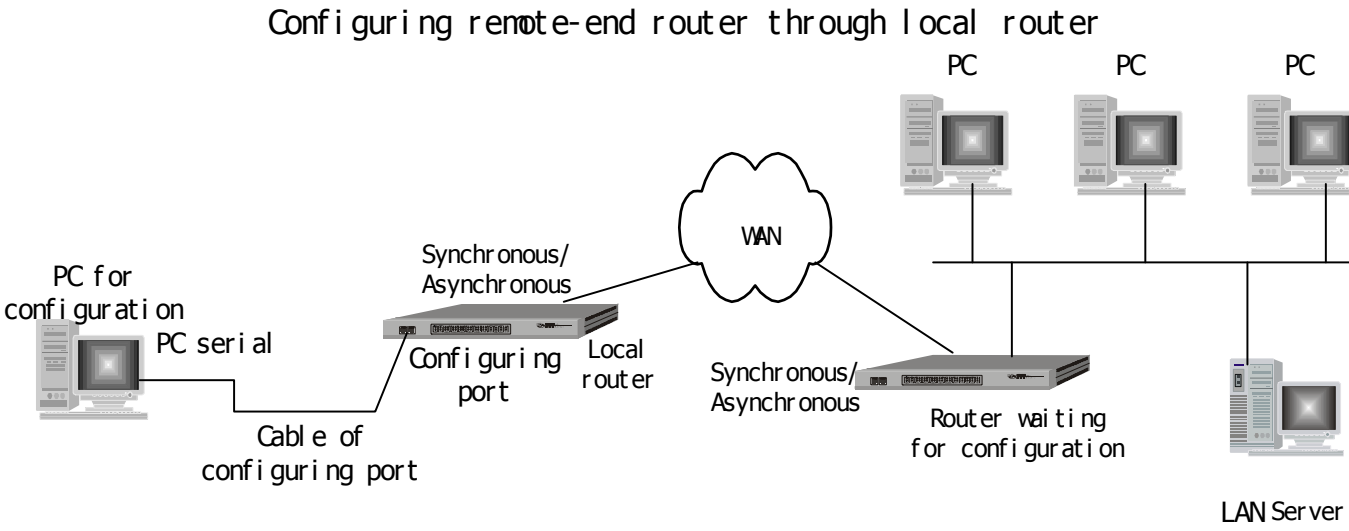


Configuring via WAN:
Connect the configured computer to the remote router via LAN router. Run the telnet client program application on locally configured computer. Other steps are the same as configuration via LAN.



Configuring a remote router via a local router:

Run the Telnet client program on the local router and configure a remote-end router by logging on to network. The method is the same as one of configuring a router via telnet on network. Following is the connection configuration:



When configuring the router via telnet, do not alter IP address of WAN interface. Change the IP address only after ensuring configuration of other parameters.

After the address is changed, telnet disconnects and re-establishes the connection. So the connection should be established again after the new IP address is input to the host.

If users log into a Signamax router from a Linux system, the configuration should be made as follows:
Input the username and password in Linux system.

Run telnet client program in shell environment of Linux system to log in the router using the following command:

telnet 128.255.255.1

After the command is executed, the output is as follows:

Connected to 128.255.255.1 ...done
Display the system prompt of the router:
router>

Press the keys "^" and "]" to return to the prompt of telnet program:

telnet>

Execute the command to cancel the local binary mode:
telnet> unset binary
Already in network ASCII mode with remote host.

router>

After the above operations are completed, command-editing environment in shell system works normally. If users log in to router via another type of telnet client program and the command edit environment works abnormally, configure the Telnet client program according to the above-mentioned specifications.

CLI

CLI is an interactive interface provided by the shell subsystem for users to configure and use a router. Users perform configuration tasks via CLI.

Users examine the system information and see the running system status via the interface.

CLI provides the following functions:

System help information management

Input and editing of system commands

Interface history commands management

Terminal displaying system management

Command Line Help

The Command Line provides the following kinds of online help:

Help

Full help

Partial help

Users get various kinds of help information. In any command mode, type help to obtain simple description about the help system:

router>help

Help may be requested at any point in a command by typing a question mark. If nothing matches, the help list will be empty and you should backup until entering a '?' shows available options.

Two types of help are provided:

Full help is available when you are ready to enter a command argument (example: ‘show?') and explains each possible argument.

Partial help is provided when an abbreviated argument is entered and you want to know which arguments match the input (example: 'show pr?')

In any command mode, type in a question mark “?” to view all possible commands and simple description in this mode. The following table lists commands that can be executed in the privileged user mode.

router#?

Command	Description
bootparams	Print/modify system boot parameters
bridge	Transparent bridge two scc interfaces
Clear	Reset function
Clock	Config the system clock information
Configure	Turn on configuration commands mode
console-speed	Set console speed
Copy	Copy a file to another
Debug	Debugging functions
Disable	Turn off privileged commands
display	Show something for debug purpose
exit	Exit from EXEC mode
filesystem	Turn on file system management commands mode
help	Description of the interactive help system
language	Set help information language
logout	Exit from EXEC shell
memdump	Dump memory image
more	Format showing output
mrt	Mrouted
netstat	Show active connections for Internet protocol socket
no	Negate a command or set its defaults
pad	Open a X.29 PAD connection
phonerxgain	Voip card receive, gain, adjust
phonetxgain	Voip card transmit, gain, adjust
ping	Send echo messages
quickping	Send echo messages
reload	Halt and perform a cold restart
reset	Set something of running system
rlogin	Open a rlogin connection
sendtrap	Send a trap to a specified host or all the host in the trap host list
set	Set something of running system
show	Show running system information
spy	Control collecting task activity data
sysupdate	Update system software
telnet	Open a telnet connection
terminal	Set terminal line parameters
trace	Show a task stack frame
traceroute	Trace route to destination

undebug	Disable debugging functions
wdogDisable	Disable system watchdog
wdogEnable	Enable the system watchdog
who	Show who is logged on
Whoami	Who am i?
write	Write running configuration to a destination
x3	Set X.3 parameters on PAD

Type in a command followed by a ? and separated by a blank. If there is to be a keyword in the place, all keywords and simple description will be listed. The following list shows all keywords following command show in the privileged user mode:

router#show ?

Command	Description
about	Print copyright information
access-lists	List access lists
accounting	Accounting data for active sessions
adsl	ADSL
arp	Print entries in the system ARP table
bridge	Bridge Forwarding/Filtering Database verbose]
card_list	Show information of hardware modules
cbwfq	Show CBWFQ status
clock	Print system clock information
compress	PPP protocol
console	Print console interface information
controllers	Controllers
cpu	Show CPU use per process
cq	Show CQ status
debugging	State of each debugging option
debuglist	Debug register list
device	Print the system devices information
dhcp	Dynamic Host Configuration Protocol status
dialer	Dialer parameters and statistics
dip-switch	Print system DIP switch
dot1Q	Dot1Q
dynamic-command	Show module name of dynamic register
enable	Print enable information
file	Print file system information
filesystem	Print file system information of device

flux	Show flux information
forward	Forward
frame-relay	Frame-Relay protocol
gre	Gre protocol
hosts	Print host tables information
if-list	Print ifnet list
ifx-list	Print ifnet_ext list
interface	Print detailed information of interface
ip	Print Internet protocol status information
keyflow	Keyflow information
language	What language you use
ld	LLC2 device
llc2	Show LLC2 status
logging	Show system logging information
mbuf	Print detailed statistics of mbuf
memory	Print the system memory usage information
modem	Modem
mpdlc	Show MPDLC information
mpls	Mpls
name-server	Print DNS Resolver configuration
ndsp	NDSP information
netDev	Print net device list
netjob	Print netJob information
nia	NIA information
pool	Show all mbuf pool
ppp	Point-to-Point protocol
pq	Show PQ status
process	Active process statistics
queueing	Show queuing configuration
rmon	Remote monitoring
route-map	Show route map information
running-config	Print system running configuration information
scriptList	Print system script list
semaphore	Print the semaphore information
snapshot	Snapshot parameters and statistics
snmp-server	Show static of SNMP Agent
snsp	Stub Network Search Protocol (SNSP)
sntp	Print sntp client information
spd	Show spd status
spy	Show spy switch status
stack	Print the Process stack utilization information

standby	Virtual Backup Router Protocol information
startup-config	Print system startup configuration information
strt-list	Static route hash table
sysadmin	Show tasks cared
sysjob	Print sysJob information
systimertask	Print all tasks scheduled on the systimer list
tacacs	Shows tacacs server statistics
tcp	Status of TCP connections
tech-support	Show system information for Tech-Support
terminal	Show terminal
time-range	Show time range
tunnel-chain	Tunnel chain
ura	User resource authorization information
users	Print the system user login information
version	Print system hardware and software status
vpdn	VPDN information
wfq	Show WFQ status
wred	Show WRED status
x25	X.25 information

Type in a command followed by one question mark "?" separated by a blank. If there is a parameter in this place, the description of parameters will be listed:

router(config)#interface ?

Command	Description
Group	Interface group
Fastethernet	Fast Ethernet network interface
Loopback	Loopback interface
dialer	Dialer interface
tunnel	Tunnel interface
Multilink	Multilink interface
virtual-template	Virtual Template interface
Serial	Serial network interface

Type in a character string closely followed by one question mark "?" and all keywords which begin with the same character string and description will be listed.

router#d?

Command	Description
display	Show something for debug purpose
disable	Turn off privileged commands
debug	Debugging functions

Type in a command followed by a character string closely with one question mark "?" and all keywords which begin with the character string and their description will be listed.

router#show h?

Command	Description
Hosts	Print host table information

Command Line Error Message

When users key in commands, the syntax is examined. If the syntax is correct, then commands execute or error messages will be reported to users. Following are the common error messages:

Error prompt messages of command line:

Error message	Reason
% Invalid input detected at '^' marker. Unknown	Cannot find the command
	Cannot find keywords
	Parameter type of is wrong
	The parameter value is beyond the range
Type "*** ?" for a list of subcommands	The input command is not integrated

The string *** represents uncompleted command-string the user input.

History Command

CLI provides the function similar to DosKey and the system will automatically save commands input by the user into the history command buffer.

Users transfer history commands saved by CLI at any time and execute them repeatedly to reduce users' unnecessary repetition of input commands. CLI stores up to 10 commands for each user connecting to a router. The most recent commands take priority over the oldest command.

Accessing history commands:

Operation	Key pressed	Function
Accessing last history command	Up-cursor key or Ctrl+p	If there are some earlier history commands, then they are taken out
Accessing next history command	Down-cursor key or Ctrl+n	If there are some later history commands, then they are taken out; or else, the system clears command line and alarms.

When the cursor key is used to access history commands and telnet runs in Windows98/NT system to log in the router, the option "terminal->premier option->simulation option" should be configured as type VT-100/ANSI.

Editing

CLI provides basic command editing functions supporting multi-line editing with a maximum of 256 characters for each command line. The following table lists basic editing functions provided by the subsystem shell.

Key	Function
Common key	If the edit buffer is not full, then the key is inserted at the location of the cursor and the cursor shifts right or the system gives alarm bell
Backspace key	Deletes the character before cursor location. If the cursor has arrived at the beginning of the command, the system gives alarm bell
Delete key	Deletes the character on the cursor location. If the cursor has arrived at the end of the command, the system gives alarm bell
Left cursor key ←, ^B	Left shifts the cursor one character location. If the cursor has arrived at the beginning of the command, the system gives alarm bell
Right cursor key →, ^F	Right shifts the cursor one character location. If the cursor has arrived at the end of the command, the system gives alarm bell
Up or down cursor key ↑ ↓	Displays history commands
^A	Shifts cursor to the beginning of command line
^E	Shifts cursor to the end of the command line
^U	Deletes all characters on the left of the cursor until the cursor arrives at the beginning of the command line
^K	Deletes all characters on right of cursor until cursor arrives at the end of command line

Display

CLI provides the following display features:

When information needed cannot be displayed on one screen, the system offers the pause function and displays a prompt "(--MORE--)" at the bottom left corner of screen. Following are some choices for users:

Type in Space key or key '↑' or Ctrl-F to continue displaying next screen of messages.

Enter '↓' key or Ctrl-B to display previous screen of messages.

Type ENTER or key '+' or '→' to scroll down one line of the displayed message on screen.

Type in the key '-' or '←' to scroll up one line of the displayed message on screen.

Typing in any other keystroke, the system displays system prompt directly.

Key	Function
Key '↓'or Ctrl-B	Displays information of previous screen
Space key (Space) or key '↑' or Ctrl-F	Goes on displaying information of next scr een
Key '-'or '←'	Information displayed on screen rolls dow n one row
Carriage return key (Enter) or key '+'or'→'	Goes on displaying information of next row
Other keys	Exits from display

System Configuration Management

This chapter explains basic configuration and management of Signamax routers including system configuration commands, user and password management, configuration of environment parameters, file management and examination of system information.

System Configuration

Following are the main tasks of system configuration in Signamax routers:

Configuring system name

Configuring system clock

Configuring system users

System configuration commands:

Configuration task	Command	Command function	Running mode	Example
Configuring name	hostname	Changing router name	Configuration mode	router(config)#hostname router
Configuring calendar	clock	Configuring the system calendar	Privileged user mode	router#clock 2001 11 15 9 25 10
Configuring system users	user	Adding system users	Configuration mode	router(config)#user Signamaxxf password 0 Signamax 1

Configuring System Name

When the router leaves the factory, its default system name is router. Users change the system name according to their needs. This change takes effect immediately; the new system name will appear in the next system prompt. The following example will change the system name from "router" to "router_1":

Following are the operating steps:

Command	Task
router#configure terminal	Executes the command #configure terminal in Privileged user mode to enter global configuration mode
router(config)#hostname router_1	Executes the command hostname with the parameter "router_1" in global configuration mode to change the system name
router_1(config)#	The new system command begins to come into effect of the system prompt

Configuring System Calendar

There is an independent clock system installed in each Signamax router to record the system time which comprises information comprises year, month, date, hour, minute, second and week.

When the system starts, the system time rests at 00:00:00 January 1,1970. Via the execution of the command clock, the router calendar system can be set to the time as shown in the following example:

```
router#clock 2001 11 15 9 36 10
The function of the executed command in the privileged user mode is
to set the time of the system calendar as 09:36:10, November 15,
2001.

router#show clock
Displays  time of the system.

UTC:THU NOV 15 09:36:15 2001
The  time is 09:36, November 15, 2001,default timezone is UTC.
```

The command show clock can be executed either in the common user mode or in the privileged user mode. The function is the same in both modes.

Because there is no real time system (i.e. the system clock is still running after it is powered off). The system clock returns to 00:00:00 January 1,1970 each time the router is turned on.

Configuring System Logon Security Service

To enhance system security, Signamax router provides system logon security service function. The main function comprises:

Prevent violence breaking off user password

Prevent high-speed connection

The prevent violence breaking off user password function is to prevent the violence for the user name and password of Signamax routers from invalid users.

The prevent high-speed connection function stops invalid users initiating a large number of logon demands to routers, which will occupy a lot of system and network resource. When the connection times reach the enactment times, the system will forbid the logon connection demand from this IP.

Following are the commands:

Command	Description	Configuration mode
service login-secure	Enable system security service	config
login-secure check-record-interval *<30m-14400m>*	Configure login secure check record time interval. The default time is 60 minutes.	config
login-secure forbid-time *<10m-144000m>*	Configure login secure forbidden time. The default is 10 minutes.	config
login-secure max-try-time *<1-20>*	Configure login secure max tried times. The default is 5 times.	config
login-secure record-aging-time *<15m-1440m>*	Configure login secure record aging time. The default is 15 minutes.	config
login-secure quick-connect max-times *<10-10000>*	Configure login secure quick connecting max times. The default is 20 times.	config
login-secure quick-connect restrict-interval *<10s-600s>*	Configure login secure quick connecting restrict time interval. The default is 30 seconds.	config
login-secure quick-connect unrestrict-interval <10m-1440m>	Configure login secure quick connecting unrestricted time interval. Default is 20 seconds.	config
show login-secure information	Examine login secure information	enable
show login-secure quick-connect	Examine login secure quick connecting record	enable

(Default status) enable login secure service when the system is enabling by default.

Execute command no service login-secure and disable login secure service. Delete all login connection records.

System Management

Storage Medium & File Types

The Signamax router has three kinds of storage media. Following are the functions:

DRAM - operating space for router application programs

FLASH - stores router application programs, configuration files and BootROM programs

EEPROM - stores user information and variable system configuration files.

There are four types of the files managed by the Signamax router:

Router application program files - used for route forwarding, files management and system management

Configuration files - stores system parameters configured by users

BootROM files - stores system initialized data

Other files - for example, the dial tone memory file of second dial-up

File System Management

Each Signamax router constructs a file system based on DOS in the system flash to store information that rarely needs to be changed such as a router application program (protocol software, device program, drivers) and BootROM program.

The file system is called True Flash File System (TFFS). In the file system configuration mode, the system provides a set of commands to manage the file system.

The file system management command list:

Command	Function	Running mode	Example
Copy	Copies file	File system configuration mode	Router(config-fs)#copy flash:file1 flash:file2
Delete	Deletes file	File system configuration mode	Router(config-fs)#delete file1
Type	Displays file contents	File system configuration mode	Router(config-fs)#type startup
Dir	Displays directory or file	File system configuration mode	Router(config-fs)#dir
cd	Changing path	File system configuration mode	Router(config-fs)#cd dir1
Pwd	Displays path	File system configuration mode	Router(config-fs)#pwd
Mkdir	Creates directory	File system configuration mode	Router(config-fs)#mkdir dir1
Rmdir	Deletes existing directory	File system configuration mode	Router(config-fs)#rmdir dir1
Volume	Displays file device information	File system configuration mode	Router(config-fs)#volume
Show	Displays file device information	Privileged user mode	Router#show filesytem

The router file system management is composed of two parts - file management and directory management. As TFFS is based on DOS file system, long file names are not supported. Each directory name can be a maximum of eight characters in length. Each file name follows the 8.3-naming standard.

Display file device information:

The file system of Signamax router is based on the physical device flash. Use the following commands to display TFFS information. Execute the command volume in the file system configuration mode.

```
router(config-fs)#volume
device name:/flash
Total number of sectors 5687
There are 5687 sectors all together in the file system.
bytes per sector: 512
Each sector has 512 bytes;
media byte: 0xf8
Type of medium: 0xf8;
# of sectors per cluster: 4   Each cluster has 4 sectors;
# of reserved sectors: 1  One reserved sector;
# of FAT tables: 2  Two FAT tables;
# of sectors per FAT: 5  Each FAT table occupies 5 sectors.
max # of root dir entries:  240  The root directory can contain at most
240 files or directories;
# of hidden sectors: 1 – One hidden sector; removable medium: false
(This device can't be removable; disk change w/out warning: ot enabled.
The file system doesn't warn about modification;
auto-sync mode: not enabled – Auto synchronization of the auto file
system isn't supported;
long file names: not enabled – Long file name isn't supported;
exportable file system: not enabled – The file system can't be replaced;
lowercase-only filenames: not enabled – File name does not differentiate
the uppercase or the lowercase.
volume mode:    O_RDWR (read/write)   The file system is read and
written; available space: 2893824 bytes. The useable space of the system
is 2893824 bytes;
Max avail. config space: 2893824 bytes  The maximum useable space of the
system is 2893824 bytes.
```

Execute the command show file in the privileged user mode. The meaning is the same as volume.

File Management

The file management commands in the file system configuration mode, allow users to operate all files in TFFS including:

List files (directories)

Copying a file

Deleting a file

Displaying a file

The following are examples of using file management commands:

1. Listing files (directories)

```
router#filesystem
router(config-fs)#dir

size          date             time         name
-----         -----            -----        ----
4         JAN-01-1980      00:00:00     RANDOM
1713        JAN-01-1980       00:00:00      STARTUP
512       JAN-01-1980      00:00:00     SignamaxXF       <DIR>
```

After executing the command filesystem to enter the file system configuration mode, execute command dir in this mode and all files and subdirectories list out in the directory.

2. Copying files

```
router(config-fs)#copy startup-config flash/Signamaxxf/newstart
```

Copies the file startup, renames it as newstart and puts it into the directory Signamaxxf.

```
router(config-fs)#dir
size             date             time         name
------           -----            -----        -----
4                  JAN-01-1980        00:00:00     RANDOM
1713        JAN-01-1980         00:00:00     STARTUP
512         JAN-01-1980         00:00:00     SignamaxXF      <DIR>

router(config-fs)#cd Signamaxxf
router(config-fs)#dir
```

```
size        date           time          name
-----       -----          ------        -----
512           JAN-01-1980    00:00:00       .           <DIR>
512           JAN-01-1980    00:00:00       ..          <DIR>
1713        JAN-01-1980    00:00:00      NEWSTART
```

3. Deleting files

```
router(config-fs)#delete startup
Deletes the file startup.

The Data of this file will be lost! if OS is deleted, the system will
hangup!
Please confirm to continue(Yes/No)y. After Y(Yes) is confirmed, the file
will be deleted, or N(No) represents that the operation will be canceled.

router(config-fs)#dir

size          date                    time         name
-----         ------                ------       ------
4               JAN-01-1980          00:00:00      RANDOM
512           JAN-01-1980           00:00:00      SignamaxXF    <DIR>
```

4. Displaying contents of files

```
router(confgi-fs)#type startup
Displays content of the file startup.
The content of file startup

interface fastethernet0
exit
interface serial0
physical-layer sync
encapsulation PPP
exit
```

Command Usage

Examine file equipment information - Router file system is based on flash physical equipment, and the basic information of FLASH (TFFS) can be gained via following commands.

volume - execute in file system configuration mode

show filesystem - execute in privileged user mode

Application example:

```
in file system configuration mode, execute command volume:
router(config-fs)#volume
volume descriptor ptr (pVolDesc):        0x2cfa968
```

```
cache block I/O descriptor ptr (cbio):    0x2cfaa40
auto disk check on mount:                 NOT ENABLED
max # of open files:      22
file descriptors in use:                  0
# of different files in use:              0
# of descriptors for deleted files:       0
# of  obsolete descriptors:               0

 volume configuration:
- volume label:         NO LABEL ; (in boot sector: )
- volume Id:            0x0
- total number of sectors:     5,213    /*file system sector number */
- bytes per sector:            512      /* bytes per sector */
- # of sectors per cluster:    4        /* sectors per cluster */
- # of reserved sectors:       1        /* reserved sectors */
 - FAT entry size:             FAT12    /* FAT entry size */
 - # of sectors per FAT copy:   4              /* sectors per FAT copy
*/
 - # of FAT table copies:       2              /* FAT table copies */
 - # of hidden sectors:         1              /* hidden sectors */
 - first cluster is in sector # 24      /* first cluster is in sector */
 - Update last access date for open-read-close = FALSE
 - directory structure:         VFAT    /* directory structure */
 - root dir start sector:        9      /* root directory start sector
*/
- # of sectors per root:        15      /* sectors per root */
- max # of entries in root:    240      /* max entries in root */
```

```
FAT handler information:
------------------------
- allocation group size: 1 clusters          /* allocation group size */
- free space on volume:  2,641,920 bytes  /* free space on volume */
router(config-fs)#
```

File management:
The user operates all files for TFFS using file management commands in file system configuration mode including:

list file (directory)

file copy

file delete

examine file content

Example of file management command:

```
List file (directory)
dir
```

Application example:

```
router(config-fs)#dir
size        date            time        name
-----       -----           -----       -----
1930        JAN-01-1980     00:00:00    LOGGING
4           JAN-01-1980     00:00:00    RANDOM
3160        JAN-01-1980     00:00:00    STARTUP
3160        JAN-01-1980     00:00:00    SCRIPT
```

file copy

File copy command is in FLASH file system, FTP server, TFTP server, starting configuration and operation configuration. Following is the command format.

```
copy  { ( ftp dest-ipaddress ftp-username ftp-password source-filename )
|

(tftp dest-ipaddress source-filename ) | ( flash source-filename ) |
running-config | startup-config }
{ ( ftp dest-ipaddress ftp-username ftp-password dest-filename ) |
( tftp dest-ipaddress dest-filename ) | ( flash dest-filename ) |
```

running-config | startup-config }

ftpcopy dest-ipaddress ftp-username ftp-password source-directory source-filename

dest-filename

tftpcopy dest-ipaddress source-filename dest-filename

xmodemcopy source-filename trans-baudrate

Description of every copy:

copy file from FLASH file system to FLASH file system

```
copy flash source-filename flash dest-filename

router(config-fs)#dir

size        date         time        name
-----       -----        -----       ----
2048        JAN-01-1980   00:00:30    mpssh     <DIR>
4           JAN-01-1980   00:00:24    random

router(config-fs)#copy flash random flash abc
Copying...  Completed
router(config-fs)#dir

size        date          time        name
-----       -----         -----       -----
2048        JAN-01-1980   00:00:30    mpssh     <DIR>
4           JAN-01-1980   00:00:24    random
4           JAN-01-1980   00:10:16    abc
```

copy file from FLASH to ftp server

```
copy flash source-filename ftp dest-ipaddress ftp-username ftp-password
dest-filename
```

Application example:

```
router(config-fs)#dir
size        date          time        name
------      -----         ----        -----
2048        JAN-01-1980   00:00:30    mpssh      <DIR>
4           JAN-01-1980   00:00:24    random
510         JAN-01-1980   00:08:26    startup
11577       JAN-01-1980   00:09:10    abc

router(config-fs)#copy flash abc ftp 128.255.42.180 123 123 test
Copying!!!!!!!!!!!!Total 11577 bytes copying completed.
router(config-fs)#
```

copy file from FLASH to tftp server

```
copy flash source-filename tftp dest-ipaddress dest-filename
```

Application example:

```
router(config-fs)#dir
size            date           time         name
--------        ------         ------       -----
2048            JAN-01-1980    00:00:30     mpssh    <DIR>
4               JAN-01-1980    00:00:26     random
510             JAN-01-1980    00:08:26     startup
11577           JAN-01-1980    00:09:10     abc

router(config-fs)#copy flash abc tftp 128.255.42.180 test
Completed!
router(config-fs)#
```

copy the file in FLASH to startup configuration

```
copy flash source-filename startup-config

application example:
router(config-fs)#dir
size        date          time       name
-----       -----         -----      -----
2048       JAN-01-1980    00:00:30   mpssh   <DIR>
4          JAN-01-1980    00:00:26   random
510        JAN-01-1980    00:05:16   abc

router(config-fs)#copy flash abc startup-config
Copying...  Completed
router(config-fs)#dir
size        date          time       name
-----       ----          ------     ------
2048       JAN-01-1980    00:00:30   mpssh    <DIR>
4          JAN-01-1980    00:00:26   random
510        JAN-01-1980    00:05:46   startup
510        JAN-01-1980  00:05:16   abc
router(config-fs)#
```

copy startup configuration to the file in FLASH

```
copy startup-config flash dest-filename
```

Application example:

```
router(config-fs)#copy startup-config flash abc
Copying...  Completed
router(config-fs)#dir
size       date          time        name
-----      ------        ------      -----
2048       JAN-01-1980   00:00:30    mpssh       <DIR>
4          JAN-01-1980   00:00:26    random
510        JAN-01-1980   00:09:40    startup
510        JAN-01-1980   00:17:08    abc
router(config-fs)#
```

copy startup configuration to host via FTP

```
copy startup-config ftp dest-ipaddress ftp-username ftp-password dest-
filename
```

Application example:

```
router(config-fs)#copy startup-config ftp 128.255.42.180 123 123 test
Copying!Total 510 bytes copying completed.
```

Copy startup configuration to host via TFTP

```
copy startup-config tftp dest-ipaddress dest-filename
```

Application example:

```
router(config-fs)#copy startup-config tftp 128.255.42.180 test
Completed!
```

Copy running configuration to the file in FLASH

```
copy running-config flash dest-filename
```

Application example:

```
router(config-fs)#dir
size         date          time        name
-----        -----         -----       -----
2048        JAN-01-1980    00:00:30    mpssh    <DIR>
4           JAN-01-1980    00:00:26    random

router(config-fs)#copy running-config flash abc
Copying...  Completed
router(config-fs)#dir
size        date          time        name
------      ------        -----       ------
2048        JAN-01-1980   00:00:30    mpssh    <DIR>
4           JAN-01-1980   00:00:26    random
510         JAN-01-1980   00:17:08    abc

router(config-fs)#
```

Copy running configuration to host via FTP

```
copy running-config ftp dest-ipaddress ftp-username ftp-password dest-filename
```

Application example:

```
router(config-fs)#copy running-config ftp 128.255.42.180 123 123 test
Copying!Total 510 bytes copying completed.
```

Copy running configuration to host via TFTP

```
copy running-config tftp dest-ipaddress dest-filename
```

Application example:

```
router(config-fs)#copy running-config tftp 128.255.42.180 test
Completed!
```

Copy running configuration to startup configuration

```
copy running-config startup-config
```

Application example:

```
router(config-fs)#dir
size        date       time       name
-----       -----     ------    --------
2048       JAN-01-1980  00:00:30   mpssh     <DIR>
4          JAN-01-1980  00:00:26   random

router(config-fs)#copy running-config startup-config
Building Configuration...done
router(config-fs)#dir

size       date          time        name
-----      -----         ----        ------
2048       JAN-01-1980   00:00:30    mpssh    <DIR>
4          JAN-01-1980   00:00:26    random
495        JAN-01-1980   00:33:28    startup

router(config-fs)#
```

Copy file to FLASH from ftp server

```
copy ftp dest-ipaddress ftp-username ftp-password source-filename flash
dest-filename same as ftpcopy command
```

Application command:

```
router(config-fs)#dir

size        date           time        name
-----       -----          -----       -----
2048        JAN-01-1980    00:00:30    mpssh     <DIR>
4           JAN-01-1980    00:00:24    random

router(config-fs)#copy ftp 128.255.42.180 123 123 test.bin flash abc
Downloading##########################OK!

router(config-fs)#dir

size        date             time          name
-----       -----            ------        -----
2048        JAN-01-1980      00:00:30      mpssh       <DIR>
4           JAN-01-1980      00:00:24      random
11577       JAN-01-1980      00:09:10      abc
router(config-fs)#
```

Copy file to startup configuration from FTP server

```
copy ftp dest-ipaddress ftp-username ftp-password source-filename
startup-config
```

Application example:

```
router(config-fs)#dir

size        date           time        name
-----       -----          -----       -----
2048        JAN-01-1980   00:00:30     mpssh       <DIR>
4           JAN-01-1980   00:00:26     random
router(config-fs)#copy ftp 128.255.42.180 123 123 test startup-config
Downloading##OK!
router(config-fs)#dir

size        date             time         name
------      ------           -----        -----
2048        JAN-01-1980      00:00:30     mpssh       <DIR>
4           JAN-01-1980      00:00:26     random
495         JAN-01-1980      00:58:02     startup

router(config-fs)#
```

Copy file to FLASH file system from TFTP server

```
copy tftp dest-ipaddress source-filename flash dest-filename
same as tftpcopy command
```

Application example:

```
router(config-fs)#dir
size        date          time        name
-----       -----         -----       ------
2048        JAN-01-1980   00:00:30    mpssh       <DIR>
4           JAN-01-1980   00:00:26    random

router(config-fs)#copy tftp 128.255.42.180 test flash abc
Downloading##OK!

router(config-fs)#dir
size        date          time        name
------      -----         ------      -----
2048        JAN-01-1980   00:00:30    mpssh      <DIR>
4           JAN-01-1980   00:00:26    random
495         JAN-01-1980   01:01:00    abc

router(config-fs)#
```

Copy file to startup configuration from TFTP server

```
copy tftp dest-ipaddress source-filename startup-config
```

Application example:

```
router(config-fs)#dir

size        date            time         name
-----       ------          ----         -----
2048        JAN-01-1980     00:00:30     mpssh      <DIR>
4           JAN-01-1980     00:00:26     random

router(config-fs)#copy tftp 128.255.42.180 test startup-config
Downloading##OK!

router(config-fs)#dir
size         date             time         name
-----        ------           ------       ------
2048        JAN-01-1980       00:00:30     mpssh     <DIR>
4           JAN-01-1980       00:00:26     random
495         JAN-01-1980       01:03:28     startup

router(config-fs)#
```

Copy file to FLASH file system via console port by using xmodem **protocol**

```
xmodemcopy dest-filename trans-baudrate
```

Application example:

```
router(config-fs)#dir
size         date           time         name
-----        -----          -----        -----
2048        JAN-01-1980     00:00:30     mpssh      <DIR>
4           JAN-01-1980     00:00:26     random

router(config-fs)#xmodemcopy abc 9600
```

Now ready to receive file. Please send file with XMODEM protocol. If you want to cancel in progress, press CTL+C key...

```
Receive file successfully!!

router(config-fs)#dir
size         date           time         name
-----        -----          -----        ------
2048        JAN-01-1980     00:00:30     mpssh      <DIR>
4           JAN-01-1980     00:00:26     random
```

```
512         JAN-01-1980    01:30:32     abc
router(config-fs)#
```

delete file

```
delete filename
```

Application example:

```
router(config-fs)#dir
size         date           time         name
-----        -----          -----        ----
2048         JAN-01-1980    00:00:30     mpssh        <DIR>
4            JAN-01-1980    00:00:26     random
512          JAN-01-1980    01:30:32     abc

router(config-fs)#delete abc
WARNING:
The Data of this file will be lost! if OS is deleted,the system will
hangup!

Please confirm to continue?(Yes/No)y
router(config-fs)#dir
size         date           time         name
-----        -----          -----        ------
2048         JAN-01-1980    00:00:30     mpssh       <DIR>
4            JAN-01-1980    00:00:26     random
router(config-fs)#
```

Examine file content

```
type filename

router(confgi-fs)#type startup - examine file startup content
The contexts of file startup
hostname router
user signamax password 0 signamax 1
enable password OW encrypt
enable timeout 0
no service password-encrypt
interface loopback0
exit
interface fastethernet0
ip address 129.255.222.26 255.255.0.0
no ip redirects
exit
interface serial1/0
physical-layer sync
clock rate 64000
tx-on dsr
encapsulation ppp
ip address 10.1.1.1 255.0.0.0
exit
```

Directory management

In routers, file system directory management content comprises:

Print working directory

Change working directory

Create directory

Remove directory

The following examples are for directory management commands:

Print working directory:

pwd

Application example:

```
router(config-fs)#pwd
/flash
router(config-fs)#
above displaying means the system is in the directory of /flash.
```

Create directory

```
mkdir dir-name
```

Application example:

```
router(config-fs)#mkdir signamax
router(config-fs)#dir
size          date           time       name
--------      -----          -----      ------
1930       JAN-01-1980      00:00:00    LOGGING
4          JAN-01-1980      00:00:00    RANDOM
3160       JAN-01-1980      00:00:00    STARTUP
512        JAN-01-1980      00:00:00    SIGNAMAX        <DIR>
3160       JAN-01-1980      00:00:00    SCRIPT
```

Change working directory:

```
cd dest-dirname
```

Application example:

```
router(config-fs)#cd signamax
router(config-fs)#pwd
/flash/signamax
```

Displaying means the system is in the directory of /flash/signamax.

Remove the directory

```
rmdir dir-name
```

Application example:

```
router(config-fs)#cd /flash
router(config-fs)#rmdir signamax

WARNING:
The Data of this dir will be lost! if OS is deleted,the system will
hangup!

Please confirm to continue?(Yes/No)y
router(config-fs)#dir
size          date            time       name
-----         -----           -----      -----
1930        JAN-01-1980     00:00:00    LOGGING
4           JAN-01-1980     00:00:00    RANDOM
3160        JAN-01-1980     00:00:00    STARTUP
3160        JAN-01-1980     00:00:00    SCRIPT
```

Router Configuration File Management

File Contents & Formats

The configuration file exists in the file system in the form of text. Following is the format:

Existing in the format of configuring commands.

To save the memory space of device flash, only those commands in the configuration modes (including global configuration mode, interface configuration mode, access list configuration mode and routing protocol configuration mode) are saved.

The organization of commands of command mode is standard. All commands in the same mode are organized together to form a paragraph.

Paragraphs are arranged in a certain order. The global configuration mode, interface configuration mode and routing configuration mode.

Sort commands according to the relation among them. All related commands are grouped together and a blank line is used to separate groups.

Example of Signamax router configuration file:

```
router#sh run
Building Configuration...done

 configuration:
version 4.2.7(YD)-2(integrity)
hostname router
enable password [WOWWWNXSX encrypt
enable timeout 0
no service password-encrypt
no service enhanced-secure
line 0 15 mode terminal
interface loopback0
exit

interface fastethernet0
ip address 192.168.0.83 255.255.255.0
exit

interface ethernet0
exit
```

```
interface serial3
Physical-layer sync
encapsulation ppp
ip address 1.1.1.2 255.255.255.0
exit

line 0 15 flowctl soft
terminal 0 15 local 192.168.0.83
terminal 0 15 remote 0 zfy 192.168.0.80 fix-terminal
terminal 0 15 enable
```

Loading Configuration File

The configuration file of Signamax routers can be edited in a text editor (for example, WordPad) according to the format prescribed in the above section. It can be downloaded to router via FTP or TFTP. This operation can be used by terminal users or via Telnet.

The following example is given to explain how to download the router configuration file via FTP:

Edit the configuration file named config on a computer.

Start FTP SERVER on the computer.

Execute ftpcopy command in the file configuration mode of the router to download from the computer.

It can be shown as:

```
router(config-fs)#ftpcopy  A.B.C.D    router  router1  j:\  config
startup
Computer's IP address user name password directory file name local file
name
```

The aim of the above command is to download the configuration file config from the root directory of disk J of the computer whose address is A.B.C.D to a router, and write it into directory of the router TFFS with the name startup.

Executing the command dir, you can see that a new file startup has been added into the directory.

```
router(config-fs)#dir
size          date                time        name
----          -----             ------      -----
512             JAN-01-1980       00:00:00    MPROUTER      <DIR>
580             JAN-01-1980       00:00:00    STARTUP
630             JAN-02-1980       00:00:00    CONFIG
```

Downloading configuration files via TFTP is very similar to downloading via FTP. The only difference between them is that the computer needs to run TFTP SERVER.

Restart the router and execute the configuration file startup, and modify system configurations.

Saving System Configuration

After validating that the modified system configurations are error free, users can save the configurations to be treated as configuration parameters for the next startup.

The following command can be executed to save the running configuration into the startup configuration file (STARTUP):

```
router#copy running-config startup-config
router#write startup-config
```

Or use another command

The following command can be executed to save the running configuration into remote host via TFTP:

```
router#copy running-config tftp A.B.C.D WORD
```

Address of the remote host:

The following command can be executed to save the startup configuration file into the remote host via TFTP:

```
router#copy startup-config tftp A.B.C.D WORD
```

The following command can be executed to save the configuration files of the remote host into the startup configuration file (STARTUP) of the router via TFTP:

```
router#copy tftp A.B.C.D WORD startup-config
```

Displaying Configuration of Running Routers

```
router#show running-config
```

System Authentication & Command Hierarchical-Authorization Command

Signamax routers enhance security by providing authentication management systems including AAA, when users log on or enter privilege mode by operating "enable" command and only those who have rights can log on or operate successfully.

Different levels of users have different levels of authorized executable command set. Command authority ranges from level 0 to level 15, in which level 0 represents the lowest authority while level 15 represents the highest.

enable

All user authority levels (from 0 to 15) can be accessible by operating "enable" command. For example, if you have some level of authority (means you have right user name and password), you will successfully pass the "enable" authentication and get right user authority level.

```
Router> or router#
```

Command	Task
enable *0~15* | *CR*	"0~15" means user authority level. If nothing is given behind "enable", default is level 15. If present user authority level is higher, it is without any authentication when entering lower level. Or, possible authentication decided by present configuration is needed when entering higher one.

Given password is set by "enable password level" command, authentication without AAA or with AAA by means of "enable" authentication in the "enable" method list will be realized by this password.

If no "enable password level" command is operated, however authentication will be realized by means of "enable" authentication in the "enable" method list, there are two possible situations as follows:

a. If users log on by TELNET, authentication will fail to pass with "% No password set" prompt without AAA configuration or with "% Error in authentication" prompt with AAA.

b. If users log on by CONSOLE, authentication with AAA configuration will first try the password set in "enable password level" command and then pass with default by means of "none" if finding no "enable password level" command is operated. While authentication without AAA configuration will fail to pass with "% No password set" prompt.

Passing "enable" authentication - present user will get right user authentication level, which can be showed by "show privilege" command.

If it is configured by "aaa authentication enable default method" command, the following authentication methods can be used to meet users' needs.

a. If it is configured by "aaa authentication enable default none" command authentication will be realized without any password.

b. If it is configured by "aaa authentication enable default line" command, authentication will be realized with password set in "line" command, or it will fail to pass with "% Error in authentication" prompt.

c. If it is configured by "aaa authentication enable default radius" command, lease note authentication user name (that is "$enab+level$", in which level is represented authentication level by the number from 1 to 15 meaning) needed by the command is invariable. Given user name denoted in fixed rules by means of radius, only password (no user name anymore) is necessary in the process of authentication. If a user is already set its password in radius server, authentication will be realized successfully by the password or unsuccessfully. For example, given "enable 10" command has been done, the fixed user name is "$enab10$" which has already existed in radius server, and authentication will be passed successfully only by its password.

d. If it is configured by "aaa authentication enable default tacacs" command, user name and password is necessary. If user name and password are already in tacacs server and "enable" authentication of tacacs has been set beforehand (tacacs server has to set right password of "enable" authentication to users), authentication will be realized successfully or unsuccessfully.

privilege

Every command has its default level. The "privilege" command can modify its default level.

Present user can only modify commands with equal or lower level than itself. For example, user with level 12 can modify commands with level from 0 to 12.

Router(config)#

Command	Task
privilege *MODE* level *0～15* all | command *LINE*	Set privilege level of command

MODE represents working mode of commands to be set and can be all system's modes.

Parameter 0～15 represents a level set to commands.

If key word "all" is used in the command, all commands in present mode will be set to a given level.

If key word "command" is used in the command, "command" can be input by the first several key parts so that all sub-commands with the same key parts will be set to the same level. For example, if running "privilege CONF level 2 command interface" command, all sub-commands starting with interface will be set to level 2in present IOS version including sub-commands group and interface. If running "privilege CONF level 2 command interface group" command, only sub-commands starting with interface group will be set to level 2 while sub-command interface won't be set.

If there is no command in the given MODE matching input character string, configuration is not set successfully with "%Invalid command string "xxx" " prompts.

Input command character string follows the rule of "match most", which means string that you input can be only found among all commands. While in the footprint, the string will be completed to match the whole command.

"no" command will set authority levels of right command set back to their default levels, in which:

a. "no privilege *MODE CR*" command will set all commands in *MODE* back to their default levels.

b. "no privilege *MODE* level *level CR*" command will set the command configured to *level* in *MODE* back to its default level.

c. rules

After configuring the command, command level will take effect at once, which can be testified in the following 2 aspects.

Whether present user has the given authority level or not is decided by this configuration when user runs commands.

Whether present user has authority level of a footprint configuration command or not is decided by this configuration when running "show run" or "show startup" command.

Enable Password

Set local enabled password for entering router with any user level.

router(config)#

Command	Task
enable password level *1～15* 0|7 *string*	Default level is 15 if it doesn't be designated
enable password [0 | 7] *string*	0 means password is decryption; 7 means password is encryption. Default is 0

The keyword "7" normally won't be used for password. If its needed, certain signamax router creates the encryption.

Use related NO command to cancel enabled password of some level.

When show run, the displayed password is cryptograph, i.e. the keyword is "7".

Now there're two kinds of encryption methods, they're new/old-encrypted methods, using 'service new-encrypt' and related NO command to shift new and old methods.

User

Set the local user database for local authentication.

router(config)#

Command	Task
user *string* password 0 *LINE*	Set user password
user *string* privilege 0-15	Set privilege level of user
user *string* autocommand <LINE>	Set authorized auto-executed command of user
user *string* autocommand-option nohangup|delay <0_120>	Set options of auto-executed command. The command "nohangup" indicates that the connection won't be disconnected after auto-executed command finished. The command "delay" indicates the time that is used to execute the auto-executed command.
user *string* callback-dialstring *string*	Set the callback number of user

Use related NO commands of above to cancel configuration.

authentication and authorization locally - use the local user databases which is configured with above commands.

User default privilege is 1.privilage 1 is meant for the default user (we should not assign the privilege 1 to any other user).

Line

Set attributes of line user, comprises password, user level, idle timeout and authentication mode.

Command	Task & Description
router(config)# line con 0	Enter line config mode
router(config)#line vty *0~15 0~15*	
line ssh-vty {*0-15*} {*0-15*}	Enter SSH user line configuration mode
router(config-line)#absolute-timeout <0_10000>	Set the total time that permit user to telnet and operate. The default '0' means no limited time. Before the expired time 5 seconds router will give a prompt about the timeout." * Line timeout expired"
router(config-line)#privilege level <0_15>	Set privilege level for telnet user, default level is 1
router(config-line)#access-list <1_1000> access list	Access-list name(only support standard access-list)

router(config-line)#autocommand <LINE>	Set auto-command after user succeeds to telnet under privilege mode; default is no auto-executed command.
router(config-line)#autocommand-option nohangup | delay <0_120>	Set options of auto-command. "Nohangup" indicates that the connection won't be disconnected after auto-command finished (default: connection will disconnect after finished). "Delay" indicates the time that is used to execute the auto-command (default is 0, i.e. no delay). After deploying "autocommand", "delay" can be in effect.
router(config-line)#exec-timeout *<0_35791> <0_2147483>*	Set idle timeout. if the time is 0, the user won't exit for ever when it's idle. Default idle timeout is 5 minutes.
router(config-line)#password 0|7 *LINE*	Configure line password
router(config-line)#login *CR* | local | authentication	Configure the authentication method for telnet. "*CR*" means using line password to authenticate; "local" indicates using local user database to authenticate; "authentication" indicates using AAA method to authenticate. Default is no login, i.e. user can telnet without authentication, only when there's no any AAA configuration.
authorization exec {*default* / *word*}	Configure authorization and statistics modes. If enabling aaa(command aaa new-model) designate exec to each line, the commands authorization and statistics mode. Please refer to AAA Configuration.
authorization commands *level* {default | word}	
accounting exec {*default*|*word*}	
accounting commands *level* {*default* / *word*}	
modem auto-detection	Enable console port modem function.
router(config-line)#timeout login respond *<0_300>*	Set the timeout of waiting user to enter username and password. Default is 30seconds

Use related NO commands of above to resume the default configuration.

User use 'line' authorized attribute to telnet in default. But if the authorized method is set as 'local', then 'local' authorized attribute has precedence over 'line' one. Only when user has no other attribute, 'line' attribute can be in effect. Other attributes are the same such as tacacs and radius.

Example:

```
Configuration:
aaa new-model
aaa authentication login default line
aaa authorization exec default if-authenticated

line vty 0 2
exec-timeout 5 0
absolute-timeout 2
timeout login respond 60
privilege level 14
autocommand show mem
autocommand-option delay 5 nohangup
password 0 vty

after telnet, user should be authorized these 'line' attributes:
debug information as followed (open 'debug author exec' command to see)
AUTHOR/EXEC/LINE  (6): processing AV priv-lvl=14
AUTHOR/EXEC/LINE  (6): processing AV autocmd=show mem
AUTHOR/EXEC/LINE  (6): processing AV nohangup=TRUE
AUTHOR/EXEC/LINE  (6): processing AV timeout=120
```

show privilege

Display the level of user.

router> or router#

Command	Task
show privilege	Default level is 1. So in default, user with 0 level cannot execute this command
user *string* privilege 0-15	Set privilege level of user
user *string* autocommand <LINE>	Set authorized auto-executed command of user
user *string* autocommand-option nohangup|delay <0_120>	Set options of auto-executed command. The command "nohangup" indicates that the connection won't be disconnected after auto-executed command finished. The command "delay" indicates the time that is used to execute the auto-executed command.
user *string* callback-dialstring *string*	Set the callback number of user

Example:

```
router#show privilege
 privilege level is 15
```

System Tools

show

Information displayed by the system command show can be categorized in the following ways:

System software and hardware resources information

System statistic information

System configuration information

Basic system information

System command 'show' keywords:

Command	Description
Stack	Displays usage information of each task stack of the system
Memory	Displays system memory information
Mbuf	Displays system buffer information
Process	Displays system task/process information
Device	Displays system physical and logical device information
Interface	Displays system network interface information
Host	Displays system interior host table information
Arp	Displays system ARP table information
Ip	Displays statistic information of IP layer (including TCP and UDP)
Bootparams	Displays system startup parameters
Startup-config	Displays contents of the system startup configuration file
About	Displays system copyright information
Version	Displays system hardware/software version information

(1) Displaying system stack

```
router#show stack

NAME        ENTRY           TID      SIZE     CUR      HIGH     MARGIN
tExcTask    0x000004b4fc    fe1488    7984     224      464      7520
tLogTask    0x0000051850    fdeb00    4984     216      1072     3912
tMPLog      0x00000f7f34    8a90e8    5112     208      1024     4088
tSccTx0     0x0000240358    8de848    3992     160      224      3768
tSccTx1     0x0000240358    8d3848    3992     160      420      3572
tSccTx2     0x0000240358    8ca848    3992     160      420      3572
tSccTx3     0x0000240358    8c1848    3992     160      420      3572
tEsccRx0    0x000013c0d8    d2ec30    3984     168      1124     2860
tPPP        0x00001d1ae8    d25d28    9320     184      1056     8264
tNetTask    0x00000d0ca0    a1c0a8    9984     192      1120     8864
tFecRxTx    0x000013c710    a0dd88    10224    152      644      9580
tEthTx      0x0000129754    8ec158    12280    168      232      12048
tEthRx      0x000012997c    8e8f40    12280    160      308      11972
tSccRx0     0x00002402dc    8dfde8    4992     152      216      4776
tSccRx1     0x00002402dc    8d4de8    4992     152      748      4244
tSccRx2     0x00002402dc    8cbde8    4992     152      524      4468
tSccRx3     0x00002402dc    8c2de8    4992     152      748      4244
tRtMsg      0x00001e7714    a19780    5368     1368     2216     3152
tModDet0    0x0000237c10    8dd690    3984     176      304      3680
tModDet1    0x0000237c10    8d2690    3984     176      304      3680
tModDet2    0x0000237c10    8c9690    3984     176      308      3676
tModDet3    0x0000237c10    8c0690    3984     176      436      3548
tSdlcTask   0x00002057a4    84d328    9456     168      1244     8212
```

```
tLapbTimer     0x00002fc640    864de8  3984      128       384      3600

tShell1        0x0000025810    82cae8  19800    10040     13128      6672

tActive        0x00001e99d0    89fe40   3992     256        512      3480

tRadius        0x000010e33c    8a64b0   4088     168        232      3856

tTacacs+       0x0000116dd4    8a51e0   2032     160        224      1808

tPkTimer       0x000022a4dc    85fde8   3984     120        408      3576

tBridge        0x000011c1c0    894858   20472    144        404      20068

tLLC2          0x000017f550    88f640   20472    192        428      20044

tDLSwPeer      0x0000200918    89d108   16368    144       1044      15324

tDLSwCore      0x0000200bd8    898ef0   16368    464       1720      14648

tEsccDet0      0x000013c1e4    d2fde8    3984    256        880       3104

tInfoGuide     0x00003a4bd8    83bde8   40272    568       2056      38216

tFecDetect     0x000013c4fc9    370e8     4984    152        944       4040

tEnetDet       0x000012a93c    8e5d28    7152     136        264       6888

tTffsPTask     0x0000259b3c    fdaeb8    2032     136        396       1636

tQLLC          0x00002076d4    85ec30    8184     136       1212       6972

tTelnetd       0x0000101134    8a1058    4080     392        616       3464

tExcTrace      0x0000011258    89ec88    3056     296        528       2528

INTERRUPT    5000      0   1052    3    948
```

(2) Displaying information about system memory

```
router#show memory

status     bytes      blocks     avg block    max block
------     ------     -------    ---------    ---------

free      35241056       16      2202566      26850984
alloc     21077416      20082      1049           -

cumulative
alloc    21571048       25563        842          -
```

```
code
code    10785360         -           -          -


STATISTICS:
Available bytes      35241056
Used bytes           21077416
Total  bytes         56318472
Used bytes percent   37%
```

(3) Displaying usage information of system buffer

```
router# show pool detail
```

Data pool
Statistics for the network stack mbuf

```
type           number
-----          ------
FREE           49887
DATA           1
HEADER         1
SOCKET         9
PCB            12
RTABLE         54
HTABLE         0
ATABLE         0
SONAME         0
ZOMBIE         1
SOOPTS         0
FTABLE         0
RIGHTS         0
IFADDR         20
CONTROL        0
OOBDATA        0
IPMOPTS        2
IPMADDR        11
IFMADDR        0
MRTABLE        0
DRVSCC         0
DRV8SA         0
DRV8S          0
DRV16A         0
DRV4M336       0
DRVEXTSCC      0
DRVQMC         0
MPLSINFO       2
TOTAL         50000
```

```
Number of mbufs: 50000
Number of times failed to find space: 0
Number of times waited for space: 0
Number of times drained protocols for space: 0

____________________
CLUSTER POOL TABLE
_____________________________________________________________________
size     clusters  free      usage
---------------------------------------------------------------------
64       6000      5966      34124
128      36000     35933     351874
256      3200      3198      3711
512      3200      3191      37
1024     180       180       0
2048     400       400       0
---------------------------------------------------------------------
Size: 12416400 bytes

Driver pool

Statistics for the network stack mbuf
type         number
-----        ------
FREE         5990
DATA         10
HEADER        0
SOCKET        0
PCB           0
RTABLE        0
HTABLE        0
ATABLE        0
SONAME        0
ZOMBIE        0
SOOPTS        0
FTABLE        0
RIGHTS        0
IFADDR        0
CONTROL       0
OOBDATA       0
IPMOPTS       0
IPMADDR       0
IFMADDR       0
MRTABLE       0
DRVSCC        0
DRV8SA        0
DRV8S         0
DRV16A        0
DRV4M336      0
DRVEXTSCC     0
DRVQMC        0
MPLSINFO      0
```

```
TOTAL        6000
```

```
number of mbufs: 6000
number of times failed to find space: 0
number of times waited for space: 0
number of times drained protocols for space: 0

CLUSTER POOL TABLE
size     clusters  free      usage
-------------------------------------------------------------------
1596     6000      5632      1119414
-------------------------------------------------------------------
Size: 10056000 bytes

All MBUF pool size: 22472400 bytes
```

(4) Displaying system device information

```
router#show device

drv   name

0     /null
1     /tyCo/0
1     /tyCo/1
4     serial0/0
4     serial1/0
4     serial2/0
4     serial3/0
2     /pipe/temp
3     /logging
3     /more
3     /config
3     /iGuide
6     WEBDEV
3     /flash
2     /pipe/terminal
9     /memory/
```

(5) Displaying status information of about all system interfaces

```
router#show interface

loopback (unit number 0):
     Flags: (0x8069) UP LOOPBACK MULTICAST ARP RUNNING
     Type: SOFTWARE_LOOPBACK
     Internet address: 127.0.0.1
     Netmask 0xff000000 Subnetmask 0xff000000
     Metric: 0, MTU: 32768, BW: 8000000Kbps
     0 packets received; 0 packets sent
     0 multicast packets received
     0 multicast packets sent
```

```
0 input errors; 0 output errors
0 collisions; 0 dropped
```

```
fastethernet (unit number 0):
     Flags: (0x8063) UP BROADCAST MULTICAST ARP RUNNING
     Type: ETHERNET_CSMACD
     Internet address: 192.168.0.83
     Subnetmask 0xffffff00
     Broadcast address: 192.168.0.255
     Ethernet address is 00:01:7a:00:39:be
     Rate:  100Mbit/s   Duplex:  full duplex
     Babbling recvive 0, babbling transmit 0, heartbeat fail 0
     Tx late collision 0, Tx retransmit limit 0, Tx underrun 0
     Tx carrier sense 0, Rx length violation 0
     Rx not aligned 0, Rx CRC error 0, Rx overrun 894
     Rx trunc frame 0, Rx too small 0, Rx alloc mbuf fail 212682
     Metric: 0, MTU: 1500, BW: 100000Kbps
     235216 packets received; 230496 packets sent
     229133 multicast packets received
     223888 multicast packets sent
     0 input errors; 0 output errors
     0 collisions; 0 dropped

ethernet (unit number 0):
     Flags: (0x8062) DOWN BROADCAST MULTICAST ARP RUNNING
     Type: ETHERNET_CSMACD
     Ethernet address is 00:01:7a:08:39:be
     Metric: 0, MTU: 1500, BW: 10000Kbps
     0 packets received; 0 packets sent
     0 multicast packets received
     0 multicast packets sent
     0 input errors; 0 output errors
     0 collisions; 0 dropped

serial (unit number 3):
     Flags: (0x8070) DOWN POINT-TO-POINT MULTICAST ARP RUNNING
     Type: PPP
     Internet address: 1.1.1.2
     Subnetmask 0xffffff00
     Destination Internet address: 0.0.0.0
Metric: 0, MTU: 1500, BW: 128Kbps
2034 packets received; 1848 packets sent
     0 multicast packets received
     0 multicast packets sent
     0 input errors; 0 output errors
     0 collisions; 0 dropped
```

(6) Displaying system version information

```
router#show version

MP3600 Router Version Information
        System ID: 3601000000f3
        Monitor Version: 2.40/1
        Software Version: 4.2.7(YD)-2(integrity)
        System image file: rpm-g-4.2.7(YD)-2.bin
        Compiled: May 29 2004, 17:27:05 by CVS
        Board Name: MP3600 (MPC8240 with 64 MBytes sdram, 8 MBytes flash)
        Board Version: 04 (0x4)

MP3600 system uptime is 1 hour 23 minute 12 second
```

(7) Displaying system copyright information

```
router#show about
```

The MP2600 series modular architecture offers users a branch office and center office that provides the versatility needed to adopt to changes in network technology, as new services and applications become available. With full support of the InfoExpressIOS software, MP2600 modular architecture will provide the power to support the following applications:

```
General Internet/intranet access
LAN-to-LAN Internetwork
Secure Internet/intranet access
Multiservice voice/data integration
Analog and digital dial access services
Virtual Private Network (VPN) access
LAN Internetwork
Interconnecting with IBM SNA Network
```

MP2600 modular architecture comprises the following optional modules:

```
1 Port V.24 Serial Sync/Async Module
1 Port V.35 Serial Sync/Async Module
33.6K/56K Async/Sync Analog MODEM Module
28K CSU/DSU S/T Module
128K CSU/DSU U Module
16 Async Port & 2 Sync Port Serial Module
IP Telephone POTS Module
IP Telephone PBX Module
ISDN BRI Module
ISDN PRI Module
```

Protocol Debugging

The system provides debugging switches of many protocols including IP, PPP, HDLC, OSPF, FR, and X25. The following example provides a simple introduction as to how to turn on/off a debugging switch:

Turning on a protocol-debugging switch
Turning on the debugging switch of IP protocol access-list datagram

```
router#debug ip packet access-list
```

Turning on the debugging switch of RIP protocol

```
router#debug ip rip events
```

Turning on the PPP protocol debugging switch (on the interface s0)

```
router#debug ppp negotiation s0
```

Turning on the HDLC protocol debugging switch

```
router#debug hdlc s0
```

FR has many protocol debugging switches, including

```
Debug frame-relay lmi [interface/cr]
Debug frame-relay log [interface/cr]
Debug frame-relay packet [interface/cr] etc.
```

Turning off a protocol-debugging switch: To turn off a protocol-debugging switch, users need to add a command word no before related command that turns on the switch.

SysLog (System Logging)

System log function comprises two aspects; one is to add top information to printed logging information such as time prickling and task name. Another is to output and save logging information in various types, including printing to console port and then to telnet terminal, writing to memory file, flash file, and sending to logging server.

Following is the system logging function command:

Command	Description	Config mode
logging enable	Enable logging function. Command no logging enable is used for disabling the function	config
logging color { alerts|critical| debugging| emergencies| errors|informational| notifications| warnings} [blue|brown|cyan| green| purple|red|white]	Configure the logging color in command line terminal	config
logging buffer	Configure enabling buffer logging information in memory. The executing command **no logging buffer** is used for enabling the function	config
logging buffer max-size <4096-409600>	Configure buffer size for recording logging information	config
logging buffer {<0-7>|alerts| critical|debugging| emergencies|errors| informational| notifications| warnings}	Configure the logging information recorded in buffer	config
logging console	Configure enabling sending logging information to console. The command **no logging console** is used to disable the function	config
logging console {<0-7>|alerts| critical|debugging| emergencies|errors| informational|	Configure logging information displaying in console	config

notifications| warnings}		
logging file	Configure enabling saving logging information to flash file system. The command **no logging file** is for disabling the function	config
logging file max-size <4096-1048576>	Configure logging file size in flash file system	config
logging file {<0-7>|alerts| critical|debugging| emergencies|errors| informational| notifications| warnings}	Configure the logging information in logging file	config
logging trap	Configure enabling sending logging information to designated logging server. The command **no logging trap** is used for disabling the function.	config
Logging {hostname|A.B.C.D} {<0-7>/alerts/ critical/debugging/ emergencies/errors/ informational/ notifications/ warnings}	Configure logging server host name or IP address	config
logging source-ip A.B.C.D	Configure the source ip address connecting logging server	config
logging event	Configure sending all operating records to logging server	config
logging monitor	Configure enabling sending logging information to terminal. The command **no logging monitor** is used for disabling the function.	config
logging monitor {<0-7>|alerts| critical|debugging| emergencies|errors| informational| notifications| warnings}	Configure the logging information displaying in terminal	config
logging facility {auth|cron| daemon|kern |local0|local1 |local2|local3 |local4|local5 |local6|local7	Configure the logging information type. Signamax routers default type is local7	config

|lpr|mail|news |sys10|sys11 |sys12|sys13 |sys14|sys9 |syslog|user |uucp}		
service timestamps log [datetime [localtime/ msec/ show-timezone]| uptime]	Configure logging information option: date, time zone, local time and whether displaying in millisecond.	config
service taskname log	Configure added task name in logging information	config
clear logging [buffer|file]	Clear memory and flash file logging content	enable
show logging [file|buffer]	Show memory and flash file logging content	enable

SysLog can record system information at every level and save in flash file. SysLog only records information at levels such as emergencies (level 0), alerts (level 1), critical (level 2), errors (level 3) or warnings (level 4). This can be changed by sysLog configuration command.

Command:

```
router(config)#logging  trap  level  <CR>
<0_7>                    Logging severity level
alerts                   Immediate action needed
   (severity=1)
critical                 Critical conditions
(severity=2)
debugging                Debugging messages
   (severity=7)
emergencies              System is unusable
   (severity=0)
errors                   Error conditions
   (severity=3)
informational            Informational messages
   (severity=6)
notifications            Normal but significant conditions
   (severity=5)
warnings                 Warning conditions[default]
   (severity=4)
```

sysLog severity level:

Severity level	Keyword	Description
0	emergencies	System is unusable
1	alerts	Immediate action needed
2	critical	Critical conditions
3	errors	Error conditions
4	warnings	Warning conditions
5	notifications	Normal but significant conditions
6	informational	Informational messages

7	debugging	Debugging messages

For example, if you configure "logging trap notifications", then those logging information from level 0 to level 5 could be recorded.

CPU Utilization

Provide the tools to examine utilization of CPU. After enabling the switch monitoring CPU, the CPU utilization of each task in a period can be examined.

Provide two groups of commands to enable/disable the switch monitoring CPU utilization: spy cpu/no spy CPU in the privileged user mode and check cpu enable/check cpu disable in the global configuration mode. The command check cpu enable can be saved in the configuration file.

Related commands in the global configuration mode are:

Command	Description
router(config)#check cpu enable	Enable the switch monitoring the CPU and start to collect data of CPU utilization
router(config)#check cpu disable	Disable the switch monitoring CPU and stop collecting the data of CPU utilization. The default status is disable
router(config)#check cpu time-interval <1_3600>	Set the interval of refreshing the CPU utilization. The default interval is 2 seconds
router(config)#check cpu view [simple|_CR_]	Whether to display in the simple mode. Namely that only the CPU task is displayed. The simple mode is disabled by default
router(config)#check cpu parameter	Examine some parameters and status of check cpu, for example, whether to enable the monitoring switch

In the privileged user mode, use show cpu to display the CPU utilization. For example:

```
router#show cpu

NAME          TID        PRI    total% (ticks)   delta%(ticks)  %
------        ----       ---    --------------   -------------  -----
tCheckCpu     37640824   30     0%(80)           0%(2)           0%
tShell1       37840344   20     35%(5868)        0%(0)           0%
tFwdTask      41410224   45     15%(2478)        0%(0)           0%
tNetTask      41420760   50     5%(918)          0%(0)           0%
KERNEL        0          0      4%(780)          0%(0)           0%
INTERRUPT     0          0      0%(12)           0%(0)           0%
IDLE          0          0      38%(6260)        99%(398)        99%

Average cpu utilization rate is 59% in timeslice 00:01:22 (16396 ticks)
 cpu utilization rate is 0% in timeslice 00:00:02 (400 ticks)
```

When the switch monitoring the CPU is enabled, the task tCheckCpu cannot stop collecting the CPU data, which will occupy some CPU source. So, if it is unnecessary to diagnose the CUP utilization of each task, you had better not enable the switch.

Configure System Alarming Temperature

MP7200 router supports system alarming temperature threshold value, when CPU temperature reaches the threshold value, the log appears and trap will be sent (need trap configuration), the default value is 85℃.

Command	Description	Configuration mode
alarm temperature *number*	Configure CPU alarming temperature threshold value, and the range is 60－85℃	config
no alarm temperature	Renew CPU alarming temperature threshold value as 85℃	config

System Remote Login Service

Telnet

MP series router provides telnet service end/client end function (service port 23), and permits the user to operate the router by telnet via LAN or WAN. It provides 16 telnet users online. The telnet property can be showed via command line vty.

It provides telnet client end command in normal user mode and privileged user mode the following command can be executed for telnet.

Command	Description	Configuration mode
telnet [vrf *vrf-name*] *hostname/ip-address*	telnet host computer or equipment, it can be host or IP address, and also VRF name	STD enable

SSH

MP router provides much more secure telnet service — SSH service (service port 22). It permits 16 SSH users login, the command line ssh-vty is used for ssh property.

Command	Description	Configuration mode
sshkeygen	New SSH key	enable config
ip ssh server	Enable SSH service	config
no ip ssh server	Disable SSH service	config
show fingerprint	Display SSH key	enable

Interface Configuration

This chapter explains interfaces supplied by Signamax series routers and how to configure them. Following topics are explained:

Interface type supported by Signamax series routers

Configuring Ethernet interfaces

Configuring high-speed serial interfaces

Configuring a 16-asyn-port/printing module

Configuring a CE1 module

Configuring an 8-syn-port module

Configuring a built-in base-band modem module

Configuring a built-in frequency-band modem module

Configuring an ISDN module

Configuring ATM module

Configuring POS module

Configuring CPOS module

Configuring interface group

Interface Types

This section explains the interface types supported by Signamax series routers and how to configure them.

Ethernet port

Configuring port

High-speed serial-port

Asynchronous serial-port

Synchronous serial-port

Synchronous/Asynchronous serial-port

Built-in 56K/33.6K frequency-band MODEM

Built-in 128K base-band MODEM

ISDN S/T interface module

ISDN U interface module

Unchannelized E1

Channelized E1

PRI Interface

IP telephone interface

Configuring Interfaces

The connection situation of physical interfaces, physical operational modes and related operational parameters

For a WAN interface, the link-layer encapsulation protocol and operational parameters should be appointed between WAN interface and the opposite-end interface connected with WAN interface.

The network-layer IP address of the interface should be configured correctly.

Correctly configuring the static route of destination network that can be reached via the interface, or configuring the operational parameters of the dynamic routing protocol on the interface.

If the interface supports dialup mode, the dialup mapping and MODEM management need be configured more.

If a firewall need be configured on the interface, it is necessary for you to configure related packet filtering and NAT parameters.

Configuring Ethernet Port

This section explains:

Protocols supported by Signamax series routers

Configuring the network address

Configuring VLAN Interface

Establishing the address resolution (ARP)

Proxy ARP

Monitoring & maintenance

Protocols

The Ethernet port of Signamax router can support the following two frame formats:

Ethernet_II (ARPA)

Ethernet_SNAP

The foregoing frame formats are used to encapsulate the network-layer IP protocol. When receiving data, the Ethernet port can automatically recognize frame formats. But when transmitting data, the port can do nothing but make encapsulation according to the specified frame format.

Ethernet Commands

Command	Description	Config. mode
ip address A.B.C.D mask	Configure IP address of Ethernet port	config-if-××
arp A.B.C.D H.H.H	Define a static ARP buffer	config
no arp A.B.C.D H.H.H	Delete a static ARP buffer	config
show arp	Observe ARP buffer	
ip proxy arp	Run proxy ARP	config-if-××
no ip proxy arp	Disable proxy ARP	config-if-××

Configuring Network Address

The router can support IP protocol on the network layer. The network/host address and sub-net mask need be configured with the following command:

Command	Description
router#configure terminal	The user enters global configuration mode from the privileged user mode
router(config)# interface fastethernet0	Enter the configuration status of interface f0
router(config-if-fastethernet0)#ip address A.B.C.D mask	Configure IP address and sub-net mask of the interface f0
router(config-if-fastethernet0)#ip address A.B.C.D mask secondary	Configure secondary address of the interface f0

A.B.C.D is the IP address of the interface, and mask is the sub-net mask of the interface. Sixty-four secondary addresses can be configured at best on the Ethernet interface. There is no limit of the secondary addresses for the master interface.

Address Resolution Protocol (ARP)

Signamax series routers can support Ethernet address resolution protocol (ARP) used to establish the relation between an IP address and a MAC address. After an IP address is input, ARP can determine a MAC address related with the IP address.

Once the MAC address is determined, the relation of IP address/MAC address will be saved into ARP high-speed buffer so as to realize the high-speed search. After that, an IP datagraph is encapsulated into a link-layer frame and transmitted in the network.

Defining Static ARP Buffer

ARP provides dynamic mapping between an IP address and MAC address. Most hosts can support the dynamic address solution, so no static ARP buffer need be specified.

If it is necessary to define ARP buffer, you can define it in the global configuration mode—namely load a permanent item into ARP buffer. MPROUTER software uses it to translate a 32-bit IP address into a 48-bit hardware address.

Execute the following commands in the global configuration mode:

Command	Description
router(config)#arp A.B.C.D H.H.H	Define static ARP buffer
router(config)#no arp A.B.C.D H.H.H	Delete static ARP buffer

A.B.C.D is a host name or IP address and H.H.H is a MAC address. H means a hexadecimal number between 0 and FFF.

Examining ARP Buffer

To display contents of ARP cache used by the system, you can use the command show arp to examine the cache.

```
router#show arp
LINK LEVEL ARP TABLE
destination      gateway           flags Refcnt   Use          Interface
-------------------------------------------------------------------------
129.255.117.5    0050.ba27.e285    405    2       32455        fastethernet0
129.255.150.1    0050.ba27.d0f5    405    2       1011270      fastethernet0
-------------------------------------------------------------------------
```

Destination: Destination IP address

Gateway: MAC address of the destination IP address

Flags: Flag bit (405—the dynamic ARP, Co5—the static ARP)

Refcnt: Number of times using ARP

Use: Number of frames transmitted to IP address

Interface: Interface connecting with IP address

To refresh ARP item, you can use privileged EXEC command clear arp to do it.

router#clear arp

Proxy ARP

If an ARP request is transmitted from a host in a network to a host in another network, the router connecting the two networks can answer the request. The foregoing procedure is called Proxy ARP.

This way can make the end sending ARP request mistake that the router is the destination host. In fact, the destination host is on another side of the router.

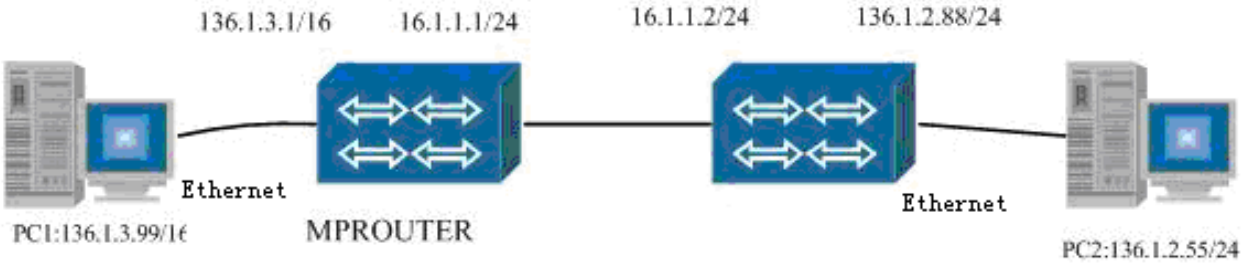
The router, whose function is equivalent to the proxy of the destination host, can transmit packets to the destination host. (RFC1027)

Signamax router supports proxy ARP.

Execute the following command in the interface configuration mode:

Command	Description
router(config-if-fastethernet0)#ip proxy-arp	Enable proxy ARP
router(config-if-fastethernet0)#no ip proxy-arp	Disable proxy ARP

The proxy ARP is enabled by default. The following example is about the typical ARP application and configuration:



136.1.0.0 is a 16-bit mask of the network segment in which PC1 is located.

136.1.2.0 is a 24-bit mask of the network segment in which PC2 is located.

No gateway is configured for PC1. For PC2 136.1.2.88 need be set its gateway or there exists a route to PC1 (IP address of the next hop is 136.1.2.88)

If ARP proxy is disabled on the Ethernet of MPROUTER, PC1 fails to ping 136.1.2.55 successfully.

For packets in the same network, PC1 broadcasts ARP request so as to acquire the MAC address of the destination host. After getting the address, PC1 transmits the packet to destination.

Both the destination host and PC1 on the same network (which can be known according to the mask of PC1), but they are not located in the same network physically. If there is no response after PC1 sends ARP request, PC1 pings unsuccessfully.

If MPROUTER enables ARP proxy, MPROUTER can use its MAC address to answer the request sent by PC1, and PC1 can ping successfully. ARP proxy of MPROUTER is applied to this case.

Monitoring & Maintenance

When finishing the configuration of the Ethernet interface, you can enter the privileged user mode and execute the command show interface to display the diverse configuration parameters and operational status of the Ethernet interface.

```
Router#show interface fastethernet0
fastethernet (unit number 0):
Flags: (0x8063) UP BROADCAST MULTICAST ARP RUNNING
(Protocol signal UP)
Type: ETHERNET_CSMACD
(Interface type: CSMA/CD(IEEE802.3) )
Internet address: 129.255.117.22
(Port address:129.255.117.22)
Netmask 0xffff0000 Subnetmask 0xffff0000
(Network mask:255.255.0.0 Sub-net mask:255.255.0.0)
Broadcast address: 129.255.255.255
(Broadcast address:129.255.255.255 )
Metric: 0, MTU: 1500, BW: 100000Kbps, DLY: 100 usec
(Maximal transmitting unit:1500；bandwidth:100M；Delay:100 microseconds)
Ethernet address is 0001.7a00.0016
(MAC address:0001.7a00.0016)
Rate:  100Mbit/s   Duplex:  full duplex
(Rate:100M；  Operational mode:full duplex mode)
Babbling recvive 0, babbling transmit 0, heartbeat fail 0
Tx late collision 0, Tx retransmit limit 0, Tx underrun 98
Tx carrier sense 0, Rx length violation 0
Rx not aligned 4, Rx CRC error 13, Rx overrun 68
(In the received frames, there are 4 un-aligned ones, 13 CRC error’s ones and
68 overrun ones. )
Rx trunc frame 0, Rx too small 0, Rx alloc mbuf fail 0
5 minute input rate 19000 bits/sec12 packets/sec
(The input rate is 19000 bits/sec, namely 12 packets/sec, in the late 5
minutes.)
5 minute output rate 6000 bits/sec2 packets/sec
(The output rate is 6000 bits/sec namely 2 packets/sec, in the late 5
minutes.)
63200024 packets received; 9128013 packets sent
(63200024 packets are received；and 9128013 packets are sent)
57157487 multicast packets received
(57157487 multicast packets are received)
1045 multicast packets sent
(1045 multicast packets are sent.)
37 input errors; 0 output errors
(There are 37 input errors and 0 output error.)
0 collisions; 24166659 dropped
(There is 0 collision; and 24166659 packets are discarded.)
```

Configuring High-speed Serial Interface

Signamax router can provides two kinds of high-speed serial interfaces: one can support both synchronous and asynchronous operation mode, called a synchronous/asynchronous serial interface; another can operate only in the asynchronous operation mode, such as a configuration interface.

The configuration interface Console is used to connect with user terminals and serves as the configuration and monitoring interface of the router. Generally, you need not configure the configuration interface, and it is not also recommended for you to do it.

The serial interface of Signamax router supports the following applications:

Connecting with the external Modem, and serving as a dialup interface or a backup interface;

Operating in the V.24/V.35 interface mode (high-speed synchronous/asynchronous WAN interface)

Supporting link-layer protocols, such as PPP, SLIP, FR, X25 and HDLC;

The extended synchronous/asynchronous serial interface or asynchronous serial interface can support link-layer protocols such as PPP, SLIP, X25, HDLC and FR (but the asynchronous serial interface cannot support FR).

The main contents of this section are listed as follows:

Configuring an asynchronous serial interface

Configuring a synchronous serial interface

Monitoring and maintenance

Configuring Asynchronous Serial Interface

Without any configuration, an asynchronous serial interface can work in the asynchronous operation mode. To make the synchronous/asynchronous serial interface work in the asynchronous operation mode, you can execute the following commands.

For example, you can execute the following commands to configure the serial interface 0 and make it work in the asynchronous operation mode:

Router(config-if-serial0) #

Command	Description
physical-layer async	Configure the asynchronous operation mode for the serial interface 0(serial0) .
speed 9600	Configure the bund rate 9600 for the asynchronous serial interface. And the baud rate can be select from 1200bps/2400bps/4800bps/ 9600bps/ 19200bps/38400bps/57600bps/115200bps.
databits 8	Configure the databits of the asynchronous serial interface: 8. And the value can be selected from 5/6/7/8.
stopbits 1	Configure the stopbits of the asynchronous serial interface: 1. And the value can be selected from 1/2.
parity none	Configure the parity of the asynchronous serial interface: none. And the value can be selected from even/none/odd/space/mark.
flow-control none	Configure the flow-control of the asynchronous serial interface: none. And the value can be hardware flow-control (none) or software flow-control.
Tx-on dcd—dsr	Set the sending condition of the serial interface. And the default condition is dcd—dsr.

When the asynchronous serial interface connects with the external Modem, the baud rate is applied to the communication between the serial interface and the Modem. So their baud rate can be set differently. The line rate can be determined after the Modem makes negotiation with the serial interface. And when two serial interfaces connect together directly, they need be configured with the same baud rate.

When working in the hardware flow-control mode, the asynchronous serial interface can, by means of detecting the CTS signal, determine whether to send data; and when working in the software flow-control mode, the asynchronous serial interface can, by means of judging the flow-control character (XON/XOFF) determine whether to send data.

Configuring Synchronous Serial Interface

Without any configuration, a synchronous serial interface can work in the synchronous operation mode. The synchronous serial interface can work in the DTE/DCE mode. When working in the DTE mode, the external DCE equipment (such as the external synchronous Modem) connecting with the interface provides the clock source; and when working in the DCE mode, the router connecting with the interface provides the clock source.

The synchronous serial-interface can provide a V.24/V.35 interface. By means of internal jumper, the router can provide different types of interfaces.

For example, you can execute the following command to configure the serial interface 0 (serial0) and make it work in the synchronous operation mode:

```
Router(config-if-serial0) #physical-layer sync
```

Configuring Operation Mode of Synchronous Serial Interface

By default, a synchronous serial interface works in the DTE mode. And you can make the interface work in the DCE mode via configuring DCE clock rate and adopting the DCE cable.

The different operation modes of the synchronous serial interface are related with the different clock options:

If the synchronous serial interface works in the DTE mode, the serial interface receives the clock provided by the external DCE equipment. Here, the DTE serial interface cannot only select the receiving /sending clock of the DCE equipment as itself receiving/sending clock, but also regard the sending clock of the DCE device as itself receiving/sending clock. For example, you can use the following command to set the sending clock of the DCE device as itself receiving/sending clock:

```
Router(config-if-serial0) )#clock multiplex – Configuring the
DTE clock multiplex.
```

When the interface works in the DTE mode, to eliminate the half clock cycle of the line some time, you can invert the receiving clock of the DTE.

```
Router(config-if-serial0) clock invert – Configuring the DTE
clock  invert.
```

The clock is not inverted by default.

If the synchronous serial interface works in the DCE mode, the serial interface need provide the clock for the external equipments. For example, you can use the following command to set the DCE clock rate:

```
Router(config-if-serial0) # clock rate 128000 - Configuring
the DCE clock rate as 128000.
```

In the synchronous operation mode, the serial interface can support a very wide clock rate scope. The lowest clock rate is 1200bps, and the highest rate is related with the operation mode of the interface.

The highest clock rates supported by the interfaces in the different interface modes are different:

In the V.24 mode, the highest clock rate can reach 200kbps;

In the V.35 mode, the highest clock rate in the DTE mode can reach 8Mbps and that in the DCE mode can reach 2Mbps.

The basic configuration of an 8 syn/asyn expansion interface is the same as that of the high-speed WAN interface. And the difference between them is that the rate supported by the former is relatively lower.

Monitoring & Maintenance

When finishing the configuration of the interface, you can enter the privileged user mode and execute the command show interface to display the diverse configuration parameters and operational status of the interface.

```
Router#show interface serial0
serial (unit number 0):


Flags: (0x8071) UP POINT-TO-POINT MULTICAST ARP RUNNING
(Protocol signal : UP)
     Type: PPP
(Interface type:PPP)
     Internet address: 10.1.1.1
(Port address:10.1.1.1)
     Netmask 0xff000000 Subnetmask 0xffffff00
(Network mask:255.0.0.0 Sub-net mask:255.255.255.0)
     Destination Internet address: 10.1.1.2
(The IP address of the opposite end:10.1.1.2)
     Metric: 0, MTU: 1500, BW: 128Kbps, DLY: 20000 usec
(Maximal transmitting unit:1500；bandwidth:128K；Delay:20 microseconds)
     5 minute input rate 790000 bits/sec14 packets/sec
     (The input rate is 790000 bits/sec, namely 14 packets/sec, in the late 5
minutes)
     5 minute output rate 788000 bits/sec, 12 packets/sec
      (The output rate is 788000 bits/sec, namely 12 packets/sec, in the late
5 minutes)
     1761641 packets received; 1827994 packets sent
(1761641 packets are received; and 1827994 packets are sent.)
     0 multicast packets received
```

```
(0 multicast packet is received.)
     0 multicast packets sent
(0 multicast packet is sent.)
     148 input errors; 146 output errors
(There are 148 input errors 146 output errors)
     0 collisions; 9 dropped
(There is 0 collision; and 9 packets are discarded)
      lcp:OPENED, ipcp:OPENED, cdpcp:OPENED
      rxFrames: 2296829, rxChars -1694564374
      (the number of the received frames is 2296829, and total bytes of the
received frames are -1694564374.)
      txFrames: 2275846, txChars -1714594630
      (The number of the sent frames is  2275846, and total bytes of the sent
frames are -1714594630.)
      rxNoOctet 17, rxAbtErrs 6, rxCrcErrs 0
(In the received frames, there are 17 un-aligned ones. Six received frames
are discarded and there exists no CRC error's frame. )
      rxOverrun 0, rxLenErrs 0, txUnderrun 0
      (there exists  0 rxOverrun frame, 0 rxLenErr frame and 0 txUnderrun
frame.)
      rate=2000000 bps
      (The line rate is 2M)
      DCD=up  DSR=up  DTR=up  RTS=up  CTS=up  Txc=up
```

Configuring 16-async Serial Interface Module

Signamax router comprises a 16-asyn-serial-interface module. The module adopts the interface standard—RS-232, uses DB25 (M)/DB25 (F) connectors and RJ45 socket, supports 9600bps-115200bps baud scope, operates in the DTE or DCE mode. Additionally, the module can support the following services:

Connecting with a terminal (with the function of terminal-number fixing)

Connecting with ATM (automated teller machine)

Connecting with a PC station

Connecting with a router

Connecting with a frequency-band/base-band Modem

Supporting PC/router dialup access

Other serial equipment.

The concrete configuration is the same as that of the asynchronous serial-interface.

Configuring CE1 Module

Brief introduction to a CE1 interface:

A CE1 interface can be physically divided into 32 time-slots whose number is from 0 to 31. Time-slot 0 cannot be used to transmit data.

Each frame of the CE1 circuit is composed of 32 time-slots and the transmission rate of each time-slot is 64K.

When a CE1 interface is used, the total time-slots (1~31) can be optionally divided into several groups. After bounded together, each group of time-slots can serve as a logical interface (use the command "channel-group" shell to realize it), supporting link-layer protocols such as PPP, X.25, HDLC and FR.

The main contents of this section are listed as follows:

Configuring a CE1 interface

Monitoring a CE1 interface

CE1 Interface

CE1 interface divides into 32 timeslots, and the number is 0-31. Timeslot 0 is not used to transmit data. Each frame on CE1 circuit is constituted of 32 timeslots, and the transmitting rate of each time-slot is 64k.

When using CE1 interface, timeslot 1-31 can be divided into different groups, and each group timeslot can be used as an interface after binding (via "channel-group" shell). The link layer supports ppp, x.25, hdlc, fr etc. protocols.

Configuring CE1 Interface

The tasks of CE1 configuration are listed as follows:

Configuring the physical-layer operation parameters of the CE1 interface, including frame check mode and line encoding format etc.

Configuring the channel-group operation parameters

Configuring an interface.

Perform the following configuration in the global configuration mode:

Command	Description
router(config)#controller e1 0/0	Use the slot-number and unit-number to determine the location (0/0) of the controller and enter the E1 configuration mode.

For the low-end routers including MP1700, MP2500 and MP2600 etc, only the slot S0 can support the CE1 module.

Configuring the physical-layer operation parameters of the CE1 interface

Command	Description
router(config-controller)#framing crc4	Use the configuration command of a framing controller to select a frame type for the E1 data line. And the following types can be selected: crc4: Specify the CRC4 check mode for the E1 interface to receive/transmit data; no-crc4: Specify the E1 interface not to adopt the CRC4 check mode for receiving/transmitting data; Default: Set the default type (CRC4 check is valid only for data transmission) .
router(config-controller)#linecode hdb3	Use the configuration command of a line code controller to select a line encoding type for the E1 line. And the following types can be selected: Ami: Set the AMI (alternate mark inversion) as the line encoding type. E1 is invalid by default.
router(config-controller)# clock source internal	Use the configuration command of a clock source controller to select a line clock for the E1 line. And the following types can be selected.: Internal: The CE1 interface provides clock source by itself; Line: Extract the clock from the line. The type is valid by default.
router(config-controller)#pri-group	The CE1 interface is configured as the PRI mode. After that, an interface similar to S0/0:15 can be generated.

Configuring the channel-group operation parameters:

Command	Description
router(config-controller)#channel-group number timeslots range	Set the time-slots occupied by each channel.

Number: The channel-group number. When an E1 data line is configured, the scope of the channel-group number is from 0 to 30.

Range: The value scope to which one or more time-slots in a channel-group belong. The first time-slot number is 1, and its range is from 1 to 31.

When a time-slot is configured, the time-slot-number of the start-time-slot should be less than that of the stop-time-slot, or else, the time-slot-number is invalid.

If two channels are configured with the repeating time-slot, the configuration is invalid and no interface can be generated.

When a time-slot is configured, the scope of the time-slot should match with a channel-group-number. And it is the service provider that defines time-slots including a channel-group.

The following example defines three channel-groups: channel-group 0 comprises a single time-slot, channel-group 2 comprises three time-slots and channel-group 7 comprises a single time-slot.

Command	Description
router(config)#controller e1 0/0	Use the slot-number and unit-number to determine the location (0/0) of the controller and enter the E1 configuration mode.
router(config-controller)#channel-group 0 timeslots 1	Configure time-slot 1 for channel-group 0.
router(config-controller)#channel-group 2 timeslots 3-5	Configure 3~5 time-slots for channel-group 2. (That is to say that the rate of the channel-group 2 is 192K)
router(config-controller)#channel-group 7 timeslots 6	Configure time-slot 7 for channel-group 7.
router(config-controller)#framing crc4	Enable CRC4
router(config-controller)#linecode hdb3	Configure the line code as HDB3.

After finishing the configuration above, you can perform the interface configuration. The interface form is s0:0 s0:2 s0:7.

Command	Description
router(config)#interface s0/0:0	Enter the channel-group 0.
router(config-if-serial0/0:0)# encapsulation ppp	Encapsulate the link-layer protocol as PPP.
router(config-if-serial0/0:0)#ip add 1.1.1.1 255.0.0.0	Configure the IP address 1.1.1.1 and subnet mask 255.0.0.0.
router(config-if)#exit	
router(config)#interface s0/0:2	Enter the channel-group 2.
router(config-if-serial0/0:2)# encapsulation hdlc	Encapsulate the link-layer protocol as HDLC.
router(config-if-serial0/0:2)#ip add 2.2.2.1 255.0.0.0	Configure the IP address 2.2.2.1 and subnet mask 255.0.0.0.
router(config-if)#end	

When multiple time-slots are configured, "-" is used between the start-slot and the stop-slot.

CE1 Interface Configuration

In the following examples, three CE1 interfaces have been established. Channel group0: single timeslot, channel group 2: 2 timeslots, channel group 7: single timeslot.

Command	Description
router(config)#controller e1 0/0	Define controller position (0/0) via unit number, and then enter E1 configuration mode.
router(config-controller)#channel-group 0 timeslots 1	Configure channel group 0 occupying timeslot 1.
router(config-controller)#channel-group 2 timeslots 3-5	Configure channel group 2 occupying timeslot 3-5. (the speed rate of channel group 2 is 192K)
router(config-controller)#channel-group 7 timeslots 6	Configure channel group 7 occupying timeslot6.
router(config-controller)#framing crc4	Configure framing CRC4 function
router(config-controller)#linecode hdb3	Configure linecode HDB3

After above configuration, start to configure the interface. The interface form is serial0/0:0 serial0/0:2 serial0/0:7.

Command	Description
router(config)#interface serial0/0:0	Enter channel group 0/0.
router(config-if-serial0/0:0)#encapsulation ppp	Encapsulate link protocol PPP.
router(config-if-serial0/0:0)#ip add 1.1.1.1 255.0.0.0	Configure IP address 1.1.1.1, subnet mask code 255.0.0.0
router(config-if)#exit	
router(config)#interface s0/0:2	Enter channel group 2
router(config-if-serial0/0:2)#encapsulation hdlc	Encapsulation link protocol is hdlc
router(config-if-serial0/0:2)#ip add 2.2.2.1 255.0.0.0	Configure IP address 2.2.2.1, subnet mask code 255.0.0.0
router(config-if)#end	

Monitoring CE1 Module

After finishing the interface configuration, the user can enter the privileged user mode and execute the command show interface to display the parameter configuration and operation status of the channel-group. Each parameter is the same as that of the serial interface.

When the interface information is examined, the massive error frames can be discovered from the E1 statistics information, the link-layer negotiation is slow, and there exists packet loss during the PING course.

The CE1 module can support two kinds of connection cables: one is 75Ω non-balance coaxial cable, and the other is 120Ω balance twisted-pair cable. When equipment connection is performed, the impedance may be unmatched.

Configuring E1 Module

By default, an E1 interface follows G.703 and the total bandwidth 2.048Mbit/ is used for data transmission. When the E1 interface is used for the frame structure, the interface can be used for G.704 common-channel associated signaling (CCS) and G.704 channel associated signaling (CAS) structure:

The sixteenth time-slot of the former structure can be used to transmit data, and the sixteen time-slot of the latter structure can be used to transmit signaling except data; and time-slot 0 of the foregoing two structures cannot be used to transmit data.

When the E1 interface is employed, the total time-slots can be optionally bound together to serve as an logical interface that has the same logic as that of the synchronous serial-interface and can support PPP, X.25 and HDLC protocols.

E1 Interface

In default status, E1 interface keeps to G.703 unframing structure standard, all bandwidth 2.048Mbit/s is used for data transmission. When using E1 interface, all timeslots can be binding together and using as an interface, it supports ppp, x.25, fr, hdlc protocols.

Configuring E1 Interface

The configuration tasks of an E1 interface are listed as follows:

Configuring the physical-layer operation parameters of an E1 interface

Configuring the link-layer operation parameters of an E1 interface

Configuring the physical-layer operation parameters of an E1 interface:

Router(config-if-serial0/0) ?

Command	Description
Router(config-if-serial0/0) #timeslot <start-slot - stop-slot>	Use the time-slot interface configuration command to enable the framed serial interface of the G.703E1 port adapter. And using the negation form of the command or setting the stat-slot as 0 can restore the default. start-slot: The first sub-frame of the master frame, the scope of the parameter value is between 1 and 31, and the parameter value should be less than or equal to stop slot. stop slot: The last sub-frame of the master frame, the scope of the parameter value is between 1 and 31, and the parameter value should be more than or equal to start slot.
Router(config-if-serial0/0) #ts16	The E1 module operates in the CCS mode. The command can take effect only in the framing mode.
Router(config-if-serial0/0) #no timeslot	The E1 mode adopts G.703 protocol and 2M mode.
Router(config-if-serial0/0) #no ts16	The E1 module operates in the CAS mode.
Router(config-if-serial0/0) #crc4 {rcrc4|tcrc4|(CR)}	Configure the check mode of the E1 data line as crc4. The follow types can be selected: crc4: Specify the E1 interface to adopt the CRC4 check mode

	for receiving/transmitting data; no-crc4: Specify the E1 interface not to adopt the CRC4 check mode for receiving/transmitting data; rcrc4: The receiving CRC4 is valid. tcrc4: The transmitting CRC4 is valid.
Router(config-if-serial0/0) # clock source <line|internal>	Set the clock mode of the interface: Line: Set the operation clock mode as the line clock. Internal: Set the operation clock mode as the internal clock.

By default, G.703 is configured as the transparent 2M mode, and the clock as the line clock.

Nothing but the serial-interface 0 of low-end routers(including MP1700, MP2500 and MP2600) can support the E1 module.

The E1 interface can only operate in the synchronism mode.

Configuring the link-layer operation parameters of an E1 interface

Router(config-if-serial0) ?

Command	Description
Router(config-if-serial0) # encapsulation < Configure encapsulation protocol>	Configure the link-layer protocol used on the E1 interface.
Router(config-if-serial0) #ip address <unicast address> < network mask>	Configure the IP address and related subnet mask of the E1 interface.

The link-layer protocols of the E1 interface can be configured as nothing but the synchronism mode;

By default, the link-layer protocol configured for the E1 interface is HDLC.

The following example defines an E1 interface: 1-31 time-slot, CCS mode, line clock, no CRC4, PPP link-layer protocol, IP address 1.1.1.1 and 8-bit mask.

Command	Description
router(config)#interface serial0/0	Enter the E1 interface.
router(config-if-serial0/0)#timeslots 1-31	Set the E1 interface to use 1-31 time-slot.
Router(config-if-serial0/0)#ts16	Set the operation mode of the E1 interface as CCS.
Router(config-if-serial0/0)#no crc4	Set the E1 interface to perform no CRC4 check for the received data and fill no CRC4 checksum in the transmitted data.
Router(config-if-serial0/0)# encapsulation ppp	Configure the link-layer protocol as PPP.
Router(config-if-serial0/0)#ip address 1.1.1.1 255.0.0.0	Configure the IP address 1.1.1.1 and 8-bit mask of the E1 interface.

When multiple time-slots are configured, "-" is used between the start-slot and the stop-slot. And when a single time-slot is configured, the time-slot can be directly filled in. when the E1 interface is configured as the CAS mode, the sixteenth time-slot is only used to transmit signaling.

E1 Interface Configuration Example

In the following example, E1 interface timeslot is 1-31, CCS, line clock, but not crc4. Configure PPP link layer protocol on interface, ip address is 1.1.1.1, mask is 8.

Command	Description
router(config)#interface serial0/0	Enter E1 interface
router(config-if-serial0/0)#timeslots 1-31	Configure E1 timeslot 1-31
router(config-if-serial0/0)#ts16	Configure E1 operating mode ccs
router(config-if-serial0/0)#no crc4	Configure no crc4 of E1 interface.
router(config-if-serial0/0)#encapsulation ppp	Configure link layer protocol ppp
router(config-if-serial0/0)#ip address 1.1.1.1 255.0.0.0	Configure E1 interface ip address 1.1.1.1, mask 8.

Monitoring E1 Interface

After finishing the interface configuration, the user can enter the privileged user mode and execute the command show interface to display the parameter configuration and operation status of the E1 interface. Each parameter is the same as that of the serial interface.

When the interface information is examined, the massive error frames can be discovered from the E1 statistics information, the link-layer negotiation is slow, and there exists packet loss during the PING course.

After finishing the interface configuration, the user can enter the privileged user mode and execute the command show run interface to display the time-slots occupied by the E1 interface.

The E1 interface supports two kinds of connection cables: one is 75Ω non-balance coaxial cable, and the other is 120Ω balance twisted-pair cable. When a 120Ω equipment is connected, the impedance may be unmatched.

So the 75Ω cable is often used. When the E1 cable connects with other equipments, pay attention to whether parameters (such as CRC4, CCS/CAS, clock mode and time-slot) of the equipment match with those of the other equipments.

Configuring 8-port Synchronous Module

An 8s module is an 8-port high-speed synchronous serial-interface module. The 8S module can be used to avoid the non-synchronous rate between the serial-interface clock based on the bus clock and the factual clock of the V.35 interface.

The 8S module shares 32 time-slots with other TDM bus modules (expect the E1 module) can only operate in the synchronism mode and support 64K/128K. When an 8S module is inserted into Signamax router, eight interfaces sync0~sync7, which support PPP, X.25 and HDLC protocols, will be added.

The main contents of this section are listed as follows;

Configuring an 8S interface

Monitoring an 8s Interface

Configuring 8S Interface

The configuration tasks of an 8S interface are listed as follows:

Configuring the physical-layer operation parameters of an 8s interface

Configuring the link-layer operation parameters of an 8s interface

Configuring the physical-layer operation parameters of an 8s interface:

Router(config-if-sync0) ?

Command	Description
Router(config-if-sync0) # nrzi-encoding	Set the line-encoding mode of the interface as the NRZI-encoding (Non-Return-To-Zero-Inverted-encoding). The negation form of the command is used to cancel the NRZI-encoding.
Router(config-if-sync0) #no nrzi-encoding	Set the line encoding mode of the interface as NRZ-encoding (Non-Return-To-Zero) (the default mode is the NRZ-encoding.)
Router(config-if-sync0) # txphase/ rxphase	Set the transmitting/receiving phase of the interface as the rising edge or falling edge. txphase txup : representing that the channel sends data at the rising edge. txdown: representing that the channel sends data at the falling edge. rxphase rxup : representing that the channel receives data at the rising edge. rxdown: representing that the channel receives data at the falling edge.
Router(config-if-sync0) #clock rate <64000/128000>	Set the clock rate of the interface and configure a bit rate receivable for the interface processor. The negation form of the command is used to cancel the configuration.
Router(config-if-sync0) #clock <rx/tx> <in/out>	Set the receiving/transmitting clock of the interface as the interval/external clock.

The default configuration is: the NRZ-encoding mode, transmitting data at the falling edge and receiving data at the rising edge, adopting the interval clock as the clock source for transmitting/receiving data.

Configure the receiving/transmitting phase, which, generally, need be reconfigured.

NRZI is applied to the EIA/TIA-232 connection in the IBM environment.

When the clock frequency of the interface is configured, the effect of 0 is equal to that of the command no clock rate, which means that the interface occupies no time-slot of the TDM bus.

Configuring the link-layer operation parameters of an 8s interface

Router(config-if-serial0) ?

Command	Description
Router(config-if-sync0) # encapsulation < Configure encapsulation protocol>	Configure the protocol that is used on the link layer of the 8S interface.
Router(config-if-sync0) #ip address <unicast address> < network mask>	Configure the IP address and subnet mask of the 8S interface.

The link-layer protocol configured on the 8S interface can but be synchronous

The default link-layer protocol of the 8S interface is HDLC

The following example defines an 8S interface (for example interface sync0): the NRZ-encoding mode, sending data at the falling edge and receiving data at the rising edge, the clock frequency 128000, adopting the interval clock as the clock source for transmitting/receiving data, PPP link-layer protocol, IP address 1.1.1.1 and 8-bit mask.

Command	Description
router(config)#interface sync0	Enter the 8s interface sync0
router(config-if-sync0)#clock rate 128000	Set the clock rate of the interface as 128000
Router(config-if-sync0)# txphase txdown	Set that the data is transmitted at the falling edge of the interface
Router(config-if-sync0)# rxphase rxup	Set that the data is received at the rising edge of the interface
Router(config-if-sync0)# clock rx in	Set the receiving clock as the external clock
Router(config-if-sync0)# clock tx in	Set the transmitting clock as the external clock
Router(config-if-sync0)# encapsulation ppp	Set the link-layer protocol as PPP
Router(config-if-sync0)#ip address 1.1.1.1 255.0.0.0	Configure the E1 interface: the IP address—1.1.1.1, the mask—8-bit

By default: no clock rate is configured

If the clock source of multiple 8S interfaces is configured as an external clock and transmitting/receiving data depends on the external clock, the external equipment is required to provide the standard clock.

Monitoring 8s Interface

After finishing the interface configuration, the user can enter the privileged user mode and execute the command show interface sync0 to display the parameter configuration and operation status of the 8S interface.

After finishing the interface configuration, the user can enter the privileged user mode and execute the command show qmc timeslots to display the system TDM bus time-slots occupied by the 8S interface

After finishing the interface configuration, the user can enter the privileged user mode and execute the command show csm to display which interface supports the clock source of the system TDM bus.

The possible cause resulting in high bit-error rate of data transmission is that:

When an external clock is configured for the 8S interface, the peripheral equipment is required to provide a standard clock, or else, packets will be lost badly and bit error rate will be high.

Configuring Built-in Base-band Modem

Signamax router supports many kinds of built-in base-band modem module and the interface name is bm0/0. For an 8-port 128 built-in modem module, the interface name adopts the format of ebmx/y: x represents 4 or 5, and y represents 0~7; and each interface can operate either in the LT mode or in the NT mode.

ebm is the interface of MP2600 series router 8-port baseband modem module, BM is interface of MP3600 series routers baseband modem module

Configuring Single-port 128 Modem Module

Only the slot S0 on the low-end router can support a single-port 128 module.

Router(config) #

Command	Description
Router(config)#interface bm0/0	Enter the configuration mode of the interface bm0/0.
router(config-if-bm0/0)#line mode nt	Operate in the NT mode.
router(config-if-bm0/0)#enca hdlc	Encapsulate the HDLC protocol.
router(config-if-bm0/0)#ip address 2.2.2.2 255.0.0.0	The IP address of the port is 2.2.2.2 and related mask is 255.0.0.0.
router(config-if-bm0/0)#clock rate 64000	The clock rate is 64K.

The single-port 128 module supports the 64k/128k synchronous communication mode.

Configuring 8-port 128 Modem Module

An 8-port base-band modem module can be inserted in the upper or lower layer of the expended slot or both.

Supporting the link-layer protocols including HDLC, PPP, Frame Relay and X.25 etc.

Supporting the network-layer protocols such as IP and IPX;

The configuration tasks of the 8-port 128 modem module are listed as follows:

Configuring the baud rate

Configuring the line mode

Configuring the operation parameters of the link-layer protocols

Configuring the IP address

Configuring the clock of the synchronous interface:

Router(config) #

Command	Description
router(config)#interface ebm4/0	Configure the interface ebm4/0 of the 8-port base-band 128 modem module
router(config-if-ebm0)#clock rate 64000|128000	Configure the clock rate: 64Kbps/128kbps. (The default value is 64Kbps)
router(config-if-ebm0)#line mode lt|nt	Set the line mode: LT/NT(The default mode is NT)
router (config-if-ebm0)#ip address 1.1.1.1 255.0.0.0	The IP address of the port is 1.1.1.1, and related subnet mask is 255.0.0.0
router (config-if-ebm0)#enca ppp	Encapsulate the PPP protocol.
router(config)#interface ebm4/1	Configure the interface ebm4/1 of the built-in 128 module
router(config-if-ebm1)#line mode lt|nt	Same as above
router(config-if-ebm1)#enca ppp	Same as above
router(config-if-ebm1)#ip address 2.2.2.1 255.0.0.0	Same as above
router(config-if-ebm1)#clock rate 64000	Same as above

Eight interfaces can support nothing but the synchronism operation mode;

Because the base-band MODEM adopts two B channels and the line baud rate need be the integer times of B, namely the integer times of 64K, the baud rate can be configured only as 64K and 128K.;

For the base-band Modem on the other end, its configuration except the operation mode and address should be the same as that of the modem on this end.

If the DIP switch of the module is ON, then the bi-direction loop is enabled on the module.

When more than 2 ports of the 8-port 128 module operate in the NT mode, the data transmission clock source of the LT equipment connecting with the two ports should be consistent, like a MP9400 128 card in DDN network.

Configuring Built-in MODEM Module

Signamax router supports many kinds of built-in frequency-band MODEM modules, such as single-port 1M56/1M336 Modem module and four-port 4M336/4M56 Modem module. Each kind of interface can operate in the synchronic/asynchronic mode.

For these interfaces, their configuration mode is the same as that of the other serial interfaces, and the difference is that they support the leased line or dialup line mode, the clock mode in the synchronism mode (internal clock, external clock and slave clock).

The main contents of this section are listed as follows:

Configuring a built-in Modem;

Debugging a built-in Modem.

The configuration of a single-port MODEM module is the same as that of a multi-port one.

Router(config) #

Command	Description
Router(config)#interface serial0	Enter the configuration mode of the interface serial0
router(config-if-serial0)#physical-layer sync/async	Configure the synchronism/asynchronic operation mode
router(config-if-serial0)#enca ppp	Encapsulate the PPP protocol
router(config-if-serial0)#ip address 2.2.2.2 255.0.0.0	The IP address of the port is 2.2.2.2, and related mask is 255.0.0.0
router(config-if-serial0)#modem clock-rate 33600	Configure the Modem line rate in the synchronism modem
router(config-if-serial0)#speed 115200	Configure the Modem line rate in the asynchronic modem
router(config-if-serial0)#modem clock-mode external/internal/slave	Configure the Modem clock mode (the external clock, the internal clock and slave clock) in the synchronism modem
router(config-if)#modem party answer/originate	Configure the Modem answer/origination
router(config-if-serial0)#modem line leased	Configure the leased line mode for Modem
router(config-if-serial0)#dialer string 5148295	Configure the phone number for the Modem to dial up in the dialup mode
router(config-if-serial0)#modem enable/disable	Enable/disable the Modem configuration

The line rate and clock type need be configured in the synchronism mode. And in the dialup mode, a phone number of the answer party need be configured on the call origination;

When in the synchronism/asynchronic mode, the highest line rate is 33600bps/115200bps.

Both sides of modems need select consistent modulation protocol, line rate, synchronism/asynchronic mode, error control protocol and compression protocol in the asynchronic mode. And when in the synchronism mode, both sides need select the Modem synchronous clock.

Call/Answer configuration: the MODEM to originate the relation is called call origination, and the other party is called answer.

Built-in MODEM Debugging

Open the MODEM debugging switch and observe its dialup status and related information:

```
mp2600#debug modem interface-number
```

Close the MODEM debugging switch:

```
mp2600#no debug modem interface-number
```

The following example explains how to use the default system scripts to dial out:

```
signamax2#debug modem serial0
serial0: Config modem for dialing out
serial0: AT configuring command:
AAT&FE0Q0W1S95=44S36=5S25=0X0
AAT&D2&Q5
AATM1L1
serial0: Success to send the 0th group configuring command
serial0: Success to send the 1st group configuring command
serial0: success to configure modem
serial0: Start dialing automatically
serial0: Dialing timeout is set as 45s(DL-mode)
serial0: Dialing 81...

serial0: modem connected.
Line protocol on Interface serial0, changed state to up
```

Configuring ISDN Module

BRI Configuration

Syntax	Description
router(config-if-bri0/0)#isdn switch-type basic-net3	Configure the switch-type of an ISDN BRI interface.

Configuration example: interface U

Router A configuration:

Command	Description
RouterA(config)#dialer-list 1 protocol ip permit	Configure dialer rule 1, permitting all ip message passing.
RouterA(config)#interface bri 0/0	Enter interface mode
RouterA(config-if-bri0/0)#ip address 22.1.1.1 255.0.0.0	Configure interface ip address 22.1.1.1/8
RouterA(config-if-bri0/0)#dialer-group 1	Use dialer rule 1 to interface
RouterA(config-if-bri0/0)# encapsulation ppp	Encapsulation ppp
RouterA(config-if-bri0/0)# no ip route-cache	Disable interface high speed forwarding
RouterA(config-if-bri0/0)#dialer string 85248001	Configure dialer string 85248001
RouterA(config-if-bri0/0)# no ndsp enable	Disable ndsp protocol
RouterA(config-if-bri0/0)# isdn switch-type basic-net3	Configure isdn switch type basic-net3
RouterA(config-if-bri0/0)# isdn activate every-time	Activate D channel
RouterA(config-if-bri0/0)# no mpls route-cache	Disable mpls high speed forwarding

Router B configuration:

Command	Description
RouterB(config)#dialer-list 1 protocol ip permit	Configure dialer rule1, permitting all ip passing
RouterB(config)#interface bri 0/0	Enter interface mode
RouterB(config-if-bri0/0)#ip address 22.1.1.2 255.0.0.0	Configure interface ip address 22.1.1.2/8
RouterB(config-if-bri0/0)#dialer-group 1	Use dialer rule 1 to interface
RouterB(config-if-bri0/0)# encapsulation ppp	Encapsulation ppp
RouterB(config-if-bri0/0)# no ip route-cache	Disable interface high speed forwarding
RouterB(config-if-bri0/0)# no ndsp enable	Disable ndsp protocol
RouterB(config-if-bri0/0)# isdn switch-type basic-net3	Configure isdn switch type basic-net3
RouterB(config-if-bri0/0)# isdn activate every-time	Activate D channel
RouterB(config-if-bri0/0)# no mpls route-cache	Disable mpls high speed forwarding

Interface ST

PRI Configuration

PRI is configured as follows: (A CE1 module should be inserted in the router.)

Syntax	Description
router(config)#controller e1 0/0	Enter the E1 configuration mode via the controller location (0) that is defined with the unit number.
router(config-controller)#pri-group timeslot 1-31	Configure multiple time-slots to create a PRI interface. Only one pri-group can be configured for one CE1. However, as long as there exists no time-slot overlapping between pri-group and channel-group, both can be configured for one CE1.
router(config-controller)#exit	Exit from the E1 configuration mode.
router(config-if-serial0/0:15)#isdn switch-type primary-net5	Configure the switch-type of an ISDN PRI interface.

Configuring ATM Module

Overview

ATM (Asynchronous transfer Mode) is a transmission mode. In this mode, information is organized as cell. ATM is different from some packet switching network, because it provides the service connection-oriented.

ATM Configuration Command

ATM main configuration command is as following:

Command	Description	Configuration mode
pvc vpi/vci	*set up ATM PVC connection	config-if-XX
inarp minute	Configure ATM InARP timeout, only for IP network	config-if-XX-atm-vc
protocol ip A.B.C.D [broadcast] protocol ip inarp protocol ppp virtual-template number	*configure different server types on LLC/SNAP encapsulation, such as IP,InARP,PPP etc.	config-if-XX-atm-vc
encapsulation aal5mux ip A.B.C.D encapsulation aal5mux ppp virtual-template number encapsulation aal5mux frame-relay encapsulation aal5mux fr-atm-srv	* configure different server types on AAL5MUX encapsulation, such as IP,PPP, frame-relay, fr-atm-srv etc.	config-if-XX-atm-vc
encapsulation aal5snap	Encapsulate AAL5SNAP on PVC	config-if-XX-atm-vc
shutdown	Configure special PVC status as activation	config-if-XX-atm-vc
broadcast	Configure special PVC transmitting broadcast or multicast message	config-if-XX-atm-vc
atm framing {sdh | sonet}	Configure network frame mode, synchronous optical frame mode or synchronous digital frame mode	config-if-XX
loopback { local | remote | utopia }	Configure line loopback mode; local loopback or remote line loopback, and remote UTOPIA loopback.	config-if-XX
clock source { internal | line }	Configure clock suource (internal clock or line clock)	config-if-XX
disppvc slot-number vpi vci	Display special VC information	config-if-XX
clearpvc slot-number vpi vci	Delete special VC information	config-if-XX
bridge-group number	Enable bridging function on LLC/SNAP encapsulation protocol	config-if-XX-atm-vc

connect connection-name {vc-group group-name | fr-itnerface DLCI} atm-interface VPI/VCI {network-interworking | service-interworking}	*configure ATM-FR interconnection forwarding mode	config
clp-bit { 0 | 1| map-de }	Configure ATM interface CLP rule	config-atm-frf-XX
De-bit map-clp	Configure frame-relay data DE according to ATM CLP.	config-atm-frf-XX
efci-bit { 0| map-fecn }	Configure ATM EFCI rule	config-atm-frf-XX
service translation	Configure translation mode in FRF.8.	config-atm-frf-XX
cbr number	Configure CBR on special VC.	config-if-XX-atm-vc
ubr output-PCR	Configure UBR on special VC.	config-if-XX-atm-vc
vbr-rt output-PCR output-SCR {output-MBS}	Configure VBR-RT on special VC.	config-if-XX-atm-vc
vbr-nrt output-PCR output-SCR {output-MBS}	Configure VBR-NRT on special VC.	config-if-XX-atm-vc
oam-pvc manage [loop-detection | frequency]	Configure enabling OAM function on special VC.	config-if-XX-atm-vc
oam retry up-count down-count frquency	Configure OAM parameters on special PV	config-if-XX-atm-vc

"*" means the command has configuration example description.

configuration mode indicates: config, config-if-××(interface name) config-××(protocol name) etc.

Set Up PVC Configuration Command

pvc

```
pvc vpi/vci
```

Set up an ATM PVC connection. Delete NO format of special PVC.

Command	Description
Vpi	ATM virtual path id, its range is from 0 to 255. VPI and VCI cannot be 0 at the same time.
Vci	ATM virtual channel id, its range is from 0 to 1024, 0-30 is used for identifying special channel, and 32-1024 is used for identifying data channel.

(Default status) none
(Command mode) interface configuration mode

Set up PVC aal5-snap

InARP Timeout Configuration Command

inarp

```
inarp minute
configure ATM InARP timeout
```

Command	Description
Minutes	Configure inarp timeout

(Default status) none
(Command mode) ATM VC configuration mode

ATM InARP mechanism is only used for IP network.

PVC Encapsulation Configuration Command

protocol

```
protocol {ip {A.B.C.D [broadcast] | inarp} | ppp virtual-
template number}
```

Configure different service types on LLC/SNAP PVC; NO is used for disabling type service.

```
protocol ip A.B.C.D [broadcast]
protocol ppp virtual-template number
protocol ip inarp
```

Command	Description
ip	Transmit IP protocol
A.B.C.D	The interface IP address of peer ATM.
broadcast	This PVC supports broadcast and multicast receiving and acceptance.
inarp	Enable ATM InARP function
ppp	Transmit PPP
number	Virtual-template interface number

(Default status) none
(Command mode) ATM VC configuration mode

Each ATM PVC supports one kind of service.

encapsulation aal5mux

```
encapsulation aal5mux { ip A.B.C.D | ppp virtual-template
number | frame-relay | fr-atm-srv}
```

configure different service types on AAL5MUX PVC; NO is used for disabling the service.

```
encapsulation aal5mux ip A.B.C.D
encapsulation aal5mux ppp virtual-template number
encapsulation aal5mux frame-relay
encapsulation aal5mux fr-atm-srv
```

Command	Description
ip	Transmit IP protocol
A.B.C.D	IP address of peer ATM.
ppp	Transmit PPP
number	Virtual-template interface number
frame-relay	Enable ATM-FR network interconnection.
fr-atm-srv	Enable ATM-FR service interconnection.

(Default status) none
(Command mode) ATM VC configuration mode

ly, each ATM PVC supports one kind of service.
encapsulation aal5snap

```
encapsulation aal5snap
encapsulate AAL5SNAP on PVC.
```

(Default status) default
(Command mode) ATM VC configuration mode

ly, each ATM PVC supports one kind of service.

PVC Property Configuration Command

shutdown

```
shutdown
```

configure special PVC as shutdown status; NO is used for activating PVC.

(Default status) none
(command mode)ATM VC configuration mode

broadcast

```
broadcast
```

Configure transmitting broadcast or multicast packet on encapsulating AAL5MUX PVC; NO is used for disabling the packet.

(Default status) no configuration
(Command mode) ATM VC configuration mode

ATM Interface Configuration Command

atm framing

```
atm framing  [sdh | sonet]
```

configure network frame mode, default is sonnet frame mode.

Command	Description
sonet	Configure sonnet frame mode
sdh	Configure sdh frame mode

(Default status) sonnet frame mode
(Command mode)interface configuration mode

loopback

```
loopback [local | remote | utopia]
```

Configure line loopback mode; NO is used for disabling the loopback. Loopback mode: remote line loopback, local diagnosis loopback, and remote UTOPIA loopback. The default is remote line loopback.

Command	Description
local	Enable local diagnosis loopback.
remote	Enable remote line loopback.
utopia	Enable remote utopia loopback.

(Default status) disable
(Command mode) interface configuration mode

clock source

```
clock source [internal | line]
```

Configure clock source, in default status, ATM switch provides sending timing signal.

Command	Description
internal	Configure internal clock
line	Configure line clock

(Default status) configure line clock.
(Command mode) interface configuration mode

disppvc

```
disppvc slot-number vpi vci
show VC information.
```

Command	Description
slot-number	ATM slot number
Vpi	ATM vpi number
Vci	ATM vci number

(Default status) disable
(Command mode) interface configuration.

clearpvc

```
clearpvc slot-number vpi vci
delete special VC information.
```

Command	Description
slot-number	ATM slot number

Vpi	ATM vpi number
Vci	ATM vci number

(Default status) disable
(Command mode) interface configuration.

ATM Transparent Bridging Configuration Command

ATM bridging function only operates in AAL5-LLC/SNAP PVC. AAL5-MUX doesn't support bridging.

bridge-group

```
bridge-group number
```

Configure enabling bridge function on LLC/SNAP PVC; NO is used for disabling the function.

Command	Description
Number	Bridge group number

(Default status) disable
(Command mode) ATM VC configuration mode

ATM Interface Monitor & Maintenance Command

show atm map

The command is used for displaying ATM mapping information.

(Default status) none
(Command mode) privileged user mode

show atm vc

The command is used for displaying ATM VC configuration information.

(Default status) no
(Command mode) privileged user mode

show atm traffic

The command is used for displaying ATM flow statistics information.

(Default status) no
(Command mode) privileged user mode

debug atm error

The command is used for debugging ATM error information.

(Default status) no
(Command mode) privileged user mode

debug atm event

The command is used for debugging ATM event.

(Default status) no
(Command mode) privileged user mode

debug atm packet

The command is used for displaying ATM receiving and sending packet information.

(Default status) no
(Command mode) privileged user mode

ATM-FR Interconnection Configuration Command

connect

```
connect connection-name {vc-group group-name | fr-interface
DLCI} atm-interface VPI/VCI {network-interworking | service-
interworking}
```

Configure ATM-FR interconnection data forwarding mode; NO is used for disabling the configuration.

Command	Description
connection-number	ATM-FR interconnection name
group-name	Vc-group name
fr-interface	Configure frame-relay interface name
DLCI	Configure frame-relay DLCI (switched mode)
atm-interface	ATM interface name
VPI/VCI	ATM PVC number

(Default status) no
(Command mode) global configuration mode

ATM-FR interconnection has two modes: networking and service-interworking. The configuration refers to the example.

clp-bit

```
clp-bit { 0 | 1 | map-de }
```

Configure ATM CLP (Cell Lost Priority); NO is used for disabling the configuration.

Command	Description
0	Configure CLP=0
1	Configure CLP=1
map-de	Configure CLP according frame-relay DE position.

(Default status) no
(Command mode) FRF.5/FRF.8 configuration mode

de-bit

-

```
de-bit map-clp
```

Configure frame-relay DE according to ATM CLP; NO is used for canceling the configuration.

(Default status) no
(Command mode) FRF.5/FRF.8 configuration mode

shutdown

-

```
shutdown
```

Configure stop using the command in ATM-FR interconnection mode; NO is used for canceling the configuration.

(Default status) no
(Command mode) FRF.5/FRF.8 configuration mode

efci-bit

-

```
efci-bit { 0 | map-fecn }
```

configure ATM EFCI；NO is used for canceling the configuration.

Command	Description
0	Configure EFCI=0

map-fecn	Configure EFCI according to frame-relay FECN

(Default status) no
(Command mode) FRF.8 configuration mode.

service translation

- `service translation`

Configure FRF.8 translation mode; NO is used for canceling the configuration, using transparent mode.

(Default status) enable
(Command mode) FRF.8 configuration mode.

ATM QoS Parameter Configuration Command

cbr

- `cbr number`

Configure using CBR for flow control in special VC; NO is used for canceling the configuration.

Command	Description
Number	CBR flow(kbps)

(Default status) no
(Command mode) ATM VC configuration mode

ly, special VC supports one kind of QoS service. Delete the before configuration if you want to modify QoS service type.

ubr

`ubr output-PCR`

Configure using UBR service flow control on special VC; NO is used for canceling the configuration.

Command	Description
output-PCR	UBR flow(kbps)

(Default status) disable
(Command mode) ATM VC configuration mode

Special VC supports one kind of QoS service type. Delete the before configuration if you want to modify QoS service type.

vbr-rt

```
vbr-rt output-PCR output-SCR {output-MBS}
```

Configure using VBR-RT for flow control on special VC; NO is used or canceling the configuration.

Command	Description
output-PCR	VBR-rt output PCR flow (kbps)
output-SCR	VBR-rt output SCR (kbps)
output-MBS	VBR-rt output MBS (default is 95 signals.)

(Default status) no
(Command mode) ATM VC configuration mode

Special VC supports one kind of QoS service. Delete the before configuration if you want to modify QoS service type.

vbr-nrt

```
vbr-nrt output-PCR output-SCR {output-MBS}
```

configure using VBR-NRT service type for flow control on special VC; no is used for canceling the configuration.

Command	Description
output-PCR	VBR-nrt output PCR flow (kbps)
output-SCR	VBR-nrt output SCR (kbps)
output-MBS	VBR-nrt output MBS (use signal as unit)

(Default status) no
(Command mode) ATM VC configuration mode

Special VC supports one kind of QoS service. Delete the before configuration if you want to modify QoS service type.

ATM OAM Command

oam-pvc manage

```
oam-pvc manage [loop-detection | frequency]
```

Configure enabling OAM function on ATM PVC; no is used for canceling the configuration.

Command	Description
Loop-detection	Use OAM LB for checking whether PVC has loopback
frequency	When PVC changes to UP. OAM sends frequency (10s by default)

(Default status) no
(Command mode) ATM VC configuration mode

Special VC only sends OAM type based on F5 loopback signal, but it can receive and deal AIS/RDI signal OAM type.

oam retry

```
oam retry up-count down-count frequency
```

modify special PVC OAM parameters; no is used for renewing the default configuration.

Command	Description
up-count	PVC status changes to UP, OAM response number is 3 by default
down-count	PVC status changes to DOWN, OAM response number is 5 by default
Frequency	When PVC is DOWN, OAM sends frequency, 1s by default

(Default status) no
(Command mode) ATM VC configuration mode

show oam-pvc information

```
show oam-pvc information
```

Display system PVC OAM configuration information.

(Default status) no
(Command mode) privileged user mode

show oam-pvc statistics

`show oam-pvc statistics interface interface-name vpi/vci`

Display special interface, PVC statistics information.

Command	Description
Interface-name	Designate displaying interface
vpi/vci	Designate displaying PVC

(Default status) no
(Command mode) privileged user mode

ATM Configuration

The following is ATM application configuration example.

PVC AAL5MUX encapsulation configuration example

PVC LLC/SNAP encapsulation configuration example

PVCInARP configuration example

PVC transparent bridge example

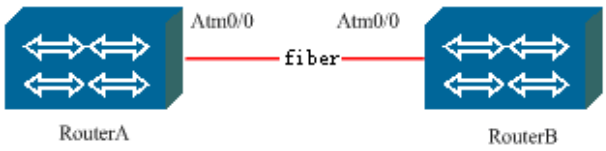
PVC PPPOA configuration example

PVC ATM-FR interconnection configuration example

PVC QoS configuration example

PVC OAM configuration example

PVC AAL5MUX Encapsulation Configuration Example



In the network, RouterA connects RouterB via ATM network; both sides use PVC for 1/32 communication. PVC use AAL5MUX encapsulation.

RouterA configuration:

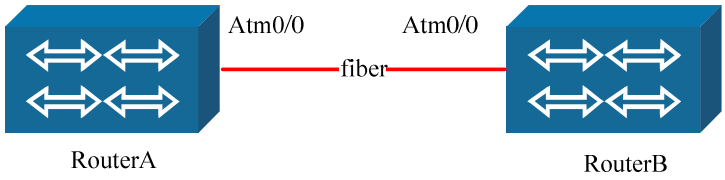
Command	Description
RouterA#configure terminal	Enter global configuration mode
RouterA (config)#interface atm0/0	Enter atm0/0
RouterA (config-if-atm0/0)#ip address 12.1.1.1 255.255.255.0	Configure IP address
RouterA (config-if-atm0/0)#pvc 1/32	Configure PVC 1/32
RouterA (config-if-atm0/0-atm-vc)#encapsulation aal5mux ip 12.1.1.2	Configure PVC encapsulation type and service type
RouterA (config-if-atm0/0-atm-vc)#exit	Exit to interface configuration mode
RouterA (config-if-atm0/0)# exit	Exit to privileged configuration mode

RouterB configuration:

Command	Description
RouterB#configure terminal	Enter global configuration mode
RouterB (config)#interface atm0/0	Enter atm0/0
RouterB (config-if-atm0/0)#ip address 12.1.1.2 255.255.255.0	Configure ip address
RouterB (config-if-atm0/0)#pvc 1/32	Configure PVC 1/32
RouterB (config-if-atm0/0-atm-vc)#encapsulation aal5mux ip 12.1.1.1	Configure PVC encapsulation type and service type
RouterB(config-if-atm0/0-atm-vc)#exit	Exit to interface configuration mode
RouterB (config-if-atm0/0)# exit	Exit to privileged configuration mode

If using back-to-back mode, configure clock on ATM interface, or it cannot transmit normally.

PVC LLC/SNAP Encapsulation Configuration Example



In the network, Router A connects Router B via ATM network; both sides use PVC for 1/32 communication. PVC use LLC/SNAP encapsulation.

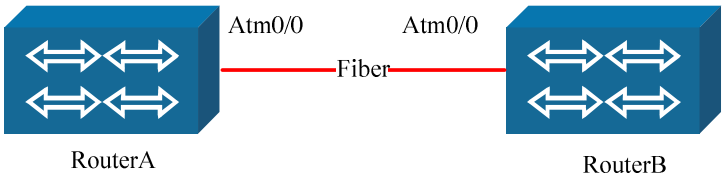
RouterA configuration:

Command	Description
RouterA#configure terminal	Enter global configuration mode
RouterA (config)#interface atm0/0	Enter atm0/0
RouterA (config-if-atm0/0)#ip address 12.1.1.1 255.255.255.0	Configure ip address
RouterA (config-if-atm0/0)#pvc 1/33	Configure PVC 1/33
RouterA (config-if-atm0/0-atm-vc)#protocol ip 12.1.1.2	Configure PVC encapsulation type and service type
RouterA (config-if-atm0/0-atm-vc)#exit	Exit to interface configuration mode
RouterA (config-if-atm0/0)# exit	Exit to privileged configuration mode

RouterB configuration:

Command	Description
RouterB#configure terminal	Enter global configuration mode
RouterB (config)#interface atm0/0	Enter atm0/0
RouterB (config-if-atm0/0)#ip address 12.1.1.2 255.255.255.0	Configure ip address
RouterB (config-if-atm0/0)#pvc 1/33	Configure PVC 1/33
RouterB (config-if-atm0/0-atm-vc)#protocol ip 12.1.1.1	Configure PVC encapsulation type and service type
RouterB(config-if-atm0/0-atm-vc)#exit	Exit to interface configuration mode
RouterB (config-if-atm0/0)# exit	Exit to privileged configuration mode

PVC InARP Configuration Example



In the network, Router A connects Router B via ATM network; both sides use PVC for 1/32 communication. PVC use LLC/SNAP encapsulation. Service type is inarp, and inarp timeout is 5 minutes.

RouterA configuration:

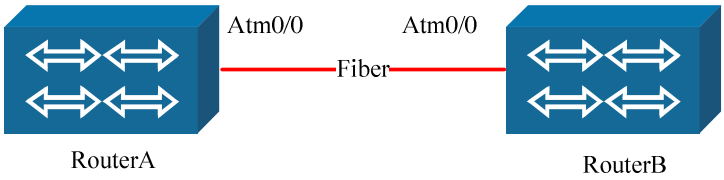
Command	Description
RouterA#configure terminal	Enter global configuration mode
RouterA (config)#interface atm0/0	Enter atm0/0
RouterA (config-if-atm0/0)#ip address 12.1.1.1 255.255.255.0	Configure ip address
RouterA (config-if-atm0/0)#pvc 1/33	Configure PVC 1/33
RouterA (config-if-atm0/0-atm-vc)#protocol ip inarp	Configure PVC encapsulation type and service type
RouterB (config-if-atm0/0-atm-vc)#inarp 5	Configure sending inarp information flow every 5 minutes
RouterA (config-if-atm0/0-atm-vc)#exit	Exit to interface configuration mode
RouterA (config-if-atm0/0)# exit	Exit to privileged configuration mode

RouterB configuration:

Command	Description
RouterB#configure terminal	Enter global configuration mode
RouterB (config)#interface atm0/0	Enter atm0/0
RouterB (config-if-atm0/0)#ip address 12.1.1.2 255.255.255.0	Configure ip address
RouterB (config-if-atm0/0)#pvc 1/33	Configure PVC 1/33
RouterB (config-if-atm0/0-atm-vc)#protocol ip inarp	Configure PVC encapsulation type and service type
RouterB (config-if-atm0/0-atm-vc)#inarp 5	Configure sending inarp information flow every 5 minutes
RouterB(config-if-atm0/0-atm-vc)#exit	Exit to interface configuration mode
RouterB (config-if-atm0/0)# exit	Exit to privileged configuration

	mode

PVC Transparent Bridge Configuration Example



In the network, Router A connects Router B via ATM network; both sides use PVC for 1/32 communication. PVC use LLC/SNAP encapsulation. Service type is transparent bridge.

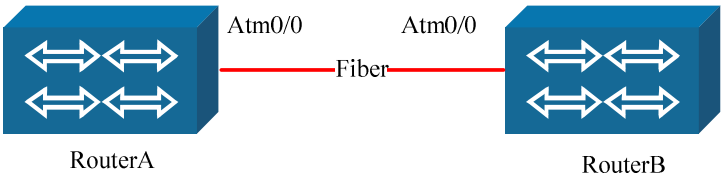
RouterA configuration:

Command	Description
RouterA#configure terminal	Enter global configuration mode
RouterA (config)#interface atm0/0	Enter atm0/0
RouterA (config-if-atm0/0)#pvc 1/33	Configure PVC 1/33
RouterA (config-if-atm0/0-atm-vc)#bridge-group 1	Configure PVC encapsulation type and service type
RouterA(config-if-atm0/0-atm-vc)#exit	Exit to interface configuration mode
RouterA (config-if-atm0/0)#exit	Exit to privileged configuration mode
RouterA (config)#intface fastethernet0	Enter fastethernet0
RouterA (config-if-fastethernet0)#bridge-group 1	Configure bridge group1
RouterA (config-if-fastethernet0)#exit	Exit to privileged configuration mode

RouterB configuration:

Command	Description
RouterB#configure terminal	Enter global configuration mode
RouterB (config)#interface atm0/0	Enter atm0/0
RouterB (config-if-atm0/0)#pvc 1/33	Configure PVC 1/33
RouterB (config-if-atm0/0-atm-vc)#bridge-group 1	Bridge group 1. 1
RouterB(config-if-atm0/0-atm-vc)#exit	Exit to interface configuration mode
RouterB(config-if-atm0/0)#exit	Exit to privileged configuration mode
RouterB(config)#intface fastethernet0	Enter fastethernet0
RouterB(config-if-fastethernet0)#bridge-group 1	Configure bridge group1
RouterB(config-if-fastethernet0)#exit	Exit to privileged configuration mode

PVC PPPoA Configuration Example



In the network, Router A connects Router B via ATM network; both sides use PVC for 1/32 communication. PVC use LLC/SNAP encapsulation, service type is PPPoA.

RouterA configuration:

Command	Description
RouterA#configure terminal	Enter global configuration mode
RouterA (config)#interface fastethernet0	Enter fastethernet0
RouterA (config-if-fastethernet0)#ip address 192.168.0.1 255.255. 255.0	Configure ip address
RouterA (config-if-fastethernet0)#exit	Exit to privileged configuration mode
RouterA (config)#interface virtual-template 1	Enter virtual-template1
RouterA (config-if-virtual-template1)#encapsulation ppp	Encapsulate PPP
RouterA (config-if-virtual-template1)#ip unnumber fastethernet0	Use Ethernet interface address
RouterA (config-if-virtual-template1)#exit	Exit to privileged configuration mode
RouterA (config)#interface atm0/0	Enter atm0/0
RouterA (config-if-atm0/0)#pvc 1/33	Configure PVC 1/33
RouterA (config-if-atm0/0-atm-vc)#protocol ppp virtual-template1	Configure PVC encapsulation type and service type
RouterA(config-if-atm0/0-atm-vc)#exit	Exit to interface configuration mode
RouterA (config-if-atm0/0)#exit	Exit to privileged configuration mode

RouterB configuration:

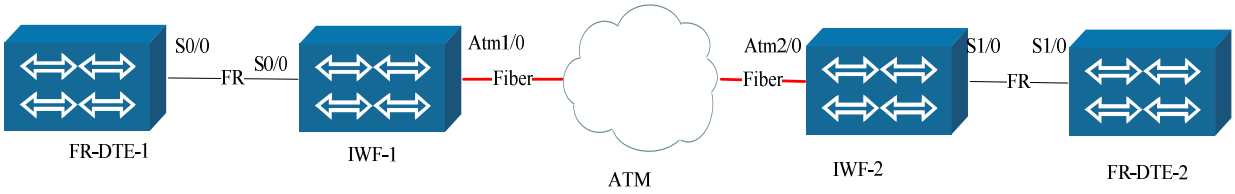
Command	Description
RouterB#configure terminal	Enter global configuration mode
RouterB(config)#interface fastethernet0	Enter fastethernet0
RouterB (config-if-fastethernet0)#ip address 192.168.0.2.255.255. 255.0	Configure ip address
RouterB (config-if-fastethernet0)#exit	Exit to privileged configuration mode
RouterB (config)#interface virtual-template 1	Enter virtual-template1
RouterB (config-if-virtual-template1)#encapsulation ppp	Encapsulate PPP
RouterB (config-if-virtual-template1)#ip unnumber fastethernet0	Use Ethernet interface address
RouterB (config-if-virtual-template1)#exit	Exit to privileged configuration Mode
RouterB(config)#interface atm0/0	Enter atm0/0
RouterB (config-if-atm0/0)#pvc 1/33	Configure PVC 1/33
RouterB (config-if-atm0/0-atm-vc)#protocol ppp virtual-template1	Configure PVC encapsulation type and service type
RouterB (config-if-atm0/0-atm-vc)#exit	Exit to interface configuration mode
RouterB(config-if-atm0/0)#exit	Exit to privileged configuration mode

PPP configuration information refers to WAN protocol configuration manual.

LLC/SNAP encapsulation PPPoA uses command protocol ppp virtualtemplate1

AAL5MUX encapsulation PPPoA uses command encapsulation aal5mux ppp virtual-template1

PVC ATM-FR Interconnection Configuration Example



IWF-1 connects IWF-2 via ATM network. Both sides use PVC for 1/33 communication.

PVC use AAL5MUX encapsulation, and service type is frame-relay. FR-DTE-1 connects IWF-1 via serial0/0, configure DLCI as 111, FR-DTE-2 connects IWF-2 via serial1/0, and configure DLCI as 222.

FR-DTE-1 configuration:

Command	Description
FR-DTE-1#configure terminal	Enter global configuration mode
FR-DTE-1 (config)#interface serial0/0	Enter serial0/0
FR-DTE-1 (config-if-serial0/0)#encapsulation frame-relay	Encapsulate frame-relay
FR-DTE-1 (config-if-serial0/0)#physical-layer sync	Configure synchronous mode
FR-DTE-1 (config-if-serial0/0)#frame-relay lmi-type ansi	Configure LMI type
FR-DTE-1 (config-if-serial0/0)# frame-relay interface-dlci 111	Configure DLCI 111
FR-DTE-1 (config-fr-dlci)#exit	Exit to interface configuration mode
FR-DTE-1 (config-if-serial0/0)# ip address 66.6.6.6 255.0.0.0	Configure interface IP address
FR-DTE-1 (config-if-serial0/0)#exit	Exit to privileged configuration mode.

IWF-1 configuration:

Command	Description
IWF-1#configure terminal	Enter global configuration mode
IWF-1 (config)#frame-relay switch	Enable frame-relay switch function.
IWF-1 (config)#interface serial0/0	Enter serial0/0
IWF-1 (config-if-serial0/0)#encapsulation frame-relay	Encapsulate frame-relay
IWF-1 (config-if-serial0/0)#physical-layer sync	Configure synchronous mode
IWF-1 (config-if-serial0/0)#clock rate 2000000	Configure clock 2M
IWF-1 (config-if-serial0/0)# frame-relay intf-type dce	Configure FR interface DCE
IWF-1 (config-if-serial0/0)# frame-relay interface-dlci 111 switched	Configure DLCI 111 switched (for ATM-FR interconnection)
IWF-1 (config-fr-dlci)#exit	Exit to interface configuration mode
IWF-1 (config-if-serial0/0)#exit	Exit to privileged configuration mode
IWF-1 (config)#interface atm1/0	Enter atm1/0
IWF-1 (config-if-atm1/0)#pvc 1/33	Configure PVC 1/33
IWF-1 (config-if-atm1/0-atm-vc)#encapsulation aal5mux frame-relay	Configure ATM-FR interconnection service
IWF-1 (config-if- atm1/0-atm-vc)#exit	Exit to interface configuration mode
IWF-1 (config-if-atm1/0)#exit	Exit to privileged configuration mode
IWF-1 (config)#connect atm-fr serial0/0 111 atm1/0 1/33 network-interworking	Switch ATM PVC 1/33 data to serial0/0 DLCI=111
IWF-1 (config-frf5)#exit	Exit to privileged configuration mode

IWF-2 configuration:

Command	Description
IWF-2#configure terminal	Enter global configuration mode
IWF-2 (config)#frame-relay switch	Enable frame-relay switch function.
IWF-2 (config)#interface serial1/0	Enter serial1/0
IWF-2 (config-if-serial1/0)#encapsulation frame-relay	Encapsulate frame-relay
IWF-2 (config-if-serial1/0)#physical-layer sync	Configure synchronous mode
IWF-2 (config-if-serial1/0)#clock rate 2000000	Configure clock 2M
IWF-2 (config-if-serial1/0)# frame-relay intf-type dce	Configure FR interface DCE
IWF-2 (config-if-serial1/0)# frame-relay interface-dlci 222 switched	Configure DLCI 222 switched (for ATM-FR interconnection)
IWF-2 (config-fr-dlci)#exit	Exit to interface configuration mode
IWF-2 (config-if-serial1/0)#exit	Exit to privileged configuration mode
IWF-2 (config)#interface atm2/0	Enter atm2/0
IWF-2 (config-if-atm2/0)#pvc 1/33	Configure PVC 1/33
IWF-2 (config-if-atm2/0-atm-vc)#encapsulation aal5mux frame-relay	Configure ATM-FR interconnection service
IWF-2 (config-if- atm2/0-atm-vc)#exit	Exit to interface configuration mode
IWF-2 (config-if-atm2/0)#exit	Exit to privileged configuration mode
IWF-2 (config)# connect atm-fr serial1/0 222 atm2/0 1/33 network-interworking	Switch ATM PVC 1/33 data to serial1/0 DLCI=222
IWF-2 (config -frf5)#exit	Exit to privileged configuration mode

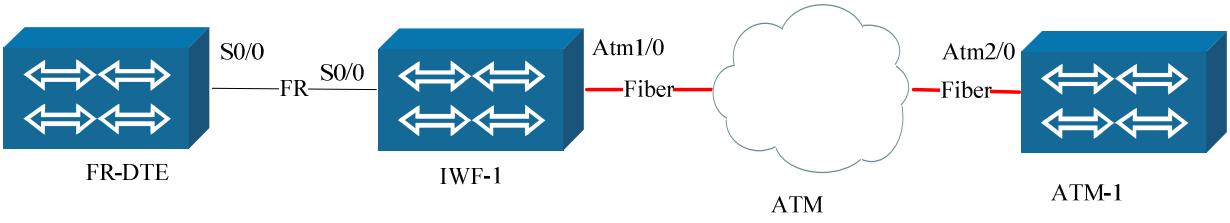
FR-DTE-2 configuration:

Command	Description
FR-DTE-1#configure terminal	Enter global configuration mode
FR-DTE-1 (config)#interface serial1/0	Enter serial1/0
FR-DTE-1 (config-if-serial1/0)#encapsulation frame-relay	Encapsulate frame-relay
FR-DTE-1 (config-if-serial1/0)#physical-layer sync	Configure synchronous mode
FR-DTE-1 (config-if-serial1/0)#frame-relay lmi-type ansi	Configure LMI type
FR-DTE-1 (config-if-serial1/0)# frame-relay interface-dlci 222	Configure DLCI 222
FR-DTE-1 (config-fr-dlci)#exit	Exit to interface configuration mode
FR-DTE-1 (config-if-serial1/0)# ip address 66.6.6.7 255.0.0.0	Configure interface IP address
FR-DTE-1 (config-if-serial1/0)#exit	Exit to privileged configuration mode

This configuration is only ATM-FR interconnection FRF.5 configuration mode1.

For the application of FRF.5 mode 2, the configuration of FR-DTE-1 and IWF-1 equipment will not be modified only IWF-2 and FR-DTE-2 are binding to a frame-relay ATM equipment. And the configuration is different.

MP network equipment cannot be used as frame-relay ATM equipment.



IWF-1 connects ATM-1 via ATM network; both sides use PVC for 1/33 communication. PVC uses AAL5MUX encapsulation, and the service type is fr-atm-srv, transparent mode. FR-DTE-1 connects IWF-1 via serial0/0, and configure DLCI 111.

FR-DTE-1 configuration:

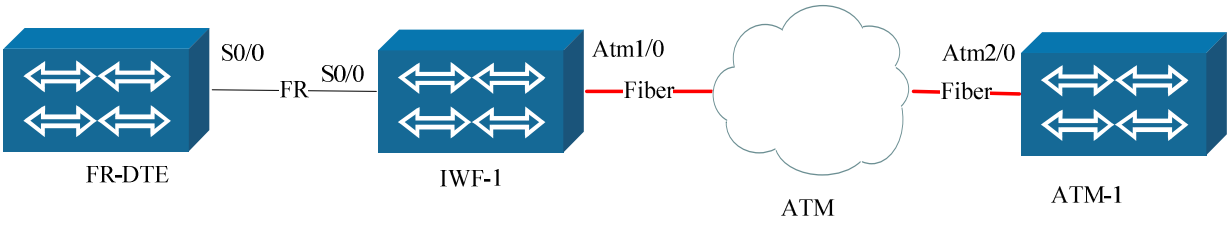
Command	Description
FR-DTE-1#configure terminal	Enter global configuration mode
FR-DTE-1 (config)#interface serial0/0	Enter serial0/0
FR-DTE-1 (config-if-serial0/0)#encapsulation frame-relay	Encapsulate frame-relay
FR-DTE-1 (config-if-serial0/0)#physical-layer sync	Configure synchronous mode
FR-DTE-1 (config-if-serial0/0)#frame-relay lmi-type ansi	Configure LMI type
FR-DTE-1 (config-if-serial0/0)# frame-relay interface-dlci 111	Configure DLCI 111
FR-DTE-1 (config-fr-dlci)#exit	Exit to interface configuration mode
FR-DTE-1 (config-if-serial0/0)#frame-relay map ip 66.6.6.7 111 Broadcast	Configure MAP
FR-DTE-1 (config-if-serial0/0)# ip address 66.6.6.6 255.0.0.0	Configure interface IP address
FR-DTE-1 (config-if-serial0/0)#exit	Exit to privileged configuration mode

IWF-1 configuration:

Command	Description
IWF-1#configure terminal	Enter global configuration mode
IWF-1 (config)#frame-relay switch	Enable frame-relay switch function.
IWF-1 (config)#interface serial0/0	Enter serial0/0
IWF-1 (config-if-serial0/0)#encapsulation frame-relay	Encapsulate frame-relay
IWF-1 (config-if-serial0/0)#physical-layer sync	Configure synchronous mode
IWF-1 (config-if-serial0/0)#clock rate 2000000	Configure clock 2M
IWF-1 (config-if-serial0/0)# frame-relay intf-type dce	Configure FR interface DCE
IWF-1 (config-if-serial0/0)# frame-relay interface-dlci 111 switched	Configure DLCI 111 switched (for ATM-FR interconnection)
IWF-1 (config-fr-dlci)#exit	Exit to interface configuration mode
IWF-1 (config-if-serial0/0)#exit	Exit to privileged configuration mod
IWF-1 (config)#interface atm1/0	Enter atm1/0
IWF-1 (config-if-atm1/0)#pvc 1/33	Configure PVC 1/33
IWF-1 (config-if-atm1/0-atm-vc)#encapsulation aal5mux fr-atm-srv	Configure ATM-FR service interconnection
IWF-1 (config-if- atm1/0-atm-vc)#exit	Exit to interface configuration mode
IWF-1 (config-if-atm1/0)#exit	Exit to privileged configuration mode
IWF-1 (config)#connect atm-fr serial0/0 111 atm1/0 1/33 service-interworking	Switch ATM PVC 1/33 data to serial0/0 DLCI=111
IWF-1 (config-frf8)#no service translation	Enable FRF.8 transparent mode
IWF-1 (config-frf8)#exit	Exit to privileged configuration mode

ATM-1 configuration:

Command	Description
ATM-1#configure terminal	Enter global configuration mode
ATM-1 (config)#interface atm2/0	Enter atm2/0
ATM-1 (config-if-atm2/0)#pvc 1/33	Configure PVC 1/33
ATM-1 (config-if-atm2/0-atm-vc)# encapsulation aal5mux ip 66.6.6.6	Configure AAL5MUX encapsulation IP mapping
ATM-1 (config-if- atm2/0-atm-vc)#exit	Exit to interface configuration mode
ATM-1 (config-if-atm2/0)#ip address 66.6.6.7 255.0.0.0	Configure interface IP address
ATM-1 (config-if-atm2/0)#exit	Exit to privileged configuration mode



IWF-1 connects ATM-1 via ATM network; both sides use PVC for 1/33 communication. PVC uses AAL5MUX encapsulation, and the service type is fr-atm-srv, translation mode. FR-DTE-1 connects IWF-1 via serial0/0, and configures DLCI 111.

FR-DTE-1 configuration:

Command	Description
FR-DTE-1#configure terminal	Enter global configuration mode
FR-DTE-1 (config)#interface serial0/0	Enter serial0/0
FR-DTE-1 (config-if-serial0/0)#encapsulation frame-relay	Encapsulate frame-relay
FR-DTE-1 (config-if-serial0/0)#physical-layer sync	Configure synchronous mode
FR-DTE-1 (config-if-serial0/0)#frame-relay lmi-type ansi	Configure LMI
FR-DTE-1 (config-if-serial0/0)# frame-relay interface-dlci 111	Configure DLCI 111
FR-DTE-1 (config-fr-dlci)#exit	Exit to interface configuration mode
FR-DTE-1 (config-if-serial0/0)#frame-relay map ip 66.6.6.7 111	Configure MAP
FR-DTE-1 (config-if-serial0/0)# ip address 66.6.6.6 255.0.0.0	Configure interface IP address

FR-DTE-1 (config-if-serial0/0)#exit	Exit to privileged configuration mode

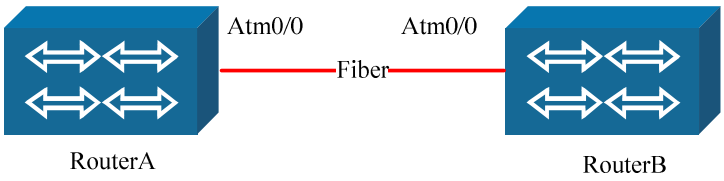
IWF-1 configuration:

Command	Description
IWF-1#configure terminal	Enter global configuration mode
IWF-1 (config)#frame-relay switch	Enable frame-relay switch
IWF-1 (config)#interface serial0/0	Enter serial0/0
IWF-1 (config-if-serial0/0)#encapsulation frame-relay	Encapsulate frame-relay
IWF-1 (config-if-serial0/0)#physical-layer sync	Configure synchronous mode
IWF-1 (config-if-serial0/0)#clock rate 2000000	Configure clock 2M
IWF-1 (config-if-serial0/0)# frame-relay intf-type dce	Configure FR interface DCE
IWF-1 (config-if-serial0/0)# frame-relay interface-dlci 111 switched	Configure DLCI 111 switched (for ATM-FR interconnection)
IWF-1 (config-fr-dlci)#exit	Exit to interface configuration mode
IWF-1 (config-if-serial0/0)#exit	Exit to privileged configuration mode
IWF-1 (config)#interface atm1/0	Enter atm1/0
IWF-1 (config-if-atm1/0)#pvc 1/33	Configure PVC 1/33
IWF-1 (config-if-atm1/0-atm-vc)#encapsulation aal5mux fr-atm-srv	Configure ATM-FR service interconnection
IWF-1 (config-if- atm1/0-atm-vc)#exit	Exit to interface configuration mode
IWF-1 (config-if-atm1/0)#exit	Exit to privileged configuration mode
IWF-1 (config)#connect atm-fr serial0/0 111 atm1/0 1/33 service-interworking	Switch ATM PVC 1/33 data to serial0/0 DLCI=111
IWF-1 (config-frf8)#service translation	Enable FRF.8 translation mode (By default)
IWF-1 (config-frf8)#exit	Exit to privileged configuration mode

ATM-1 configuration:

Command	Description
ATM-1#configure terminal	Enter global configuration mode
ATM-1 (config)#interface atm2/0	Enter atm2/0
ATM-1 (config-if-atm2/0)#pvc 1/33	Configure PVC 1/33
ATM-1 (config-if-atm2/0-atm-vc)#protocol ip 66.6.6.6	Configure LLC/SNAP encapsulation IP mapping
ATM-1 (config-if- atm2/0-atm-vc)#exit	Exit to interface configuration mode
ATM-1 (config-if-atm2/0)#ip address 66.6.6.7 255.0.0.0	Configure interface IP address
ATM-1 (config-if-atm2/0)#exit	Exit to privileged configuration mode

PVC QoS Configuration Example



RouterA connects RouterB via ATM network; and both sides use PVC for 1/33 communication. PVC uses LLC/SNAP encapsulation, and the service type is IPOA.

RouterA configuration:

Command	Description
RouterA#configure terminal	Enter global configuration mode
RouterA (config)#interface atm0/0	Enter atm0/0
RouterA (config-if-atm0/0)#pvc 1/33	Configure PVC 1/33
RouterA (config-if-atm0/0-atm-vc)#protocol ip 12.1.1.1	Configure MAP
RouterA (config-if-atm0/0-atm-vc)#cbr 2000	Configure CBR 2M
RouterA(config-if-atm0/0-atm-vc)#exit	Exit to interface configuration mode
RouterA(config-if-atm0/0)#ip address 12.1.1.2 255.0.0.0	Configure interface IP address
RouterA (config-if-atm0/0)#exit	Exit to privileged configuration mode

RouterB configuration:

Command	Description
RouterB#configure terminal	Enter global configuration mode
RouterB (config)#interface atm0/0	Enter atm0/0
RouterB (config-if-atm0/0)#pvc 1/33	Configure PVC 1/33
RouterB (config-if-atm0/0-atm-vc)#protocol ip 12.1.1.2	Configure MAP
RouterB (config-if-atm0/0-atm-vc)#cbr 2000	Configure CBR 2M
RouterB(config-if-atm0/0-atm-vc)#exit	Exit to interface configuration mode
RouterB(config-if-atm0/0)#ip address 12.1.1.1 255.0.0.0	Configure interface IP address
RouterB(config-if-atm0/0)#exit	Exit to privileged configuration mode

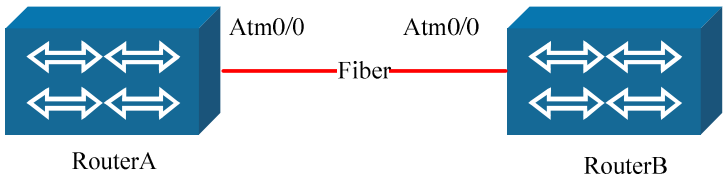
ATM other QoS service type configuration is similar with CBR configuration.

Confirm PVC has configured service type before QoS service type configuration.

Delete QoS parameters before configuring new QoS service type.

If using back-to-back mode, configure clock on ATM, or it cannot transmit normally.

PVC OAM Configuration Example



RouterA connects RouterB via ATM network; and both sides use PVC for 1/33 communication. PVC uses LLC/SNAP encapsulation, and the service type is IPOA.

RouterA configuration:

Command	Description
RouterA#configure terminal	Enter global configuration mode
RouterA (config)#interface atm0/0	Enter atm0/0
RouterA (config-if-atm0/0)#pvc 1/33	Configure PVC 1/33
RouterA (config-if-atm0/0-atm-vc)#protocol ip 12.1.1.1	Configure MAP
RouterA (config-if-atm0/0-atm-vc)#oam-pvc manage	Enable OAM management
RouterA(config-if-atm0/0-atm-vc)#exit	Exit to interface configuration mode
RouterA(config-if-atm0/0)#ip address 12.1.1.2 255.0.0.0	Configure interface IP address
RouterA (config-if-atm0/0)#exit	Exit to privileged configuration mode

RouterB configuration:

Command	Description
RouterB#configure terminal	Enter global configuration mode
RouterB (config)#interface atm0/0	Enter atm0/0
RouterB (config-if-atm0/0)#pvc 1/33	Configure PVC 1/33
RouterB (config-if-atm0/0-atm-vc)#protocol ip 12.1.1.2	Configure MAP
RouterB (config-if-atm0/0-atm-vc)#oam-pvc manage	Enable OAM management
RouterB(config-if-atm0/0-atm-vc)#exit	Exit to interface configuration mode
RouterB(config-if-atm0/0)#ip address 12.1.1.1 255.0.0.0	Configure interface IP address
RouterB(config-if-atm0/0)#exit	Exit to privileged configuration mode

Confirm that PVC has configured service type before OAM configuration.

If using back-to-back mode, configure clock on ATM, or it cannot transmit normally.

POS Module Configuration

POS card type is R0181POS, and it can be used on 3700 and 7200 platform, which provides 1-port POS interface. The basic feature is as following:

Interface number: 1-port;
Rate: 155.520Mbit/S；
Physical interface: 155M 的 STM-1 的 SDH(SONET) optical interface;
Physical frame format: STM-1(SDH), OC-3(SONET)
Hot swappable: supporting;
Supported protocol: PPP, HDLC
MTU: 1500 bytes.

Basic Configuration Commands

Basic configuration command provides interface basic parameter configuration command in interface mode. Pos interface supported protocol is PPP and HDLC, the default is PPP, and the interface type is serial type.

The configuration about protocol and serial is the same as original, here only gives the new added pos configuration command.

POS main configuration command is as following:

Command	Description	Configuration mode
clock source { internal | line}	*send clock configuration	config-if-XX
crc {32 | 16 | none}	Data frame crc check mode	config-if-XX
pos delay trigger line {<CR> | time} pos delay trigger path {<CR> | time}	Line time delay configuration	config-if-XX
pos flag c2 {<CR> | value} pos flag j0 {<CR> | value} pos flag s0s1 {value}	Line flag configuration	config-if-XX
pos scramble-atm	Enable scramble-atm	config-if-XX
loopback {local | remote}	Line loopback (for testing)	config-if-XX
pos report {<CR> | slof | slos | lais | pais | prdi | sd-ber | sf-ber}	Alarming configuration	config-if-XX
pos threshold sd-ber {<CR> | number} pos threshold sf-ber {<CR> |	Alarming threshold configuration	config-if-XX

number}		

"*" means the command has configuration example description.

Configuration mode is executing the configuration command mode, for example, config, config-if-××(interface name) config-××(protocol name).

Clock Configuration Command Clock Source

Pos sending port has 2 modes:

Internal clock: produced by pulsator.
External clock: the clock from the line of receiving port.

Command	Description
router(config-if-pos0/0)# clock source internal	Configure internal clock mode
router(config-if-pos0/0)# clock source line	Configure external clock mode

External clock by default.

CRC Check Mode

POS supported protocol is PPP and HDLC, CRC checks the data frame. The command is used for configuring CRC check mode.

Command	Description
router(config-if-pos0/0)#crc 32	Configure CRC-32(4Byte) mode
router(config-if-pos0/0)# crc 16	Configure CRC-32 (4Byte) mode
router(config-if-pos0/0)# crc none	No crc check

CRC-32(4Byte) check mode by default.

pos delay trigger

Interface status is confirmed by line status, the change of interface status is triggered by line status event, and the default event is: LOS, LOF and LAIS. When there is no event, the line connection is normal, DCD signal is UP, when there is event, DCD is DOWN.

The event divides into two kinds:

Line event: LOS, LOF, LAIS
Channel event: PAIS, PRDI, PLOP, SD, SF

Configure the interface response to event via configuration command, and add some responses to other events.

Command	Description
router(config-if-pos0/0)# pos delay triggers line	Configure line trigger event (default time is 0)
router(config-if-pos0/0)# pos delay triggers line time	Configure line trigger event and time
router(config-if-pos0/0)# pos delay triggers path	Configure path trigger event (50ms by default)
router(config-if-pos0/0)# pos delay triggers path time	Configure path trigger event and time
router(config-if-pos0/0)# no delay triggers line	Cancel line trigger event
router(config-if-pos0/0)# no delay triggers path	Cancel path trigger event

In default status, the change of interface status is triggered by line status event, the default trigger

Event is: LOS, LOF and LAIS. When there is event, the interface status is down. Via the command:
pos delay triggers line [time]
configure interface response to line event time delay, and the range is 50~10000, unit is ms.
no delay triggers line
cancel line event time delay.

The event can also be triggered by channel status event, including: PAIS, PRDI, PLOP, SD and SF. The minimum time delay is 50ms.

pos delay triggers path [time]

add channel event to trigger the interface status, time designates response time delay, the range is
50~10000, unit is ms, default is 50ms.

no pos delay triggers path
cancel interface status response to channel event.

Configure line pos flag

In SDH, each lay has different flags for showing different kinds of information. In pos port, use command pos flag for configuration.

Command	Description
router(config-if-pos0/0)#pos flag c2 value	Define C2 value
router(config-if-pos0/0)#no pos flag c2	Use default c2 configuration
router(config-if-pos0/0)#pos flag j0 value	Define j0 value
router(config-if-pos0/0)#no pos flag j0	Use default j0 configuration
router(config-if-pos0/0)#pos flag S0S1 value	Define ss value(0~2)
router(config-if-pos0/0)#no pos flag S0S1	Use default ss configuration

C2 default rule is as following:

```
HDLC encapsulation 0xCF
Payload scramble PPP encapsulation 0x16(RFC2615)
No encapsulation of PPP 0xCF(RFC2615)
If configure c2 byte via pos flag, adopt user configured c2
byte.
J0 default transmitting mode is single byte mode; configure
j0 content via pos flag j0.
The default is 0. and the transmission mode can be configured
via extended command.
S0S1 default rule:
If SONET, it is 0
If SDH, it is 2
The use can define ss via pos flag s0s1.
```

enable payload scramble-atm

In order to pick up clock of receiving end, SDH will do X7＋X6＋1scramble in stm-1 frame.

Command	Description
router(config-if-pos0/0)# pos scramble-atm	Enable payload scramble-atm
router(config-if-pos0/0)#no pos scramble-atm	Disable payload scramble-atm.

The rule is as following:
PPP: enable
HDLC: disable

loop back

Configure loopback for testing.

Command	Description

router(config-if-pos0/0)# loopback local	Configure local loopback
router(config-if-pos0/0)# loopback remote	Configure line loopback
router(config-if-pos0/0)#no loopback	Cancel loopback configuration (By default)

Alarming Command Report

Configure whether report alarming signals on console, (not display by default)

Command	Description
router(config-if-pos0/0)# pos report slof	Enable lof alarming
router(config-if-pos0/0)# pos report slos	Enable os alarming
router(config-if-pos0/0)# pos report lais	Enable lais alarming
router(config-if-pos0/0)# pos report pais	Enable pais alarming
router(config-if-pos0/0)# pos report prdi	Enable prdi alarming
router(config-if-pos0/0)# pos report sd-ber	Enable sdv
router(config-if-pos0/0)# pos report sf-ber	Enable sf alarming
router(config-if-pos0/0)#no pos report slof	Disable lof alarming
router(config-if-pos0/0)# no pos report slos	Disable los alarming
router(config-if-pos0/0)# no pos report lais	Disable lais alarming
router(config-if-pos0/0)# no pos report pais	Disable pais alarming
router(config-if-pos0/0)# no pos report prdi	Disable prdi alarming
router(config-if-pos0/0)# no pos report sd-ber	Disable sd alarming
router(config-if-pos0/0)# no pos report sf-ber	Disable sf alarming
router(config-if-pos0/0)#pos report	Report all alarming
router(config-if-pos0/0)# no pos report sf-ber	Disable all alarming

Configure Alarming Threshold

Configure line error code alarming threshold.

Command	Description
router(config-if-pos0/0)# pos threshold sd-ber threshold	Configure signal inferior threshold, and the configuration range is 3~9 (10-3~10-9), default is 10－6
router(config-if-pos0/0)# pos threshold sf-ber threshold	Configure signal disfigurement threshold, and the range is 3~~9 (10-3~10-9), default is 10－3

Extended Configuration Command

Extended command comprises some added parameter configuration commands and interface diagnosis commands. Extended command should be configured after entering cont mode via controller pos [slot/port]

Command	Description	Configuration mode
pos frame {sonet | sdh}	Line frame type	config-controller-XX
overhead j0 length {16/64 | 1} overhead j0 transmit string overhead j0 expect string overhead j1 length {16/64 | 1} overhead j1 transmit string overhead j1 expect string	Configure j0, j1 mode	config-controller-XX

Frame

POS frame has two kinds:
STM-1 in SDH system
OC-3 in SONET system
This command can configure the line transmission frame format.

Command	Description
router(config)# controller pos 0/0	
router(config-controller)# pos frame [sonet | sdh]	

Default is sdh mode

Configure J0 and j1 Mode

SDH segment and channel spending don't have tracking flag; the tracking flag can be single and multiple bytes (16byte). POS adopts single byte mode by default, and the content can be configured via pos flag, this command can also configured multiple bytes mode.

j0 configuration:

Command	Description
router(config)# controller pos 0/0	Enter extended configuration mode
router(config-controller)# overhead j0 length 1	Configure j0 sending mode as single byte mode
router(config-controller)# overhead j0 length 16	Configure j0-sending mode as multiple bytes mode.
router(config-controller)# overhead j0 transmit	Configure multiple bytes mode

[string]	content
router(config-controller)# overhead j0 expect [string]	Configure multiple bytes mode expecting value

Single byte mode by default.
Send string in multiple bytes mode: signamax tech.

J1 configuration:

Command	Description
router(config)# controller pos 0/0	Enter extended configuration mode
router(config-controller)# overhead j1 length 1	Configure j1 sending mode as single byte mode
router(config-controller)# overhead j1 length 16	Configure j1 sending mode as multiple bytes mode
router(config-controller)# overhead j1 transmit [string]	Configure multiple bytes mode content
router(config-controller)# overhead j1 expect [string]	Configure multiple bytes mode expecting value

Single byte mode by default.
Send string in multiple bytes mode: signamax tech.

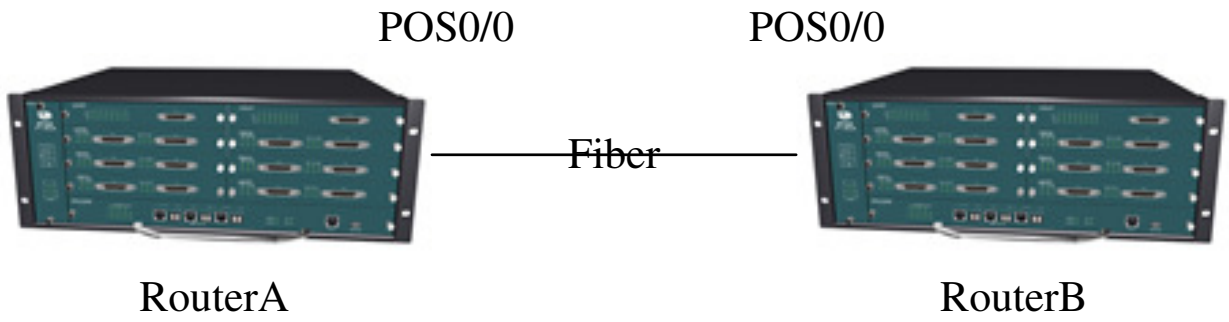
PoS Physical Layer Display Command

Display driver inner information.

```
    Command format:
            show controller pos [slot/port]
    output interface statistics information by default.
    Output format:
    router#show cont pos 0/0
     Interface: pos0/0
     Frame: sdh stm-1    Payload:POS(Package on SDH)
     Frame scramble:Tx enable,   Rx enable
     Paylaod scramble:Tx enable,   Rx enable
    Clock:internal
    SECTION   /* section status information*/
      ALARM:  /*alarming*/
        OOF: 0, LOF: 0, LOS: 0, TIU: 0, TIM: 0
      J0Z0:     /*tracking flag*/
        Tx: signal byte  j0: 00
        Rx: signal byte  j0: 00
    LINE  /* line status information*/
      ALARM  /*alarming*/
        AIS: 0, RDI: 0, SF: 0, SD: 0, PSBF: 0
      K1: 0, K2: 0, S1: 0 /*spending segment*/
    PATH  /* status information*/
      ALARM
        AIS: 0, RDI: 0, ERDI: 0, ARDI: 0, LOP: 0, TIM: 0, TIU: 0,
PSLM: 0, PSLU: 0
    /*1 means alarming, 0 means no alarming*/
       TxPTR: 0, TxSS: 2,  TxC2: 16
       RxPTR: 0, RxSS: 2, RxC2: 16
```

```
      J1:
        Tx: signal byte  j1: 00
        Rx: signal byte  j0: 00
    PAYLOAD
    LINE INTERFACE

    SYSTEM INTERFACE
    RFCLK LOCK: 1, RFCLK ERR: 0, TFCLK LOCK: 1, TFCLK ERR: 0

    SECTION
    BIP: 0  /*B1 error statistics*/
    LINE
    BIP: 0, REI: 0 /*B2、FEBE error statistics*/
    PATH
    BIP: 0, REI: 0 /*B3、FEBE error statistics*/
    PAYLOAD /*physical layer statistics information*/
    RxBytes: 2186, RxFrame: 57, RxAbrtFrame: 0, RxFcs: 0, RxMinLen: 0,
RxMaxLen: 0
    TxBytes: 2252, TxFrame: 60, UsrAbrtFrame: 0, UnderRun: 0
```

PoS Configuration Example



RouterA connects RouterB via SDH network.

RouterA configuration:

Command	Description
RouterA#configure terminal	Enter global configuration mode
RouterA (config)#interface pos0/0	Enter pos0/0
RouterA (config-if-pos0/0)#ip address 12.1.1.1 255.255.255.0	Configure ip address
RouterA (config-if-pos0/0)# exit	Exit to privileged configuration mode

RouterB configuration:

Command	Description
RouterB#configure terminal	Enter global configuration mode
RouterB (config)#interface pos0/0	Enter pos0/0

RouterB (config-if-pos0/0)#ip address 12.1.1.2 255.255.255.0	Configure ip address
RouterB (config-if-pos0/0)#clock source internal	Configure internal clock in back-to-back mode.
RouterB (config-if-pos0/0)# exit	Exit to privileged configuration mode

If using back-to-back mode, configure clock on POS, or it cannot transmit normally.

CPOS Module Configuration

SONET/SDH is a integrated information network technology combing multiplexer, line transmission and switching together, and managed by network system. POS directly transmits IP service data via high-speed transmission channel provided by SONET/SDH, which has effectively supported increased IP data flow.

POS provides smart solution for different transmission application, such as network backbone construction, network edge data aggregation and spreading. POS of the router always connects to ADM, end point to point SONET/SDH connection. POS can also be connected via fiber or DWDM system. POS uses PPP as link layer encapsulation protocol.

CPOS is channelized POS, so the logical channel division can be done on CPOS.

CPOS is compatible with SONET/SDH interface standard, it can be divided to 63 E1 channels. Each E1 channel can operate in framing or unframing mode. Link layer supports hdlc, ppp and fr protocols encapsulation.

Configure CPOS

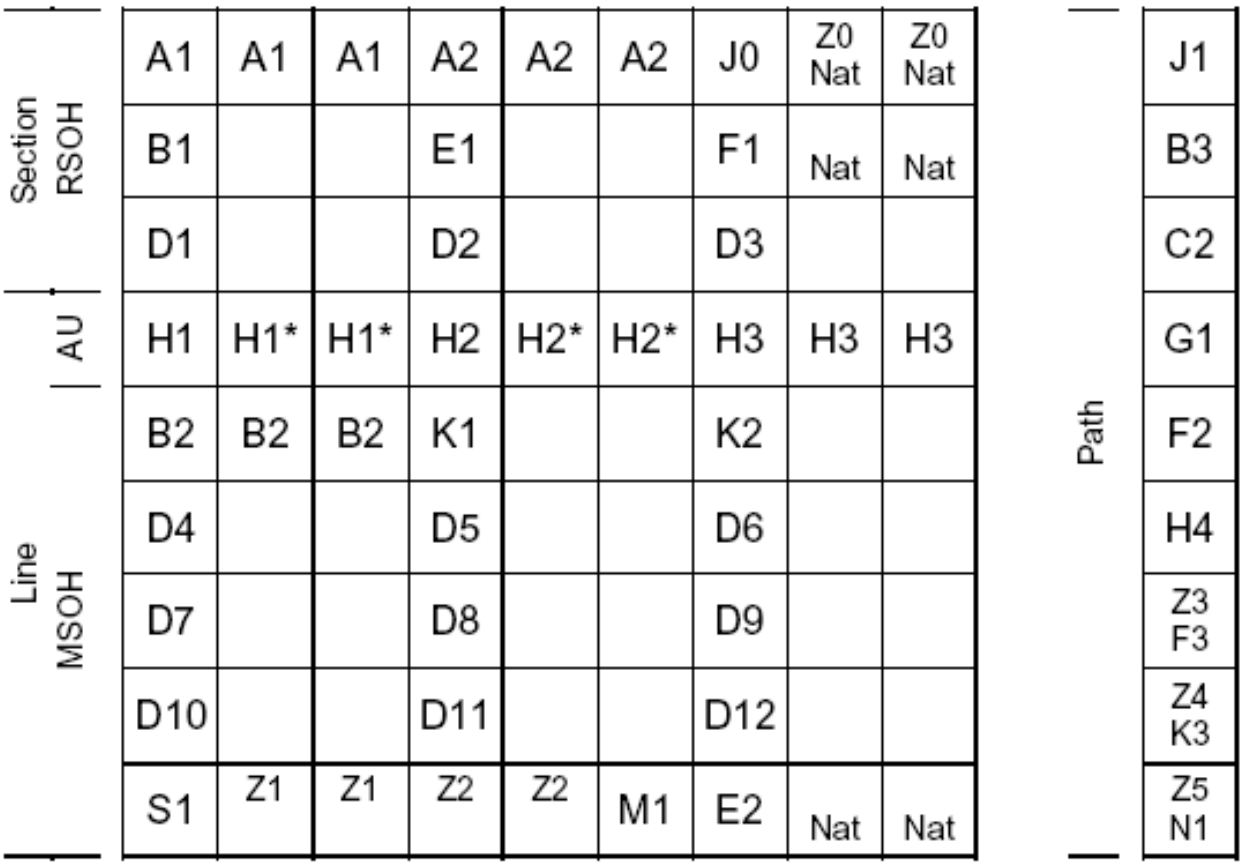
Command	Description	Config mode
controller cpos slot/unit	Define controller (slot/unit) to enter CPOS configuration mode via unit number.	config
framing {sonet|sdh}	Choose network frame mode: sonet: synchronous optical network, the national version doesn't support. sdh: synchronous digital system structure, valid by default.	config-controller-cpos
aug mapping {au3|au4}	Choose mapping mode: au3:adopt tug2—>vc3—>au3—>aug1—>STM1 route, and the national version doesn't support. au4:adopt tug2—>tug3—>vc4—>au4—>aug1—>STM1 route, valid by default.	config-controller-cpos
clock source {internal|line}	Choose port sending clock source: internal: port provides clock. line: pick up clock from line, valid by default.	config-controller-cpos
loopback {local|remote}	Configure loopback mode: local: local loopback. remote: remote loopback	config-controller-cpos
flag {k1|k2|s1|z0|j1|c2|f2|f3|k3|n1} value	*configure section spending and channel spending byte value.	config-controller-cpos
overhead {j0|j1} length {16|64}	Configure trail message length: 16:configure trail message length 16, valid by default. 64:configure trail message length 64.	config-controller-cpos
overhead {j0|j1} transmit string	Configure trail message sending string.	config-controller-cpos
overhead {j0|j1} expected string	Configure section or channel trail expected string.	config-controller-cpos
report {all|lais|lom|lrdi|pais|plop|prdi|sd-ber|sf-ber|slof|slos|uneq-p|pslm}	Enable designated alarming information displaying: all:enable all alarming information displaying lais:enable received section AIS signal alarming lom:enable framing lost alarming lrdi:enable received segment RDI signal alarming pais:enable received high rank channel AIS signal alarming plop: enable high rank channel index lost	config-controller-cpos

	alarming prdi: enable received high rank channel RDI signal alarming sd-ber:enable received error signal attenuation threshold alarming sf-ber:enable received error signal invalidation threshold alarming slof:enable SDH frame synchronous lost alarming slos:enable SDH analog signals lost alarming uneq-p:enable high rank channel no use alarming pslm:enable received the not matched of high rank channel signal and expected value. flag byte valu enable received the not matched alarming of high rank channel signal and expected value.	
threshold {sd-ber|sf-ber} value	Configure signal degrade and fail threshold: sd-ber:signal degrade threshold, value range is 3～9, BIP error code level value is 6 by default, 10-6 sf-ber:signal fail threshold, value range is 3～9, BIP error code level is 3 by default, 10-3	config-controller-cpos
bundle-group number tributary range	*set up multiple link binding interface, number range is 0～41； the branch range is designated by range	config-controller-cpos
mode {c11|c12}	Branch mode: c11:T1 frame, the national version doesn't support. c12:E1 frame, valid by default.	config-controller-cpos
tributary trib channel-group number timeslots range	*set up single link interface: Set up a channel number on trib branch, CPOS interface is similar with serial slot/unit/trib:number,and the timeslot is designated by range	config-controller-cpos
tributary trib unframed	*set up single link interface: Set up an unframed interface on trib branch	config-controller-cpos
tributary trib loopback {local|remote}	Loopback on trib branch: local:local loopback remote::remote loopback	config-controller-cpos
tributary trib clock source {internal|line}	Choose sending clock source on trib branch: internal:branch provides clock	config-controller-cpos

	line:pick up clock from the line, valid by default.	
tributary order number	*choose branch number mode, and the range value is 0～5,default value is 0.	config-controller-cpos
show tributary order number	Display number branch number list	config-controller-cpos
show controllers cpos slot/unit	*display designated CPOS controller statistics information	config-controller-cpos
reset controllers cpos slot/unit	Clear CPOS controller statistics information	config-controller-cpos
no loopback	Cancel port loopback	config-controller-cpos
no report {all|lais|lom|lrdi|pais|plop|prdi|sd-ber|sf-ber|slof|slos|uneq-p|pslm}	Disable all alarming information display	config-controller-cpos
no bundle-group number	Delete bundle group number	config-controller-cpos
no tributary trib channel-group [number]	Delete number interface on branch trib	config-controller-cpos
no tributary trib loopback	Cancel trib loopback	config-controller-cpos

"*" means the command has configuration example description.

The configuration mode can be config, config-controller-cpos flag configure section and channel spending byte value, and the position is as following:



flag {k1|k2|s1|z0|j1|c2|f2|f3|k3|n1} [value]

Command	Description
Value	Configured value

(Default status) z0 value by default is 0xCC, c2 value by default is 0x01,and other bytes value is 0.

bundle-group
Configure this command when setting up multiple link binding interface, NO is used for deleting the command.

bundle-group number tributary range [framed]
no bundle-group number

Command	Description
number	Binding interface number, and the range is 0～41,the interface is similar with serial slot/unit/0:number
range	Branch number group, and the range is 1～63,such as 1-8
framed	The branch adopts framed mode, no input means it adopts unframed mode.

(Default status)no

The branch number cannot be over 12. All branches should be framed or unframed modes tributary trib channel-group

Configure this command when setting up CPOS; NO is used for deleting CPOS.

```
tributary trib channel-group number timeslots range
tributary trib unframed
no tributary trib channel-group [number]
```

Command	Description
trib	Choose to set up interface on which branch, and the range is 1～63
number	Interface channel group number, 0～31
range	Timeslot range of the interface, choosing from 1～31, using "-" for connection, for example, 1-31； using "," for disconnection, for example, 1,3,5-7
unframed	Unframed mode, channel group number is 0 by default.

(Default status)no

tributary order

Configure branch number mode, use command show tributary order to display mapping list.

tributary order number

Command	Description
number	Branch number mode, and the value is 0～5 0—tug3 added, and then tug2,finally tu 1—tu added, and then tug2,finally tug3 2—tug3 added, and then tu,finally tug2 3—tu added, and then tug3,finally tug2 4—tug2 added, and then tug3,finally tu 5—tug2 added, and then tu,finally tug3

(Default status)0

show controllers cpos
display slot CPOS controller statistics information.

show controllers cpos slot/unit

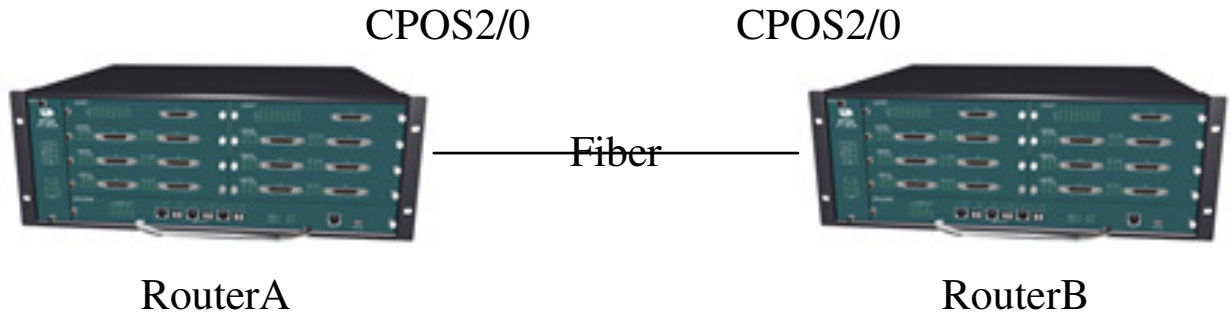
Command	Description
slot	Slot number
unit	Port number, 0 for 1×CPOS

(Default status)no

Statistics information list:

Level	Information	Description
SECTION	OOF, LOF, LOS	0—not happen, 1—being happen
	BIP (B1)	B1 error number
	J0	Trail message content
LINE	RDI, AIS	0—not happen, 1—being happen
	REI	Received remote error total number
	BIP (B2)	B2 error number
	K1, K2, S1	Received K1, K2, S1 bytes content
PATH	RDI, AIS	0—not happen, 1—being happen
	REI	Received remote error total number
	BIP (B3)	B3 error number
	LOP, NEWPTR	0—not happen, 1—being happen
	TPTR, RPTR	Sending and receiving (AU-PTR) value
	RPJE, RNJE	Received negative and positive index adjustment total number
	TPJE, TNJE	Sending negative and positive index adjustment total number
	J1	Received trail message content

CPOS Configuration Example



RouterA connects RouterB via fiber. There 3 branches, one is unframed mode, the second is framed mode, and the third is timeslot.

RouterA configuration:

Command	Description
RouterA#configure terminal	Enter global configuration mode
RouterA (config)#controller cpos 2/0	Enter cpos2/0 extended command configuration mode
RouterA (config-controller-cpos)# tributary 1 unframed	Configure tributary 1 unframed
RouterA (config-controller-cpos)#tributary 2 channel-group 0 timeslots 1-31	Configure tributary 2 framed, timeslot is 1-31
RouterA (config-controller-cpos)#tributary 3 channel-group 0 timeslots 1	Configure tributary 3 using timeslot 1, channel group number is 0
RouterA (config-controller-cpos)#exit	Exit to privileged configuration mode
RouterA (config)#interface serial 2/0/1:0	Enter tributary 1s2/0/1:0
RouterA (config-if-serial2/0/1:0)#encapsulation ppp	
RouterA (config-if-serial2/0/1:0)#ip address 44.1.0.1 255.255.255.0	
RouterA (config-if-serial2/0/1:0)#exit	
RouterA (config)#interface serial 2/0/2:0	Enter tributary 2 s2/0/2:0
RouterA (config-if-serial2/0/2:0)#encapsulation ppp	
RouterA (config-if-serial2/0/2:0)#ip address 44.2.0.1 255.255.255.0	
RouterA (config-if-serial2/0/2:0)#exit	
RouterA (config)#interface serial 2/0/3:0	Enter tributary 3 s2/0/3:0, 2/0 is slot number of cpos, channel number is 0

RouterA (config-if-serial2/0/3:0)#encapsulation ppp	
RouterA (config-if-serial2/0/3:0)#ip address 44.3.0.1 255.255.255.0	
RouterA (config-if-serial2/0/3:0)#exit	

RouterB configuration:

Command	Description
RouterB#configure terminal	Enter global configuration mode
RouterB (config)#controller cpos 2/0	Enter cpos2/0 extended command configuration mode
RouterB (config-controller-cpos)#clock source internal	Configure internal clock, only in Back-to-back mode.
RouterB (config-controller-cpos)#tributary 1 unframed	Configure tributary 1 unframed
RouterB (config-controller-cpos)#tributary 2 channel-group 0 timeslots 1-31	Configure tributary 2 framed, timeslot is 1-31
RouterB (config-controller-cpos)#tributary 3 channel-group 0 timeslots 1	Configure tributary 3 using timeslot 1, channel group number is 0
RouterB (config-controller-cpos)#exit	Exit to privileged configuration mode
RouterB (config)#interface serial 2/0/1:0	Enter tributary 1s2/0/1:0
RouterB (config-if-serial2/0/1:0)#encapsulation ppp	
RouterB (config-if-serial2/0/1:0)#ip address 44.1.0.2 255.255.255.0	
RouterB (config-if-serial2/0/1:0)#exit	
RouterB (config)#interface serial 2/0/2:0	Enter tributary 2 s2/0/2:0
RouterB (config-if-serial2/0/2:0)#encapsulation ppp	
RouterB (config-if-serial2/0/2:0)#ip address 44.2.0.2 255.255.255.0	
RouterB (config-if-serial2/0/2:0)#exit	
RouterB (config)#interface serial 2/0/3:0	Enter tributary 2 s2/0/3:0
RouterB (config-if-serial2/0/3:0)#encapsulation ppp	
RouterB (config-if-serial2/0/3:0)#ip address 44.3.0.2 255.255.255.0	
RouterB (config-if-serial2/0/3:0)#exit	

CPOS Usage Attention

Clock Configuration

CPOS card clock has SDH (line clock) and E1 (service clock). In typical network application, SDH clock is always external clock, which is picking up 155M clock from the line; E1 clock is external clock too, but sometimes internal clock.

Channel Trail Message (J1) Configuration

Some SDH equipment needs to check trail message, if not matching, it alarms, which will cause the stop of the data transmission. If this happens, use command overhead j1 transmit to receive the message.

Tributary Orientation

SDH frame structure comprises 63 E1 tributaries, and both sides only can communicate by using the same position E1. CPOS adopts E1 orientation mode in MP9700 SDH.

Configuring Interface-group

Bind multiple interfaces together as an interface-group. Once interface commands are configured in the interface-group, all interfaces in the interface-group will automatically generate those commands. This can reduce the repeat of configuring the same commands on each interface. The main contents of this section are listed as follows:

Basic interface-group configuration commands

An example of interface-group configuration

Configuration and statistics information of interface-group

Basic Interface-group Configuration Commands

Create an interface-group

router(config)#interface group <0-255> ?

Syntax	Description
Enum	Adopt the enumeration mode to specify some interfaces for the generation of an interface-group
Range	Set the interface range of the interface-group via specifying the start interface and end interface
Display	Display all interfaces contained by the interface-group

The type of each interface in an interface-group should be the same such as asynchronous interface. The above are the basic commands to create an interface-group. If no interface-group is created, the system will display the inexistence of the command such as the command show if-group related with the interface-group.

The commands related with the configuration and statistics information of the interface-group do not exist until at least one interface-group is created.

Interface-group Configuration

Configure interface-group parameters:

Syntax	Description
router(config)#interface group 2 range async1/0 async1/15	Set interface-group 2 containing 16 asynchronous interfaces (from interface async1/0 to async1/15)
router(config-if-group2)#encapsulation terminal	Encapsulate the terminal protocol on the interface-group
router(config-if-group2)#speed 9600	Configure the rate on the interface-group
router(config-if-group2)#flow-control software 65535	Configure the flow-control on the interface

Configuration result:

```
router#show running-config
...
interface group 2 range async1/0 async1/15   (Configure an
asynchronous interface-group.)
....
interface async1/0              (Configure the asynchronous
                          interface contained by the interface-
                          group to be automatically generated on
                          the interface-group.)
 speed 9600
 databits 8
 stopbits 1
 parity none
 flow-control software 65535
 tx-on dsr
 encapsulation terminal
 exit

interface async1/1
 speed 9600
 databits 8
 stopbits 1
 parity none
 flow-control software 65535
 tx-on dsr
 encapsulation terminal
 exit
.... (The following configuration is omitted)
```

Configuration & Statistics of Interface-group

`show interface group _0_255_`
Use the command above to display the detailed interface information of all interfaces contained by the specified interface-group.

(Command mode) the privileged user configuration mode.

`show if-group`
Use the command above to display all interface information of each interface-group.
(Command mode)the privileged user configuration mode.

`show running-config interface group _0_255_`

Use the command above to display the configuration information of all interfaces contained by the specified interface-group.

(Command mode) the privileged user configuration mode.

Interface Traffic Statistics Configuration

The router can do traffic statistics to any interface.

Configuration Command

Modify traffic statistics time interval
`router(config-if-xxx)#load-interval <30-600> ?`

Syntax	Description
load-interval	Configure traffic statistics time interval, and the default time is 5 minutes
<30-600>	Time interval (unit is second)

1. Time interval is the multiple of 10.

Traffic Statistics Configuration Example

Syntax	Description
router(config-if-fastethernet0)#load-interval 400	Configure interface traffic statistics time interval 400 seconds (6 minutes and 40 seconds)

Configuration result:

```
    router#show int f0
    fastethernet0:
         Flags: (0x408863) UP BROADCAST MULTICAST ARP RUNNING
GWUP
         Type: ETHERNET_CSMACD
         Internet address: 1.1.1.2/24
         Broadcast address: 1.1.1.255
         Internet address: 128.255.43.89/22
         Broadcast address: 128.255.43.255
         Queue strategy: FIFO Output queue: 0/40 (/max packets)
         Metric: 0, MTU: 1500, BW: 100000 Kbps, DLY: 100 usec,
VRF: kernel
         Reliability 255/255, Txload 1/255, Rxload 1/255
         Ethernet address is 80ff.2b59.0000
         6 minutes 40 seconds input rate 1000 bits/sec, 1
packets/sec
         6 minutes 40 seconds output rate 0 bits/sec, 0
packets/sec
         3698 packets received; 19 packets sent
         3698 multicast packets received
         17 multicast packets sent
         15 input errors; 0 output errors
         0 collisions; 0 dropped
            0 no buffer for receive, speed 100Mbit/s, mode full
duplex
            receive 10727 broadcasts, 0 runts, 0 giants, 0
throttles
            0 input error 0 CRC, 0 frame, 0 overrun, 0 ignored
            0 output error0 collisions, 0 interface resets, 0
underrun
            0 babbles, 0 late collision, 0 deferred
            0 lost carrier, 0 no carrier 0 excessive collison
```

802.1 Configuration

This chapter explains how to configure Signamax series routers so it can connect to a VLAN (Virtual LAN) and an exterior network.

802.1Q Protocol

802.1Q standard defines the principle of VLAN (Virtual LAN) and how to realize it. VLAN is used for realizing the isolation of data link layer, and expanding and managing effectively to switch Ethernet

DA	SA	Type	Data	CRC

Standard Ethernet frame

DA	SA	Tag				Type	Data	CRC
		0x8100	Priority	FI	VLAN ID			

IEEE 802.1Q standard frame
Key fields explanation:
DA: destination MAC address
SA: source MAC address
Type: protocol type
Data: user data in the frame
CRC: Cyclic Redundancy Check
CFI: Canonical Format Indicator
Priority: user priority
VLAN ID: VLAN ID number

Compared with standard Ethernet frame, 802.1Q protocol has added Tag field, to include VLAN information, and confirm the property of the data frame.

802.1Q Configuring Principles

A VLAN ID number is added to all network devices via the 802.1Q protocol. All devices with the same VLAN ID number will be able to communicate with each other.

Equipment in different VLAN groups won't be able to communicate with each other – unless they're configured to the same VLAN ID number. The following section will tell you how to set up your devices to ensure proper communications.

VLAN Functions

An Ethernet supporting 802.1Q can be divided into many subnets, and each subnet will correspond to a certain VLAN. When a data packet passes through a switch, it is checked against 802.1Q standards.

A VLAN **tag** will then be added to describe which the packet it belongs to. When a router's Ethernet interface receives a data packet, the interface will compare its own VLAN tag with the interface's related tag.

If the receiving interface and data packet both belong to the same VLAN, the interface will receive the incoming data. Or, the packet will be discarded.

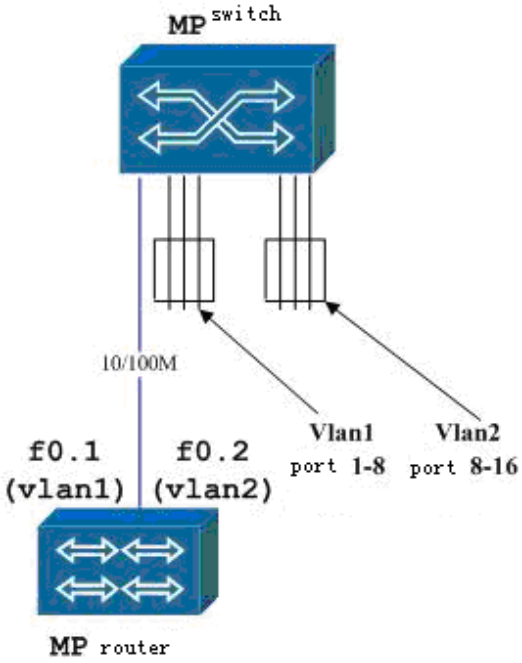
Similarly, when the router sends a data packet, the router also checks the tag. All devices with the same VLAN tag will be able to communicate with each other, but should pass according to layer three routing.

Router On A Stick

In order to accomplish router-on-a-stick routing, many links between a router and a switch are formed. Namely, each of the router's Ethernet interface which needs connects with a switch's port. The method is very simple, but it doesn't make effective use of the router's interface so it isn't an ideal method.

The interface is used fully via router-on-a-stick.

The switch is configured as two VLANs – VLAN1 and VLAN2. Port 1 is configured as a relay port belonging to both VLAN 1 and VLAN 2. Two sub-interfaces are configured on a fast Ethernet router interface and are each assigned to an independent IP subnet. Two related VLAN IDs are named in each sub-interface.



Router-On-A-Stick Routing

VLAN1 or VLAN 2's data stream can get to router sub-interface f0.1/ f0.2 via relay port 1. The routing between two VLANs is accomplished via the use of two sub-interfaces. Because the router only has one physical interface that connects to a switch port, the router will have a router-on-a-stick router alias.

Subnet Isolation

As long as two sub-interfaces and their related VLAN are configured in default mode, the two VLANs can communicate with each other. But in some implementation, it isn't what we expected.

To do this, you will have to create a new access list based on the router-on-a-stick configuration to filter communications between the two VLANs. The access list should be applied to related VLAN sub-interface.

802.1Q Configuration Command

Only sub-interfaces 1 to 63 of the Ethernet interface can be encapsulate to 802.1Q protocols. Each sub-interface can be configured with any VLAN ID number from 1 to 4,094.

The 802.1Q protocol configuration involves the following three steps:

Command	Description	Config. command
interface fastethernet interface unit number[.sub-unit number]	*Set up fast Ethernet interface subnet interface.	config
encapsulation dot1q vlan id [native]	*Configure encapsulation 802.1Q protocol and VLAN ID(native: configure VLAN as Native VLAN)	config-if-××
shutdown	Shutdown sub-interface	config-if-××
no shutdown	Re-enable the sub-interface	config-if-××
ip address unicast address network mask	*Configure sub-interface network address and mask.	config-if-××
ip access-group {IP access list | Access-list name} {in | out}	*Apply the access list on the sub-interface	config-if-××

"*" before command means it has configuration example description;

the configuration mode can be config, config-if-××(interface name) config-××(protocol name) etc.

The detailed configuration command is:

interface fastethernet

In order to encapsulate 802.1Q protocol, the sub Ethernet interface should be created, and no is used to disable the command.

```
interface fastethernet 0.?
no interface fastethernet 0.?
```

Command	Description
[0-1023]	Sub interface number

fastethernet0.0 is the main interface, which cannot encapsulate 802.1Q protocol. Sub interface at most can reach 1023.

(Default status) no definition

encapsulation dot1q

In order to encapsulate 802.1Q protocol and use this command; or shutdown is used to disable the interface. Command no shutdown is used to restart this interface.

```
encapsulation dot1q vlan id[native]
shutdown
no shutdown
```

Command	Description
encapsulation dot1q vlan id [native]	Encapsulate 802.1Q protocol, and configure VLAN ID(native: configure VLAN as Native VLAN)
shutdown	Disable the interface
no shutdown	Reenabling the interface

The ethernet sub interface only encapsulates 802.1Q protocol; the use needs to configure VLAN ID. VLAN ID is 1—4094.

(Default status) no definition

ip

The ip layer can use 802.1Q protocol and use these two commands; or, no is used to disable the commands. ip address is used to configure the interface ip address and mask; while ip access-group is used to configure access list.

```
ip address unicast address network mask
no ip address unicast address network mask
ip access-group  {IP access list |  Access-list name} {in |
out}
no ip access-group  {IP access list |  Access-list name} {in
| out}
```

Command	Description
address unicast address network mask	Configure IP address and mask on sub-interface
access-group {IP access list | Access-list name} {in | out}	Apply the access list on sub-interface

The IP address on sub-interface should be in the same segment of VLAN IP address. If using router-on-a-stick function, some communication among devices should be disabled. The access list should be applied on sub-interface.

(Default status) no definition

802.1Q Configuration Example

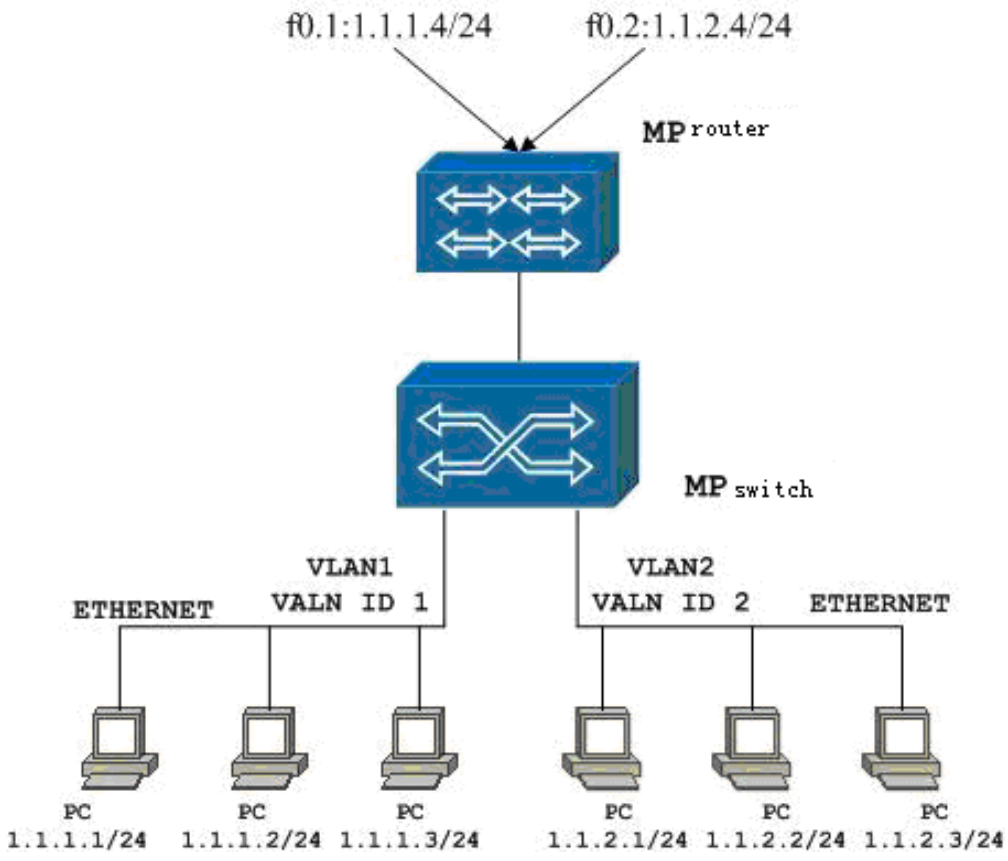
This section explains:

Router-on-a-stick typical application

Subnet isolation typical application

Configuration and statistics information

Router-On-A-Stick Application



Router-On-A-Stick

The fastethernet interface of Router MP2600 connects with the relay interface, MP5124A. The two Ethernet sub-interfaces have been configured as fastethernet0.1 and fastethernet0.2. Related VLAN IDs are 1 and 2.

Two VLANs have been set on MP5124A. The VLAN ID 1 interface connects with the left three PCs and the VLAN ID 2 interface connects with the right three PCs. The relay interface comprises two VLAN groups.

The PCs named in VLAN ID 1 are in the subnet 1.1.1.0/24, while the PCs in VLAN ID 2 are in the subnet 1.1.2.0/24. This allows communication between two VLANs.

To configure fastethernet0.1:

Command	Task
router(config) #interface fastethernet0.1	Creates the router's fastethernet0.1 sub-interface
router(config-if-fastethernet0.1)#encapsulation dot1q 1	Sets the VLAN ID of fastethernet0.1 as 1
router (config-if-fastethernet0.1)#ip address 1.1.1.4 255.255.255.0	Sets the IP address of fastethernet0.1 as 1.1.1.4, a subnet mark with 24 bits

To configure fastethernet0.2:

Command	Task
router(config) #interface fastethernet0.2	Creates the router's fastethernet0.2 sub-interface
router(config-if-fastethernet0.2)#encapsulation dot1q 2	Set VLAN ID of fastethernet0.2 as 2
router (config-if-fastethernet0.2)#ip address 1.1.2.4 255.255.255.0	Set IP address of fastethernet0.2 as 1.1.2.4, a subnet mark with 24 bits

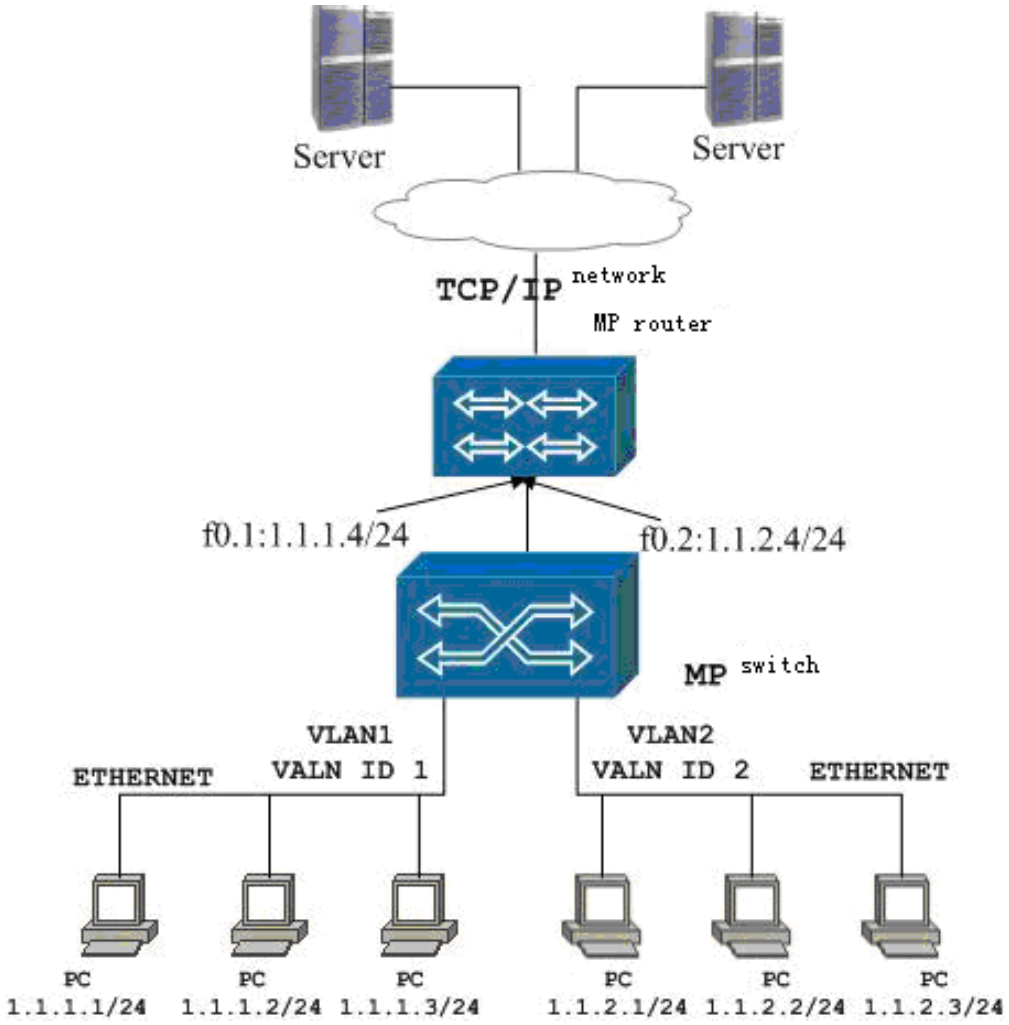
The VLAN 1 PC's default gateway is set to IP address 1.1.1.4 in the MP2600's fastethernet0.1 interface. The VLAN 2 PC's default gateway is set to IP address 1.1.2.4 in the MP2600's fastethernet0.2 interface.

Configuration Results:

```
router#show run
Building Configuration...done
hostname router
no service password-encrypt
no service enhanced-secure
interface loopback0
exit
interface fastethernet0
exit
interface fastethernet0.1
ip address 1.1.1.4 255.255.255.0
```

```
encapsulation dot1q 1
exit
interface fastethernet0.2
ip address 1.1.2.4 255.255.255.0
encapsulation dot1q 2
exit
```

Typical Subnet Isolation Application



Subnet Isolation Sketch Map

The router's fast Ethernet interface connects with MP5124A's relay interface. Two Ethernet interfaces are configured to fastethernet0.1 and fastethernet0.2. The responding VLAN ID is set to 1 and 2.

The MP2600 uses a WAN interface to connect with server1 and server2 via a TCP/IP network.

MP2600 router adds two access lists to prohibit communications between VLAN1 and VLAN2. These VLANs access their own business servers via the router's WAN interface and aren't permitted to communicate with each other.

Two VLANs has been set on the MP5124A. The VLAN ID 1 interface connects with the left three PCs, while the VLAN ID 2 interface connects with the right three PCs. The relay interface comprises two VLAN groups.

The PCs in the VLAN ID 1 group are in network segment 1.1.1.0/24. The PCs in VLAN ID 2 are in network segment 1.1.2.0/24.

Parameter Configuration:

To configure an access list:

Command	Task
Router config #ip access-list standard 1	Creates a standard access list 1 on the router
router (config-std-nacl)#deny 1.1.1.0 0.255.255.255	Sets the first access list 1 rule to prohibit data from 1.1.1.0/24 from passing via
router (config-std-nacl)#permit any	Sets the second access list 1 rule to permit any data packet from passing through
Router config #ip access-list standard 2	Creates a standard access list 2 on the router
router (config-std-nacl)#deny 1.1.2.0 0.255.255.255	Sets the first access list 2 rule to prohibit data from 1.1.2.0/24 from passing through
router (config-std-nacl)#permit any	Sets the second access list 2 rule to permit any data packet from passing through

To configure fastethernet0.1:

Command	Task
Router config #interface fastethernet0.1	Creates sub-interface fastethernet0.1
router (config-if-fastethernet0.1)#encapsulation dot1q 1	Sets the fastethernet0.1 VLAN ID as 1
router (config-if-fastethernet0.1)#ip address 1.1.1.4 255.255.255.0	Sets the IP address of fastethernet0.1 as 1.1.1.4 and the subnet mask to 24 bits
router (config-if-fastethernet0.1)#ip access-group 2 out	the data sent from fastethernet0.1 is limited by access list 2

To configure fastethernet0.2

Command	Task
config #interface fastethernet0.2	Creates sub-interface fastethernet0.2
(config-if-fastethernet0.2)#encapsulation dot1q 2	Sets the fastethernet0.2 VLAN ID as 2
(config-if-fastethernet0.2)#ip address 1.1.2.4 255.255.255.0	Sets the IP address of fastethernet0.2 to 1.1.2.4 and the subnet mask as 24 bits
(config-if-fastethernet0.2)#ip access-group 1 out	The data sent from fastethernet0.2 is limited by the access list 1

Configuration Results:

```
router#show run
Building Configuration...done
hostname router
no service password-encrypt
no service enhanced-secure
ip access-list standard 1
deny 1.1.1.0.0.255.255.255
permit any
exit
ip access-list standard 2
deny 1.1.2.0 0.0.255.255.255
permit any
exit
interface loopback0
exit
interface fastethernet0
exit
interface fastethernet0.1
ip address 1.1.1.4 255.255.255.0
encapsulation dot1q 1
ip access-group 2 out
exit
interface fastethernet0.2
ip address 1.1.2.4 255.255.255.0
encapsulation dot1q 2
ip access-group 1 out
exit
```

Configuration Information & Statistics

Display Configuration Sub-Interface Results

```
router#show run
```

After input the preceding command, you can observe configuration data for each interface. The following is an example of extracted configuration information:

```
interface fastethernet0.1
ip address 2.2.2.2 255.255.0.0
encapsulation dot1q 1
exit
```

Display Sub-Interface Statistics

```
router#show dot1q interface f0.1
```

After input the above command, you can observe statistical information about packets sent or received by sub-interface f0.1:

```
fastethernet0.(unit number 1):
0 untagged packets received
0 tagged packets received
91 untagged packets sent
2 tagged packets sent
```

WAN Protocol Configuration

Signamax routers support the following familiar WAN protocols: PPP, HDLC, X.25, LAPB, X.25, Frame Relay, SLIP, ISDN and dial-up connection. This chapter explains how to configure Signamax MP series routers to connect with a WAN.

This chapter explains:

PPP protocol

HDLC protocol

SLIP protocol

TCP/IP header compression

X.25 protocol

Frame Relay protocol

Virtual Ethernet Bridge protocol

PPP Protocol

The PPP protocol is a kind of data link layer protocol used to transmit network layer packets on the connection from point-to-point. PPP comprises Link Control Protocol (LCP), Network Control Protocol (NCP), Authentication Protocol (PAP and CHAP) and it can support synchronous/asynchronous line.

PPP can be applied to serial systems with different properties to transmit many kinds of network layer protocol data. PPP is a universal method of connecting various kinds of hosts, bridges and routers.

PPP is composed of the following three components:

A method which encapsulates many kinds of network protocol datagrams

The Link Control Protocol (LCP) used to establish, configure and test the data link connection

A group of Network Control Protocols (NCP) used to establish and configure different network layer protocols

PPP Instructions

Command	Description	Configuration mode
encapsulation ppp	*encapsulate PPP protocol	config-if-××
ppp ac	PPP frame address and controlling segment compression	config-if-××
ppp accounting aaa-name	Configure PPP statistics method	config-if-××
ppp authentication chap [aaa-name] ppp authentication ms-chap [aaa-name] ppp authentication pap [aaa-name]	*configure PPP authentication(CHAP/PAP/MS-CHAP)	config-if-××
ppp authorization aaa-name	Configure PPP authentication	config-if-××
ppp bridge ip	Configure PPP bridge	config-if-××
ppp callback {accept | initiate | request}	Configure callback as accept, directly callback and requirement party	config-if-××
ppp chap hostname host-name ppp chap password password ppp chap send-hostname	*configure CHAP hostname *configure CHAP authentication password *configure whether sending CHAP authentication username(no means sending empty user name)	config-if-××
ppp compression {predictor | stacker}	*configure PPP data compression	config-if-××
ppp encrypt des keys	*configure PPP data encryption	config-if-××
ppp ipcp dns PrimaryDNS [SecondaryDNS] ppp ipcp wins PrimaryWINS [SecondaryWINS]	*configure dns, wins of PC	config-if-××
ppp ipcp ignore-map	Configure denying address via DDR MAP.	config-if-××
ppp mpls	*configure PPP supporting MPLS	config-if-××
ppp multilink ppp multilink fragment-delay milliseconds ppp multilink interleave	*configure interface multilink binding. Configure multilink fragment delay configure multilink fragment interleave	config-if-××

ppp pap sent-username user-name password password	*configure PAP username and password	config-if-××
ppp pc	Configure PPP frame protocol segment compression	config-if-××
ppp timeout authentication number ppp timeout ipcp number ppp timeout retry number	Configure PPP timeout interval	config-if-××
ppp bap number default phone-number	Configure BAP calling number	config-if-××
ppp bap call { accept | request }	Configure BAP call type	config-if-××
ppp bap call timer seconds	Configure BAP call interval	config-if-××
ppp bap callback { accept | request }	Configure BAP callback type	config-if-××
ppp bap callback timer seconds	Configure BAP callback interval	config-if-××
ppp bap drop { accept | request }	Configure BAP drop type	config-if-××
ppp bap drop after-retries	Designate BAP drop condition	config-if-××
ppp bap drop timer seconds	Configure BAP drop time interval	config-if-××
ppp bap link types {analog | isdn }	Configure BAP link types	config-if-××
ppp bap max dial-attempts number	Configure BAP max attempts numbers	config-if-××
ppp bap max dialers number	Configure BAP max dialing times	config-if-××
ppp bap number default phone-number	Configure calling number	config-if-××
ppp bap number secondary phone-number	Configure secondary calling number	config-if-××
ip local pool pool-name A.B.C.D E.F.G.H ip local pool default A.B.C.D E.F.G.H	*define an address pool named pool-name. starting address is A.B.C.D, ending address is E.F.G.H *define a default address pool, starting address is A.B.C.D, ending address is E.F.G.H	config
ip address-pool local	Enable default address pool on all interfaces	config
peer default ip address A.B.C.D peer default ip address pool peer default ip address pool pool-name	*distribute a fixed ip address A.B.C.D to peer *enable default address pool *enable address pool named pool-name	config-if-××
ip address negotiated	*enable address negotiation	config-if-××

"*" before command means it has configuration example description.

The configuration mode is config, config-if-××(interface name) config-××(protocol name) etc.

ppp authentication

In order to ensure dialing connection security, PPP authentication protocol is needed; or, no is used.

```
ppp authentication pap [aaa-name]
ppp authentication chap [aaa-name]
ppp authentication ms-chap [aaa-name]
no ppp authentication
```

Syntax	Description
Pap	Enable PAP authentication
Chap	Enable CHAP authentication
ms-chap	Enable ms CHAP authentication
aaa-name	Enable AAA server authentication

(Default status) no definition

ppp authorization

In order to support AAA server authorization function on PPP protocol, use this command; or, use no format.

```
ppp authorization aaa-name
no ppp authorization
```

Syntax	Description
aaa-name	Authorization name on AAA server

(Default status)no definition

ppp callback

In order to use callback function on PPP negotiation, use this command; or, use no format.

```
ppp callback {request | accept | initiate}
no ppp callback {request | accept | initiate}
```

Syntax	Description
accept	Configure as callback accepting party
initiate	Configure as direct callback
request	Configure as callback request

(Default status)no definition

When PPP protocol doesn't have callback option but it still needs, please use command ppp callback initiate (for example, the callback negotiation between router and Linux).

When the router is on callback with windows, and windows is used as callback server, we suggest using command ppp callback accept.

ppp chap password

Configure authentication password. No is used to cancel the configuration.

```
ppp chap password password
no ppp chap password
```

Syntax	Description
password	Password by default

(Default status)no definition

ppp chap hostname

Configure chap user name, no is used to cancel the configuration.

```
ppp chap hostname host-name
no ppp chap hostname
```

Syntax	Description
Host-name	Designate CHAP authentication hostname

(Default status) hostname of routers

ppp chap send-hostname

for chap authentication, enable sending user name switch, no is used to disable the switch, sending empty user name.

```
ppp chap send-hostname
no ppp chap send-hostname
```

(Default status)no definition.

PPP protocol deals with user name authentication information by default, ms-chap also supports empty user name, and the configuration is the same.

ppp compression

use this command to enhance PPP viaput; or use no format.
ppp compression {predictor | stacker}

no ppp compression

Syntax	Description
predictor	Enable predictor compression (memory type)
stacker	Enable stacker compression (CPU type)

(Default status)no definition.

ppp encrypt des

In order to enhance PPP line security, configure DES encryption; or use no format.

```
ppp encrypt des encrypt-key
no ppp encrypt
```

Syntax	Description
encrypt-key	Configure encryption key

(Default status)no definition.

ppp ipcp dns

Use this command to distribute DNS address for windows PC dialing; or use no format.

```
ppp ipcp dns A.B.C.D [E.F.G.H]
no ppp ipcp dns
```

Syntax	Description
A.B.C.D	First DNS address
E.F.G.H	Secondary DNS address

(Default status)no definition

This command uses to the dialing between router and windows.

ppp ipcp wins

Use this command to distribute WINS address for windows PC dialing; or use no format.

```
ppp ipcp wins A.B.C.D [E.F.G.H]
```

```
no ppp ipcp wins
```

Syntax	Description
A.B.C.D	First DNS address
E.F.G.H	Secondary DNS address

(Default status)no definition

This command uses to the dialing between router and windows.

ppp ipcp ignore-map

Use this command to negotiate IP address without dialer map; or use no format.

```
ppp ipcp ignore-map
no ppp ipcp ignore-map
```

(Default status)no definition

ppp ipcp ignore-map and dialer map use together, and is based on the existence of dialer map. When configuring dialer map, we negotiate peer ip address by default. If don't need this negotiation, ppp ipcp ignore-map is configured.

ppp mpls

Use this command to support MPLS packet transmission on PPP protocol; or use no format.

```
ppp mpls
no ppp mpls
```

(Default status)no definition

ppp multilink

Use this command to enhance link bandwidth by PPP multilink; or use no format.

```
ppp multilink [bap |fragment-delay milliseconds |interleave]
no ppp multilink [bap |fragment-delay|interleave]
```

Syntax	Description
bap	Enable multilink BAP function
frag ment-delay milliseconds	Adjust multilink fragment size
interleave	Enable multilink fragment interleave

(Default status)no definition

ppp bap call

Use this command to configure PPP BAP call parameter. Use no to disable the disconnection of designated type.

```
ppp bap call { accept | request | timer seconds }
no ppp bap call { accept | request | timer }
```

Syntax	Description
accept	Permit peer enabling link adding process, and it is default value
request	Permit enabling local link adding process
timer seconds	The time of the router sending call request, and the range is 2~120 seconds, no default value

(Default status)accept ---------peer enables link adding to multi-link.

ppp bap callback

Use the command to configure PPP BAP callback and its parameters. Use command no to delete PPP BAP callback configuration.

```
ppp bap callback { accept | request | timer seconds }
no ppp bap callback { accept | request | timer }
```

Syntax	Description
Accept	Permit enabling link adding process by peer notification of local routers
Request	Permit local router requiring for link adding process
timer seconds	The time of the router sending call request, and the range is 2~30 seconds, disable by default

(Default status)disable for callback.

ppp bap drop

Use this command to delete link parameter from a multilink. Use command no to disable the dealt of designated type.

```
ppp bap drop { accept | after-retries | request | timer
seconds } no ppp bap drop { accept | after-retries |request |
timer }
```

Syntax	Description
Accept	Permit enabling link deletion process of peer, and it is default value
Request	Permit local enabling link deleting process
timer seconds	The time of the router sending IRQ, and the unit is second, no default value
after-retries	The local router can delete link without BAP negotiation

(Default status)accept request-------permit peer enables link deletion, and local router enables link deletion.

ppp bap link types

Use this command to designate link type in multilink. Use command no to delete an interface type.

```
ppp bap link types [ isdn | analog ]
no ppp bap link types [ isdn | analog ]
```

Syntax	Description
isdn	ISDN link can be added to a multilink binding
analog	Asynchronous serial link can be added to multilink binding

(Default status)no definition

ppp bap max

Use this command to configure much bigger PPP BAP retransmission parameters. Use command no to delete the retransmission times.

```
ppp bap max { dial-attempts number|ind-retries number | req-
retries number | dialers number }
no ppp bap max { dial-attempts | ind-retries | req-retries |
dialers }
```

Syntax	Description
dial-attempts number	Permit the destination number dial max attempts number, and the range is 1～3, default value is 1
ind-retries number	Permit the max retries number of call status information, and the range is 1～10,default value is 3
req-retries number	Permit the request max retries number, and the range is 1～5,default value is 3

dialers number	Permit the dialers number, and the range is 1～10

(Default status)
1 time dial retries
5 times indication information retries
3 times request retries

ppp bap number

Use this command to designate a local telephone number, so that the peer sets a multilink binding via dialing. Use command no to delete a configured number.

```
ppp bap number { default phone-number | secondary phone-number } no ppp bap number { default | secondary }
```

Syntax	Description
default phone-number	The default phone number, used to enter dial
secondary phone-number	Secondary phone number used for the second channel B, only for BRI interface

(Default status)no definition.

ppp bap monitor load

Use this command to add or delete the link. Or use command no.

```
ppp bap monitor load
no ppp bap monitor load
(Default status) definition
```

ppp bap timeout

Use this command to configure PPP BAP hang up and response timeout value. Use command no to delete the value.

```
ppp bap timeout { pending seconds | response seconds }
no ppp bap timeout { pending | response }
```

Syntax	Description
pending seconds	Permit the pending seconds, and the range is 2～180, default value is 20
response seconds	Permit response seconds, and the range is 2～120, default value is 3

(Default status)accept - peer enables link added to multilink bind.

ip local pool

Configure IP address pool range, or use command no.

```
ip local pool {pool-name | default} A.B.C.D E.F.G.H
no ip local pool {pool-name | default} A.B.C.D E.F.G.H
```

Syntax	Description
pool-name	Address pool name
default	Default address pool
A.B.C.D	Starting address
E.F.G.H	Ending address

(Default status) no definition

ip address-pool local

Use this command to use address pool by default. Or use command no.

```
ip address-pool local
no ip address-pool local
(Default status) no definition
```

peer default ip address

Use this command to distribute IP address to PPP equipment, or use command no.

```
peer default ip address { A.B.C.D | pool [pool-name] }
no peer default ip address
```

Syntax	Description
A.B.C.D	Special IP address
pool-name	Special address pool name

(Default status) no definition

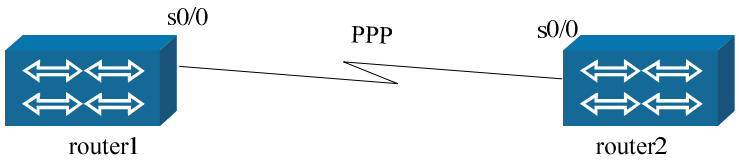
ip address negotiated

Use this command to auto get IP address of PPP negotiation, or use command no.

```
ip address negotiated
no ip address negotiated
(Default status) no definition
```

PPP Configuration Examples

Synchronous PPP Protocol



PPP configuration example

The port S0 (3.3.3.1) of local router connects with the port S0 (3.3.3.2) of the opposite router.

Router1 configuration:

Command	Description
router(config)#interface serial0/0	Enter the interface
router(config-if-serial0/0)#physical-layer sync	Configure synchronous mode
router(config-if-serial0/0)#encapsulation ppp	Encapsulate ppp protocol
router(config-if-serial0/0)#ip address 3.3.3.1 255.0.0.0	Configure ip address
router(config-if-serial0/0)#exit	Exit to interface

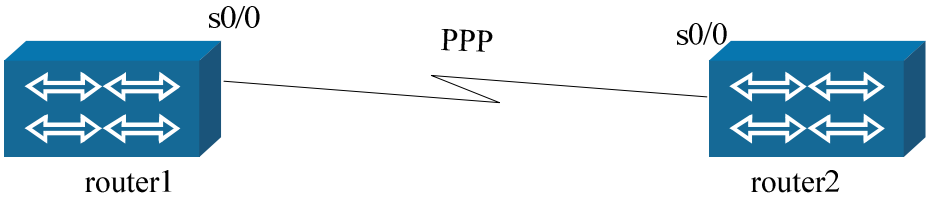
Router2 configuration:

Command	Description
router(config)#interface serial0/0	Enter the interface
router(config-if-serial0/0)#physical-layer sync	Configure synchronous mode
router(config-if-serial0/0)#encapsulation ppp	Encapsulate ppp protocol
router(config-if-serial0/0)#ip address 3.3.3.2 255.0.0.0	Configure ip address
router(config-if-serial0/0)#clock rate 128000	Configure line clock
router(config-if-serial0/0)#exit	Exit to interface

Configuring PPP Authentication

The PPP authentication between a local router and remote router supports PAP and CHAP, and it can be bi-directional

An example of configuring the PAP authentication



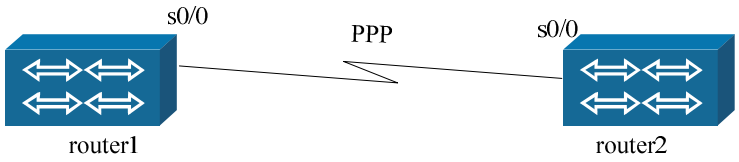
Router1 configuration:

Command	Task
Router1#configure terminal	Enters the global configuration mode
Router1(config)#user goat pass 0 Signamax	Configures the user name as goat and password as Signamax
Router1(config)#interface s0	Enters the interface S0
Router1(config-if-serial)#physical-layer sync	The physical layer works in synchronous mode
Router1(config-if-serial)#encapsulation ppp	Encapsulates PPP as link layer protocol
Router1(config-if-serial)#ppp authentication pap	Configures pap authentication
Router1(config-if-serial)#ip address 3.3.3.1 255.255.255.0	Configures IP address
Router1(config-if-serial)#clock rate 128000	Provides clock
Router1(config-if-serial)#exit	

Router2 configuration

Command	Task
Router2(config)#interface s0	Enters the interface S0
Router2(config-if-serial0)#physical-layer sync	The physical layer works in synchronous mode. (Related to the partner)
Router2(config-if-serial0)#encapsulation ppp	Encapsulates PPP protocol
Router2(config-if-serial0)#ip address 3.3.3.2 255.255.255.0	Configures an IP address
Router2(config-if-serial0)#ppp pap sent-username goat password Signamax	Configures the negotiated user name and related password
Router2(config-if-serial0)#exit	

Configuring CHAP authentication:



Router1 configuration:

Command	Description
router1#configure terminal	
router1(config)# user mp2 password 0 signamax	Configure peer user name and password
router1(config)# interface serial0/0	Enter interface
router1(config-if-serial0/0)# physical-layer sync	Configure interface as synchronous
router1(config-if-serial0/0)# clock rate 128000	Configure line clock
router1(config-if-serial0/0)# encapsulation ppp	Encapsulate PPP protocol
router1(config-if-serial0/0)# ppp authentication chap	Configure chap authentication
router1(config-if-serial0/0)# ppp chap hostname mp1	Configure authentication user name
router1(config-if-serial0/0)# ip address 3.3.3.1 255.0.0.0	Configure IP address
router1(config-if-serial0/0)# exit	

Router2 configuration:

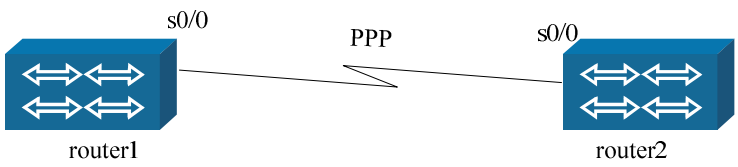
Command	Description
router2#configure terminal	
router2(config)#user mp1 password 0 signamax	Configure peer user name and password
router2(config)#interface serial0/0	Enter interface
router2(config-if-serial0/0)#physical-layer sync	Configure interface as synchronous
router2(config-if-serial0/0)#encapsulation ppp	Encapsulate PPP protocol
router2(config-if-serial0/0)#ppp chap hostname mp2	Configure authentication user name
router2(config-if-serial0/0)#ip address 3.3.3.2 255.0.0.0	Configure IP address
router2(config-if-serial0/0)#exit	

Monitoring & Debugging PPP Information

Command	Description
show ppp information (Display PPP information)	serial2 LCP Stats LCP phase ESTABLISH LCP state REQUEST SENT lcp echo timer OFF IPCP Stats IPCP state INITIAL NDSPCP Stats NDSPCP state INITIAL PAP Stats client PAP state INITIAL server PAP state INITIAL CHAP Stats client CHAP state INITIAL server CHAP state INITIAL
Router#show ppp multilink	Displays PPP multilink status information
Router#show ppp version	Displays PPP version information
Router#debug ppp negotiation [serial serial-number]	Opens debugging PPP negotiation information and use this command to see the compression information such as tcprtppredictor and stacker
Router#debug ppp header serial serial-number	Opens debugging header information of packets when PPP is negotiated
Router#debug ppp packer serial serial-number	Opens debugging PPP receiving/sending messages information
Router#show compress XXX	Displays compressed information

PPP Address Negotiation & Address Pool

In order to simplify the equipment and manage easily, the address negotiation is adopted for lower equipment while the address pool is used for distribute-address of upper equipment.



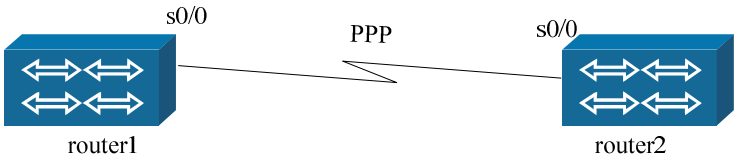
Router1 configuration

Command	Description
router#configure terminal	Enter global configuration mode
router(config)#interface serial0/0	Enter interface
router(config-if-serial0/0)#physical-layer sync	Physical layer operating mode is synchronous.
router(config-if-serial0/0)#clock rate 64000	Configure clock
router(config-if-serial0/0)#encapsulation ppp	Encapsulate link layer protocol PPP
router(config-if-serial0/0)# ip address 3.3.3.1 255.0.0.0	Configure network layer ip address
router(config-if-serial0/0)#peer defaut ip address 3.3.3.2	Designate peer ip address
router(config-if-serial0/0)#exit	

Router2 configuration:

Command	Description
router#configure terminal	Enter global configuration mode
router(config)#interface serial0/0	Enter interface
router(config-if-serial0/0)#physical-layer sync	Physical layer operating mode is synchronous.
router(config-if-serial0/0)#encapsulation ppp	Encapsulate link layer protocol PPP
router(config-if-serial0/0)#ip address negotiated	Configure address negotiation
router(config-if-serial0/0)#exit	

In the large-scale dial access network, in order to distribute address to lower end equipment, use local address pool.



The routers router1 and router2 connect with each other via S0, encapsulate the PPP protocol, and an address pool is configured in router1 (Users can also configure a default address pool). In router2 the address negotiation is configured to learn the IP address distributed by the opposite router.

Router1 configuration:

Command	Task
Router(config)#ip local pool goat 10.0.0.2 10.0.0.10	Defines an address pool called goat with network addresses from 10.0.0.2 to 10.0.0.10
Router(config)#interface serial0	Enters the interface S0
Router(config-if-serial0)#physical-layer sync	Configures it as the synchronous mode
Router(config-if-serial0)#clock rate 128000	Configures the clock rate
Router(config-if-serial0)#encapsulation ppp	Encapsulates the PPP protocol
Router(config-if-serial0)#peer default ip address pool goat	Designates the opposite terminal to use the addresses in address pool goat (distribute addresses from big to small)
Router(config-if-serial0)#ip address 10.0.0.11 255.0.0.0 Router(config-if-serial0)#exit	Configures the IP address

Router2 configuration:

Command	Task
Router(config)#interface serial0	Enters the interface
Router(config-if-serial0)#physical-layer sync	Configures it as the synchronous mode
Router(config-if-serial0)#encapsulation ppp	Encapsulates PPP protocol
Router(config-if-serial0)#ip address negotiated	Uses address negotiation to negotiate IP addresses distributed by the opposite terminal
Router(config-if-serial0)#end	

If you want to use a default address pool, you should first configure the default address pool, and then enable it. After ip add negotiated is configured on the opposite router, it will work. If ip address-pool local is configured in the global configuration mode, then all the interfaces will use the default address pool, and then it is unnecessary to configure peer default ip address pool.

If you want to use a given address pool, you should first configure the given address pool, and then configure peer default ip address pool-name on the given interface.

PPP Multilink

PPP multilink binding can be used to provide load balance for dialup lines (PSTN/ISDN) or synchronous lines, enhance line via put and reduce the transmission delay among systems. By means of the PPP multilink binding, a packet can be divided into multiple slices, which can be transmitted over the multiple parallel links and then can be restored to the original packet orderly.

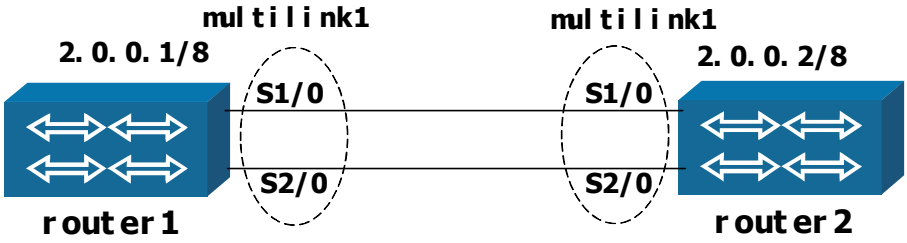
The PPP multilink supports three binding modes: multilink, dialer and BRI. Dialer and logical interface multilink modes are applied to the binding of physical interfaces, and the BRI mode is applied to the binding of B channels (MP router can also support the binding of two ISDN B channels.). The three binding modes support related network modes.

The multilink-binding mode: the mode is generally applied to synchronous line binding (such as DDN and SDH) instead of dialup line binding (such as PSTN and ISDN).

The dialer-binding mode: the mode is generally applied to the PSTN dialup line binding instead of the ISDN dialup line binding. Besides that, the mode can also be applied to the synchronous line binding, but it is not recommended.

The BRI binding mode: when the multilink is adopted, the mode can be applied to nothing but the binding of two B channels of ISDN dialup line.
The following three examples are given for the foregoing three kinds of multilink binding modes.

Multilink binding mode:



Two private lines are adopted for the connection of Router1 and Router2. To use PPP multilink, you should establish a multilink interface for Router1 and Router2 and bind the physical interfaces to the multilink interface.

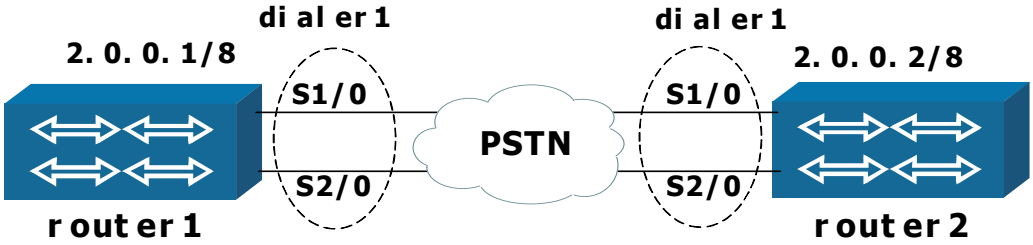
The multilink interface of router1 is configured as follows:(related configuration of router2 is similar to that of router1)

Syntax	Description
router1#configure terminal	Enter the global configuration mode
router1(config)#int multilink1	Create a multilink logical interface multilink1
router1(config-if-multilink1)#ip add 2.0.0.1 255.0.0.0	Configure the IP address
router1(config-if- multilink1)#encapsulation ppp	Enable the PPP protocol
router1(config-if- multilink1)#ppp multilink	Enable the PPP multilink

The physical interface of router1 is configured as follows:(related configuration of router2 is similar to that of router1)

Syntax	Description
router1(config)#int s1/0	Enter an interface
router1(config-if-serial1/0)# encapsulation ppp	Encapsulate the PPP protocol
router1(config-if-serial1/0)#multilink-group 1	Relate the physical interface with the multilink interface
router1(config-if-serial1/0)#physical-layer sync	Configure the synchronous mode
router1(config)#int s2/0	Enter an interface
router1(config-if-serial2/0)# encapsulation ppp	Encapsulate the PPP protocol
router1(config-if-serial2/0)#multilink-group 1	Relate the physical interface with multilink interface
router1(config-if-serial2/0)#physical-layer sync	Configure the synchronous mode

Dialer binding mode:



Two physical interfaces (frequency-band modem interface or serial interface adopts the external modem mode) are adopted for the connection of Router1 and Router2. To use PPP multilink, you should establish a dialer interface for Router1 and Router2 and bind the physical interfaces to the dialer interface.

The dialer interface of Router1 is configured as follows. (The configuration of the dialer interface on Router2 is similar to that of Router1.)

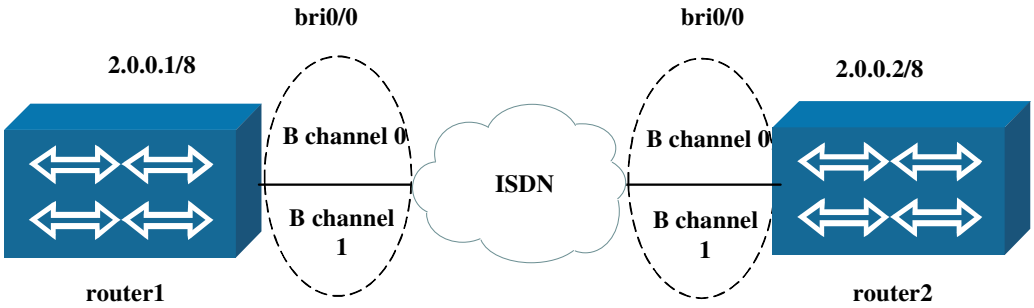
Syntax	Description
router1#configure terminal	Enter the global configuration mode
router1(config)#dialer-list 1 protocol ip permit	Define a dialer-list
router1(config)#int dialer1	Create a dialer interface dialer1
router1(config-if-dialer1)#ip add 2.0.0.1 255.0.0.0	Configure the IP address
router1(config-if-dialer1)#encapsulation ppp	Enable the PPP protocol
router1(config-if-dialer1)#dialer in-band	Enable DDR of the interface
router1(config-if-dialer1)#dialer-group 1	Define an access group for access control
router1(config-if-dialer1)#ppp multilink	Enable the PPP multilink
router1(config-if-dialer1)#dialer string	Configure the phone number for dialer (two phone numbers need be configured for two lines)
router1(config-if-dialer1)#dialer load-threshold	Specify the load-threshold (such as 1) for the dialer

The physical interface of Router1 is configured as follows. The configuration of the physical interface on Router2 is similar to that of Router1.

Syntax	Description
router1(config)#int s1/0	Enter an interface
router1(config-if-serial1/0)# encapsulation ppp	Encapsulate the PPP protocol
router1(config-if-serial1/0)#dialer rotary-group 1	Relate the physical interface with the dialer interface
router1(config-if-serial1/0)#physical-layer async	Configure the asynchronous mode (Generally, PSTN adopts the asynchronous modes)
router1(config)#int s2/0	Enter an interface
router1(config-if-serial2/0)# encapsulation ppp	Encapsulate the PPP protocol
router1(config-if-serial2/0)#dialer rotary-group 1	Relate the physical interface with the dialer interface
router1(config-if-serial2/0)#physical-layer async	Configure the asynchronous mode (Generally, PSTN adopts the asynchronous modes)

The above is the basic configuration of the modem. If the interface adopts the external modem mode, modem out need still be configured on the serial-interface more.

BRI binding mode:



One ISDN line is employed for Router1 and Router2 to access ISDN. Two B channels of the line are bound together for a PPP multilink. By default, two B channels are bound with the BRI interface. The BRI binding mode needs no manual configuration of the binding of two B channels and the BRI interface.

The BRI interface of Router1 is configured as follows. The configuration of the BRI interface on Router2 is similar to that of Router1.

Syntax	Description
router1#configure terminal	Enter the global configuration mode
router1(config)#dialer-list 1 protocol ip permit	Define a dialer-list
router1(config)#int bri0/0	Enter the BRI interface
router1(config-if- bri0/0)#ip add 2.0.0.1 255.0.0.0	Configure the IP address
router1(config-if- bri0/0)#encapsulation ppp	Enable the PPP protocol
router1(config-if- bri0/0)#dialer in-band	Enable the interface DDR
router1(config-if- bri0/0)#dialer-group 1	Define an access group for access control
router1(config-if- bri0/0)#ppp multilink	Enable the PPP multilink
router1(config-if- bri0/0)#dialer string	Configure an ISDN number for dialup
router1(config-if- bri0/0)#dialer load-threshold	Specify the load-threshold (such as 1) for the dialer

PPP Data Compression

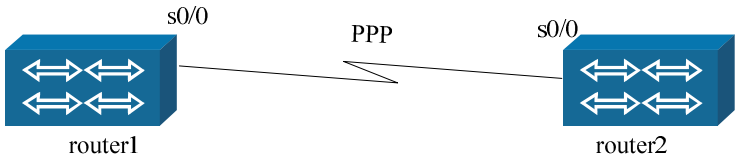
Signamax routers can use compression to optimize its performance and then can provide higher data viaput capacity.

The compression modes supported by Signamax routers are as follows:

Predictor - uses the index method to forecast the next character sequence of the data stream according to the compression dictionary; it can first judge whether the data is compressed. If the data has been compressed, it will be sent out at once and the system does not waste time to compress the data that has been compressed.

Stacker is a compression method based on Lempel-Ziv(LZ). It sends each kind of data only one time, and then only sends information about each kind of data that is located in the data stream. The receiver can assemble the data stream again int understandable information. TCP/IP Header Compression----is employed to compress the length of TCP/IP header。

RTP Compression - is employed to compress the real-time voice data.



The predictor compression is adopted for connection of the port S1/0(3.3.3.1) of the local router router1 and the port S1/0 (3.3.3.2) of the opposite router router2.

Both sides should be compressed.

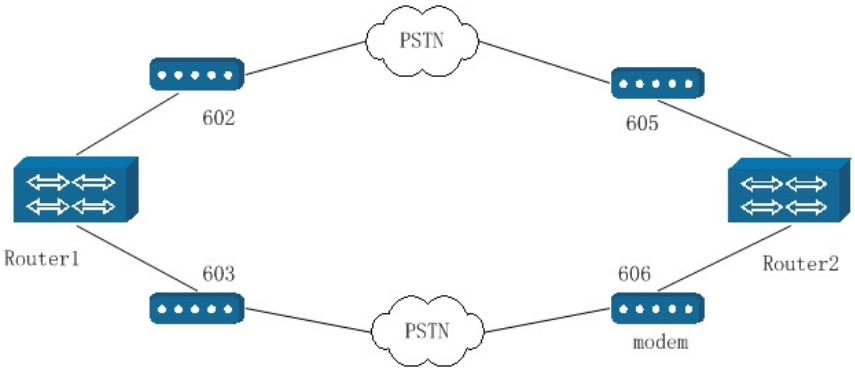
Router1 configuration:

Syntax	Description
router1#configure terminal	Enter the global configuration mode
router1(config)#interface s1/0	Enter the interface S1/0
router1(config-if-serial1/0)#physical-layer sync	The physical layer operates in the synchronous mode
router1(config-if-serial1/0)#encapsulation ppp	Encapsulate the link-layer protocol PPP
router1(config-if-serial1/0)#ppp compress predictor	Configure the predictor compression
router1(config-if-serial1/0)#ip address 3.3.3.1 255.0.0.0	Configure the IP address
router1(config-if-serial1/0)#clock rate 128000	Provide the clock rate
router1(config-if-serial1/0)#exit	

Router2 configuration:

Syntax	Description
router2(config)#interface s1/0	Enter the interface S1/0
router2(config-if-serial1/0)#physical-layer sync	The physical layer operates in the synchronous mode (related with the opposite end)
router2(config-if-serial1/0)#encapsulation ppp	Encapsulate the PPP protocol
router1(config-if-serial1/0)#ppp compress predictor	Configure the predictor compression
router2(config-if-serial1/0)#ip address 3.3.3.2 255.0.0.0	Configure the IP address
router2(config-if-serial1/0)#exit	

PPP BACP Configuration



Router1 and router2 are connected together via two PSTN lines, and DDR dialup is configured for them. There are two phone numbers 602 and 603 on the side of router1, and there are two phone numbers 605 and 606 on the side of router2.

The aim of the example is that the second dialup line will be activated when the traffic of the first dialup line arrives at some specified value.

BAP is configured on the BRI interface:

Router1 is configured as follows:

Command	Task
router1# configure terminal	
router1(config)# user router2 password 0 signamax	
router1(config)# dialer-list 1 protocol ip permit	
router1(config)# interface bri0/0	
router1(config-if-bri0/0)#ip address 12.1.1.2 255.0.0.0	
router1(config-if-bri0/0)# dialer in-band	Activate the DDR dialup 起用 DDR.
router1(config-if-bri0/0)# dialer idle-timeout 20	
router1(config-if-bri0/0)# dialer fast-idle 2000	
router1(config-if-bri0/0)# dialer enable-timeout 20	
router1(config-if-bri0/0)# dialer map ip 12.1.1.1 name router2 broadcast 605	
router1(config-if-bri0/0)# dialer load-threshold 14 outbound	Set the link load threshold as 14/255 so that the second link will be activated when the link load exceeds the threshold.
router1(config-if-bri0/0)# dialer-group 1	
router1(config-if-bri0/0)# encapsulation ppp	
router1(config-if-bri0/0)# ppp multilink bap	Negotiate BACP and BAP on the multilink.
router1(config-if-bri0/0)# ppp authentication chap	
router1(config-if-bri0/0)# ppp chap hostname router1	
router1(config-if-bri0/0)# ppp bap call request	Sent the BAP call request when some links need be added.
router1(config-if-bri0/0)# ppp bap link types isdn	Set the type of the multilink as ISDN.
router1(config-if-bri0/0)# ppp bap number default 602	Set the default dialup string (the local number, used for the dialup of the opposite end)
router1(config-if-bri0/0)# ppp bap number secondary 603	Set the secondary dialup string (configured only on the BRI interface and applied to the opposite end)
router1(config-if-bri0/0)# ppp bap drop after-retries	Directly delete the link instead of sending BAP distconnection request. (directly send LCP interrupt request)

B) Router1 2s configured as follows:

Command	Task
router2# configure terminal	
router2(config)# user router1 password 0 signamax	
router2(config)# dialer-list 1 protocol ip permit	
router2(config)# interface bri0/0	
router2(config-if-bri0/0)#ip address 12.1.1.1 255.0.0.0	
router2(config-if-bri0/0)# dialer in-band	Active the DDR dialup
router2(config-if-bri0/0)# dialer idle-timeout 20	
router2(config-if-bri0/0)# dialer fast-idle 2000	
router2(config-if-bri0/0)# dialer enable-timeout 20	
router2(config-if-bri0/0)# dialer map ip 12.1.1.2 name router1 broadcast 602	
router2(config-if-bri0/0)# dialer load-threshold 14 outbound	Configure the link load
router2(config-if-bri0/0)# dialer-group 1	
router2(config-if-bri0/0)# encapsulation ppp	
router2(config-if-bri0/0)# ppp multilink bap	Negotiate BACP and BAP on the multilink
router2(config-if-bri0/0)# ppp authentication chap	
router2(config-if-bri0/0)# ppp chap hostname router2	
router2(config-if-bri0/0)# ppp bap call accept	Receive the BAP call of the opposite end. (it is the default configuration and can be omitted.)
router2(config-if-bri0/0)# ppp bap link types isdn	
router2(config-if-bri0/0)# ppp bap number default 605	
router2(config-if-bri0/0)# ppp bap number secondary 606	
router2(config-if-bri0/0)# ppp bap drop after-retries	

BAP is configured on the serial interface:

A) Router1 is configured as follows:

Command	Task
router1# configure terminal	
router1(config)# user router2 password 0 signamax	
router1(config)# dialer-list 1 protocol ip permit	
router1(config)# interface dialer0	Create a logical dialer interface.
router1(config-if-dialer0)# ip address 12.1.1.2 255.0.0.0	
router1(config-if-dialer0)# dialer idle-timeout 20	
router1(config-if-dialer0)# dialer fast-idle 2000	
router1(config-if-dialer0)# dialer enable-timeout 20	
router1(config-if-dialer0)# dialer in-band	
router1(config-if-dialer0)# Dialer string 605	The opposite-end number used to activate the first link.
router1(config-if-dialer0)# dialer load-threshold 14 outbound	Configure the link load.
router1(config-if-dialer0)# dialer-group 1	
router1(config-if-dialer0)# encapsulation ppp	
router1(config-if-dialer0)# ppp multilink bap	Negotiate BACP and BAP on the multilink.
router1(config-if-dialer0)# ppp authentication chap	
router1(config-if-dialer0)# ppp chap hostname router1	
router1(config-if-dialer0)# ppp bap callback request	Sent the BAP callback request when a link need be added.
router1(config-if-dialer0)# ppp bap link types analog	Set the type of the multilink as analog.
router1(config-if-dialer0)# ppp bap drop after-retries	Directly delete the link instead of sending BAP disconnection request (directly send LCP interrupt request)
router1(config-if-dialer0)# interface s1/0	Enter the configuration mode of the physical interface.
router1(config-if-Serial1/0)# physical-layer async	
router1(config-if-Serial1/0)# encapsulation ppp	
router1(config-if-Serial1/0)# dialer rotary-group 0	Subject to the logical interface dialer0.
router1(config-if-Serial1/0)# ppp bap number default 602	The dialup string provided for the opposite end.
router1(config-if-Serial1/0)# interface s2/0	
router1(config-if-Serial2/0)# physical-layer async	
router1(config-if-Serial2/0)# encapsulation ppp	
router1(config-if-Serial2/0)# dialer-rotary-group 0	Subject to the logical interface dialer0.
router1(config-if-Serial2/0)# ppp bap number	The dialup string provided for the

default 603	opposite end.

B) Router 2 is configured as follows:

Command	Task
router2# configure terminal	
router2(config)# user router1 password 0 signamax	
router2(config)# dialer-list 1 protocol ip permit	
router2(config)# interface dialer0	
router2(config-if- dialer0)# ip address 12.1.1.2 255.0.0.0	
router2(config-if-dialer0)# dialer idle-timeout 20	
router2(config-if-dialer0)# dialer fast-idle 2000	
router2(config-if-dialer0)# dialer enable-timeout 20	
router2(config-if-dialer0)# dialer in-band	
router2(config-if-dialer0)# Dialer string 602	The opposite-end number used to activate the first link
router2(config-if-dialer0)# dialer load-threshold 14 outbound	Configure the link load
router2(config-if-dialer0)# dialer-group 1	
router2(config-if-dialer0)# encapsulation ppp	
router2(config-if-dialer0)# ppp multilink bap	Negotiate BACP and BAP on the multilink
router2(config-if-dialer0)# ppp authentication chap	
router2(config-if-dialer0)# ppp chap hostname router2	
router2(config-if-dialer0)# ppp bap callback accept	Receive the BAP callback request (By default)
router2(config-if-dialer0)# ppp bap link types analog	Set the type of the multilink as analog
router2(config-if-dialer0)# ppp bap drop after-retries	
router2(config-if-dialer0)# interface s1/0	
router2(config-if-Serial1/0)# physical-layer async	
router2(config-if-Serial1/0)# encapsulation ppp	
router2(config-if-Serial1/0)# dialer rotary-group 0	Subject to the logical interface dialer0
router2(config-if-Serial1/0)# ppp bap number default 605	The dialup string provided for the opposite end
router2(config-if-Serial1/0)# interface s2/0	
router2(config-if-Serial2/0)# physical-layer async	
router2(config-if-Serial2/0)# encapsulation ppp	
router2(config-if-Serial2/0)# dialer-rotary-group 0	Subject to the logical interface dialer0
router2(config-if-Serial2/0)#ppp bap number	

default 606	

BACP monitoring and debugging

`show ppp bap group`

To display the configuration and operation status of a multilink bundle, use the command show ppp bap group.

`show ppp bap group`

Syntax	Description
Group	Display BAP group information

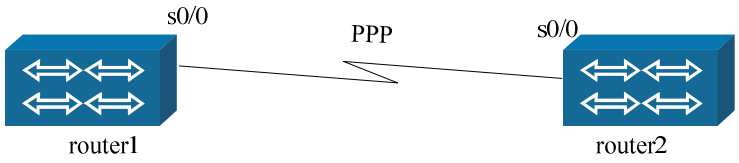
(Command mode) the privileged configuration mode

`show ppp multilink`

To display information about multilink PPP bundle, use the command show ppp multilink.

(Command mode) the privileged configuration mode

PPP Supports MPLS



Router1 and router2 are connected directly in the MPLS core network.

Router1 is configured as follows.

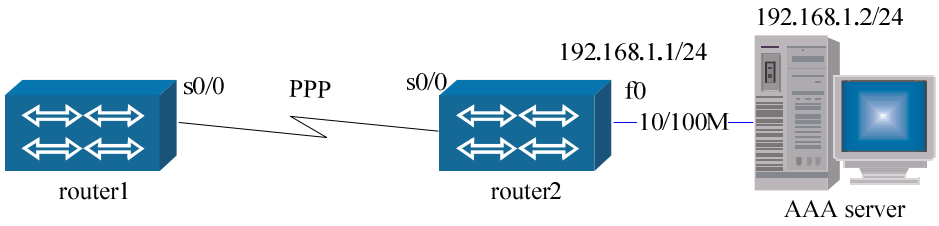
Syntax	Description
router1#configure terminal	Enter the global configuration mode
router1(config)#interface s1/0	Enter the interface S1/0
router1(config-if-serial1/0)#physical-layer sync	The physical layer operates in the synchronous mode
router1(config-if-serial1/0)#encapsulation ppp	Encapsulate the link-layer protocol PPP
router1(config-if-serial1/0)#ppp mpls	Configure PPP to support MPLS
router1(config-if-serial1/0)#mpls ip	Configure an interface to support MPLS
router1(config-if-serial1/0)#ip address 3.3.3.1 255.0.0.0	Configure the IP address
router1(config-if-serial1/0)#clock rate 128000	Provide clock rate
router1(config-if-serial1/0)#exit	

Router2 is configured as follows.

Syntax	Description
router2(config)#interface s1/0	Enter the interface S1/0.
router2(config-if-serial1/0)#physical-layer sync	The physical layer operates in the synchronous mode (related with the opposite end)
router2(config-if-serial1/0)#encapsulation ppp	Encapsulate the PPP protocol
router1(config-if-serial1/0)#ppp mpls	Configure PPP to support MPLS
router1(config-if-serial1/0)#mpls ip	Configure an interface to support MPLS
router2(config-if-serial1/0)#ip address 3.3.3.2 255.0.0.0	Configure the IP address

router2(config-if-serial1/0)#exit	

PPP Supports AAA Authorization



router1 S0/0(3.3.3.1) connects to router2 S0/0 (3.3.3.2),using PAP authentication.

AAA server address is 192.168.1.2, router2 192.168.1.1 is in the same LAN. Address user name, password and authorized IP address on AAA server.

router1 configuration:

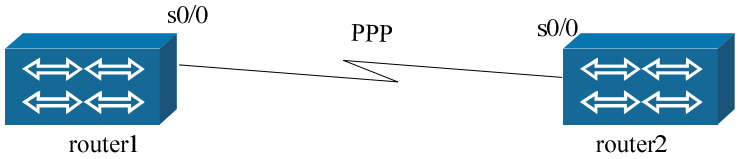
Command	Description
router1#configure terminal	Enter global configuration mode
router1(config)#interface serial0/0	Enter the interface
router1(config-if-serial0/0)#physical-layer sync	The physical layer operates in the synchronous mode
router1(config-if-serial0/0)#encapsulation ppp	Encapsulate link layer PPP
router1(config-if-serial0/0)#ppp pap sent-username signamax password a	Configure authentication user name and password
router1(config-if-serial0/0)#ip address negotiated	Configure ip address
router1(config-if-serial0/0)#clock rate 128000	Provide the clock
router1(config-if-serial0/0)#exit	

router2 configuration:

Command	Description
router2(config)#aaa new-model	Enable AAA function
router2(config)#aaa authentication ppp aaa-authen radius	Configure AAA authentication name aaa-authen and type radius
router2(config)# aaa authorization network aaa-author radius	Configure AAA authentication name aaa-authen and type radius
router2(config)# radius-server host 192.168.1.2 auth-port 1645 acct-port 1646 priority 0 key signamax	Configure radius server address and key
router2(config)#interface fastethernet0	Enter the interface

router2(config-if-fastethernet0)#ip address 192.168.1.1 255.255.255.0	Configure IP address
router2(config-if-fastethernet0)#exit	
router2(config)#interface serial0/0	Enter the interface
router2(config-if-serial0/0)#physical-layer sync	The physical layer operates in the synchronous mode.(Related with the opposite end)
router2(config-if-serial0/0)#encapsulation ppp	Encapsulate PPP
router2(config-if-serial0/0)#ip address 3.3.3.2 255.0.0.0	Configure IP address
router2(config-if-serial0/0)#ppp authentication pap aaa-authen	Enable AAA PAP authentication
router2(config-if-serial0/0)#ppp authorization aaa-author	Enable AAA authentication
router2(config-if-serial0/0)#exit	

PPP Encryption



The DES encryption is adopted for the connection of the port S1/0(3.3.3.1) of the local router router1 and the port S1/0 (3.3.3.2) of the opposite router router2.

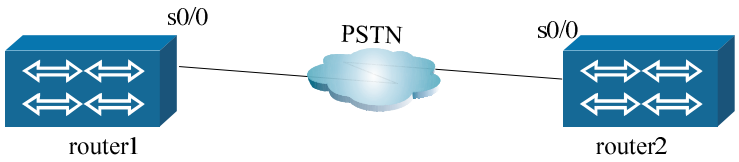
Router1 is configured as follows.

Syntax	Description
router1#configure terminal	Enter the global configuration mode
router1(config)#interface s1/0	Enter the interface S1/0
router1(config-if-serial1/0)#physical-layer sync	The physical layer operates in the synchronous mode
router1(config-if-serial1/0)#encapsulation ppp	Encapsulate the link-layer protocol PPP
router1(config-if-serial1/0)#ppp encrypt des 123	Configure the DES encryption key (should be consistent with that of the opposite end)
router1(config-if-serial1/0)#ip address 3.3.3.1 255.0.0.0	Configure the IP address
router1(config-if-serial1/0)#clock rate 128000	Provide the clock rate
router1(config-if-serial1/0)#exit	

Router2 is configured as follows.

Syntax	Description
router2(config)#interface s1/0	Enter the interface S1/0
router2(config-if-serial1/0)#physical-layer sync	The physical layer operates in the synchronous mode (related with the opposite end)
router2(config-if-serial1/0)#encapsulation ppp	Encapsulate the PPP protocol
router1(config-if-serial1/0)#ppp encrypt des 123	Configure the DES encryption key (should be consistent with that of the opposite end)
router2(config-if-serial1/0)#ip address 3.3.3.2 255.0.0.0	Configure the IP address
router2(config-if-serial1/0)#exit	

PPP Callback



router1 connects router2 via PSTN dialing, router1 initiates callback requirement and router2 accepts the request.

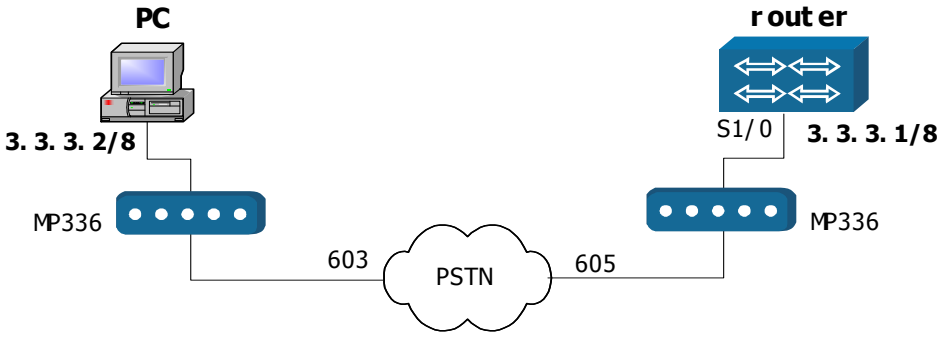
Router1 configuration:

Command	Description
router1#configure terminal	Enter configuration mode
router1(config)# dialer-list 1 protocol ip permit	Configure spring dial list
router1(config)# interface serial0/0	Enter the interface
router1(config-if-serial0/0)# physical-layer async	Configure asynchronous mode
router1(config-if-serial0/0)# speed 9600	Configure line rate
router1(config-if-serial0/0)# dialer in-band	Enable DDR dial
router1(config-if-serial0/0)# dialer-group 1	Enable spring dial list
router1(config-if-serial0/0)#encapsulation ppp	Encapsulate PPP protocol
router1(config-if-serial0/0)# ppp callback request	Configure callback request
router1(config-if-serial0/0)# ppp pap sent-name signamax password a	Configure user name and password
router1(config-if-serial0/0)# ip address 80.1.1.1 255.255.255.0	Configure IP address
router1(config-if-serial0/0)# dialer string 601	Configure dialer number
router1(config-if-serial0/0)#exit	

router2 configuration:

Command	Description
router2#configure terminal	Enter configuration mode
router2 (config)# dialer-list 1 protocol ip permit	Configure spring dial list
router2 (config)# user signamax password 0 a	Configure user name and password
router2 (config)# map-class dialer a	Produce a callback mapping type
router2 (config)# dialer callback-server	Enable callback server
router2 (config)# interface serial0/0	Enter the interface
router2 (config -if-serial0/0)# physical-layer async	Configure asynchronous mode
router2 (config -if-serial0/0)# speed 9600	Configure line rate
router2 (config -if-serial0/0)# dialer in-band	Enable DDR dial
router2 (config -if-serial0/0)# encapsulation ppp	Encapsulate PPP protocol
router2 (config -if-serial0/0)#ppp authentication pap	Enable PAP authentication
router2 (config -if-serial0/0)#ip address 80.1.1.2 255.0.0.0	Configure IP address
router2 (config -if-serial0/0)#dialer callback-secure	Configure callback strategy
router2 (config -if-serial0/0)#dialer-group 1	Enable spring dialer list
router2 (config -if-serial0/0)#ppp callback accept	Configure callback acceptance
router2 (config -if-serial0/0)# dialer map ip 80.1.1.1 name signamax 605 class a	Configure DDR MAP for callback
router2 (config -if-serial0/0)#exit	

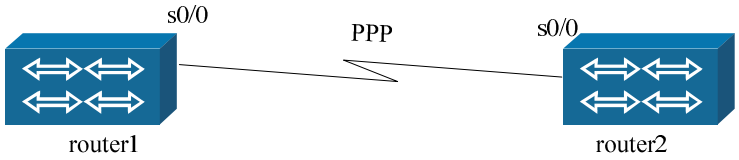
Negotiate DNS & WINS over PPP



PC connects to the router via the PSTN dialer, and the router allocates DNS, WINS address and an IP address to PC. The router is configured as follows:

Syntax	Description
router1#configure terminal	Enter the global configuration mode
router1(config)#interface s1/0	Enter the interface S1/0
router1(config-if-serial1/0)#physical-layer async	The physical layer operates in the asynchronous mode
router1(config-if-serial1/0)#encapsulation ppp	Encapsulate the link-layer protocol PPP
router1(config-if-serial1/0)#modem out	Set the external MODEM mode
router1(config-if-serial1/0)#ip address 3.3.3.1 255.0.0.0	Configure the IP address
router1(config-if-serial1/0)# peer default ip address 3.3.3.2	Allocate an IP address to PC
router1(config-if-serial1/0)#ppp ipcp dns 1.1.1.1 1.1.1.2	Allocate DNS address to PC
router1(config-if-serial1/0)#ppp ipcp wins 2.1.1.1 2.1.1.2	Allocate WINS address to PC
router1(config-if-serial1/0)#exit	

Null Username CHAP Authentication Over PPP



To enhance security, some access systems will not send user name for chap; and at this time configure default password on peer equipment for identification.

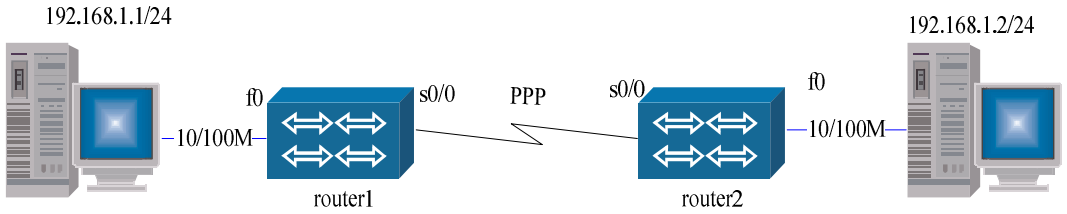
router1 configuration

Command	Description
router1#configure terminal	Enter the global configuration mode
router1(config)#interface serial0/0	Enter the interface
router1(config-if-serial0/0)#physical-layer sync	The physical layer operates in the asynchronous mode
router1(config-if-serial0/0)#encapsulation ppp	Encapsulate link layer protocol PPP
router1(config-if-serial0/0)#ip address 3.3.3.1 255.0.0.0	Configure the IP address
router1(config-if-serial0/0)#ppp chap hostname abc	Configure the user name of access system
router1(config-if-serial0/0)#ppp chap password 123	Configure the password of the access system
router1(config-if-serial0/0)#exit	

router2 configuration:

Command	Description
router1#configure terminal	Enter the global configuration mode.
router1(config)#user abc password 0 123	Configure user name and password
router1(config)#interface serial0/0	Enter the interface
router1(config-if-serial0/0)#physical-layer sync	The physical layer operates in the asynchronous mode.
router1(config-if-serial0/0)#encapsulation ppp	Encapsulate link layer protocol PPP
router1(config-if-serial0/0)#ip address 3.3.3.2 255.0.0.0	Configure the IP address.
router1(config-if-serial0/0)# ppp authentication chap	Configure CHAP authentication
router1(config-if-serial0/0)#ppp chap hostname router1	Configure hostname
router1(config-if-serial0/0)# no ppp chap send-hostname	Designate not sending local user name for CHAP negotiation
router1(config-if-serial0/0)#exit	

Signamax router forwards data between PPP interface and Ethernet interface via PPP Bridge.



1, router1 connects routers via S0/0, with PPP protocol;

Router1 S0/0(3.3.3.1) connects router2 S0/0 (3.3.3.2);

The f0 of router1 and router2 access to the same Ethernet network.

router1 configuration:

Command	Description
router1(config)#int serial0/0	Enter the interface
router1(config-if-serial0/0)#physical-layer sync	Configure synchronous mode
router1(config-if-serial0/0)#clock rate 128000	Configure the clock
router1(config-if-serial0/0)#encapsulation ppp	Encapsulate PPP protocol
router1(config-if-serial0/0)# ppp bridge ip	Enable PPP bridge
router1(config-if-serial0/0)# bridge-group 1	Add s0/0 to network bridge group 1
router1(config-if-serial0/0)#exit	
router1(config)#interface fastethernet0	Enter f0 interface mode
router1(config-if-fastethernet0)# bridge-group	Add f0 to network bridge group 1

1	
router1(config-if-fastethernet0)#exit	

router2 configuration:

Command	Description
router2(config)#interface serial0/0	Enter the interface
router2(config-if-serial0/0)#encapsulation ppp	Encapsulate PPP protocol
router2(config-if-serial0/0)# physical-layer sync	Configure synchronous mode
router2(config-if-serial0/0)# ppp bridge ip	Enable PPP bridge
router2(config-if-serial0/0)# bridge-group 1	Add s1/0 to network bridge group 1
router2(config-if-serial0/0)#exit	
router2(config)#interface fastethernet0	Enter f0 interface mode
router2(config-if-fastethernet0)# bridge-group 1	Add f0 to network bridge group 1
router2(config-if-fastethernet0)#exit	

PPP bridge function only enables after the configuration of ppp bridge ip on interface;

After configuring ppp bridge ip on interface, the interface will be up, and no need to configure IP address.

HDLC Protocol

HDLC is a bit-oriented synchronous communication procedure developed by the International Standards Organization (ISO)(bit-oriented means that any combination of bits can be transmitted). From the point of link access, HDLC has several main subsets, such as LAP (Link Access Protocol), LAPB (Link Access Procedure Balanced)and LAPD(Link Access Procedure for D channel).

HDLC Commands

Command	Description	Configuration mode
encapsulation hdlc	*interface link layer encapsulating HDLC	config-if-××
keepalive [seconds]	Configure keepalive time interval	config-if-××
peer ip addr ipaddress	Designate peer IP address	config-if-××
compress stac	Configure stac compression	config-if-××
ip tcp header-compression [passive]	Configure TCP/IP head compression	config-if-××
ip tcp compression-connections number	Configure TCP/IP head compression connection number	config-if-××
ip rtp header-compression [passive]	Configure RTP head compression	config-if-××
bridge ip ipaddress port {client | server}	*bridge under HDLC and TCP/IP connection	config-if-××
bridge-group number	*add an interface to a bridge group	config-if-××

"*" before the command means it has configuration example description.

Configuration mode is config, config-if-××(interface name) config-××(protocol name) etc.

Encapsulation HDLC:
On interface, encapsulation link layer protocol is HDLC.
(Default status)LAN interface default link layer protocol is HDLC.

Keepalive:
Configure keepalive time interval; use no to disable the configuration.

```
keepalive [seconds]
no keepalive
```

Syntax	Description
seconds	Keepalive check time interval unit is second, and the range is 0～32767(configure 0 as not do keepalive check, the same as no keepalive) . If not input parameters, the keepalive time interval is configured as default.

(Default status)10 seconds

peer ip addr
Designate peer IP address. After this configuration, HDLC will not send address request. When physical layer is up and receives peer keepalive frame, the protocol is up (it is a compatible command, in some condition, we need to designate peer IP address by hand). Or use no format.

```
peer ip addr ipaddress
no peer ip addr
```

Syntax	Description
ipaddress	Designate peer IP address

(Default status)no designation

ip tcp header-compression
Configure TCP/IP head compression. Or use no format.

```
ip tcp header-compression [passive]
no ip tcp header-compression
```

Syntax	Description
passive	Configure the parameter, it is passive mode head compression, Which is passive mode. Only peer has compressed, itself can compress

(Default status)no definition
ip tcp compression-connections

Configure TCP/IP head compression connection number. Or use **no** format.

```
ip tcp compression-connections number
no ip tcp compression-connections
```

Syntax	Description
number	Head compression connection number, and the range is 3～255.

(Default status)16.

ip rtp header-compression
configure RTP head compression. Or use **no** format.

```
ip rtp header-compression [passive]
no ip rtp header-compression
```

Syntax	Description
passive	Configure the parameter, it is passive mode head compression, which is passive mode. Only peer has compressed, itself can] compress

(Default status)no definition

bridge ip

Bridge between HDLC and TCP/IP connection. Or use **no** format.

```
bridge ip ipaddress port {client | server}
no bridge ip ipaddress port
```

Syntax	Description
ipaddress	Bridge IP address
port	Bridge port number
client	Bridge client
server	Bridge server

(Default status)no definition

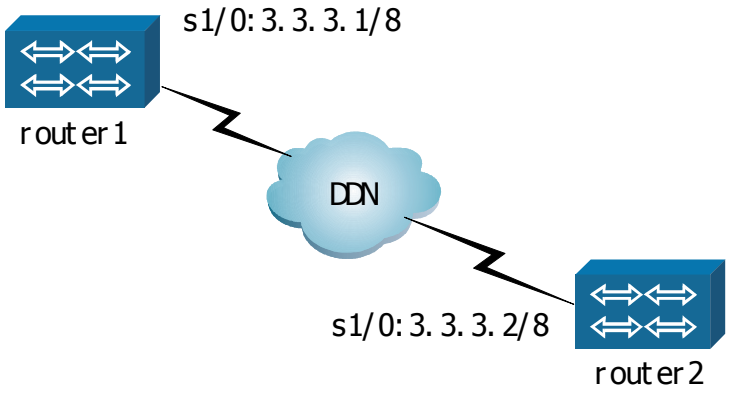
bridge-group
Add interface to a bridge group. Or use **no** format.

```
bridge-group number
no bridge-group number
```

Syntax	Description
number	Bridge group number, and the range is 1～63

(Default status)no definition

HDLC Configuration Example



As shown in the figure above, router1 and router2 connects to each other via serial port s0 and use HDLC protocol. The port S0 (3.3.3.1) of local router router1 connects to the port S0 (3.3.3.2) of the opposite router router2.

Router1 configuration:

router1(config)#int s1	Enters the interface configuration mode
router1(config-if-serial1)#ip add 1.0.0.1 255.0.0.0	Configures IP address
router1(config-if-serial1)#phy sync	Configures it as the synchronization mode
router1(config-if-serial1)#clock rate 128000	Configures clock
router1(config-if-serial1)#encapsulation hdlc	Configures the HDLC protocol

Router2 configuration:

router2(config-if-serial1)#encapsulation hdlc	Encapsulates the HDLC protocol
Router2(config-if-serial1)#phy sync	Configures it as the synchronization mode
Router2(config-if-serial1)#ip add 1.0.0.2 255.0.0.0	Configures the IP address

HDLC Debug Information

There are two main debug switches for HDLC, which can analyze the working situation of HDLC by comparing information in DEBUG with the frame format of HDLC. Turn on the debugging switch of the interface that encapsulates HDLC:

Router#

Command	Description
debug hdlc serial-number all	Display all the received/sending frames and contents of a whole frame on the interface that encapsulates HDLC
debug hdlc serial-number head	Display all the received/sending frames and contents of the frame headers on the interface that encapsulates HDLC

Configuring HDLC Bridge-connection Mode

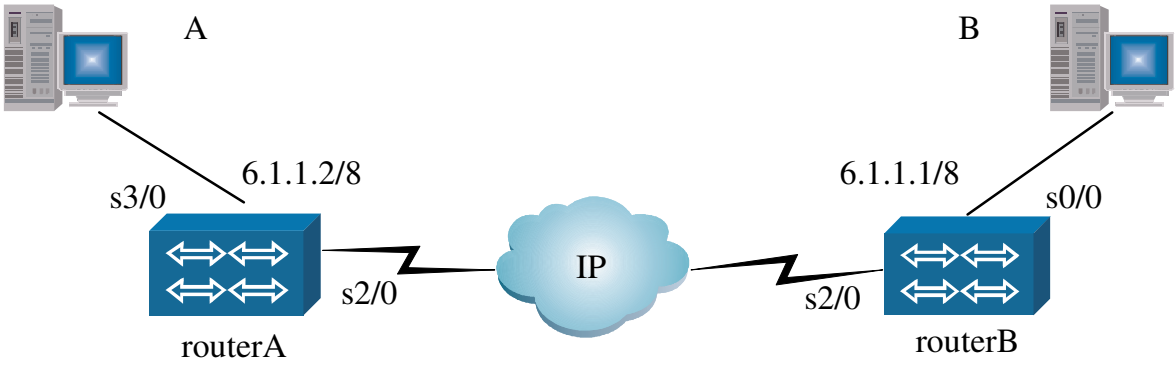
Signamax routers can be configured to work in HDLC bridge mode. In this mode the equipment connected together at the two ends of the bridge can transmit data transparently via the TCP/IP network.

From the viewpoint of users, the equipment at two ends of bridge was connected to each other via a pair of MODEMs would be connected to each other, while the intermediate TCP/IP network looks like a direct-cable.

Configuration command:
router(config-if-XXX)#

Command	Description
encapsulation hdlc	Encapsulate HDLC protocol
bridge ip <A.B.C.D> <bridge prot number> <client / server>	Configure bridge server address and bridge port number

Configuration example:



HDLC bridge configuration via the configuration showed in the above figure, the user PCs Equipment A and B connect on the both sides of the bridges to routerA and routerB, which can transmit data transparently across the TCP/IP network.

Configurations are as follows:

RouterA configuration:

Command	Task
routerA(config)#interface serial2	Enters the interface s2
routerA(config-if-serial2)#physical-layer sync	Configures it as synchronization mode
routerA(config-if-serial2)#encapsulation ppp	Encapsulates the PPP protocol
routerA(config-if-serial2)#ip address 6.1.1.2 255.255.255.252	Configures the IP address
routerA(config-if-serial2)#exit	Returns to the global configuration mode
routerA(config)#interface serial3	Enters the interface s3
routerA(config-if-serial3)#physical-layer sync	Encapsulates the synchronization mode
routerA(config-if-serial3)#clock rate 128000	Configures the clock as 128K
routerA(config-if-serial3)#encapsulation hdlc	Encapsulates HDLC protocol
routerA(config-if-serial3)#bridge ip 6.1.1.1 5000 client	The IP of the bridge-connection server, the port number 5000, Client end
routerA(config-if-serial3)#exit	Finishes configuration
Configuration of routerB	
Command	Task
routerB(config)#interface serial2	
routerB(config-if-serial2)# physical-layer sync	Configures it as the synchronization mode
routerB(config-if-serial2)#clock rate 128000	Configures the clock as 128K
routerB(config-if-serial2)#encapsulation ppp	Encapsulates the PPP protocol
routerB(config-if-serial2)#ip address 6.1.1.1 255.255.255.252	Configures the IP address
routerB(config-if-serial2)#exit	Exits from interface mode
routerB(config)#interface serial0	Enters the port s0 mode
routerB(config-if-serial0)#physical-layer sync	Configures it as synchronization mode
routerB(config-if-serial0)#encapsulation hdlc	Configures HDLC encapsulation
routerB(config-if-serial0)#bridge ip 6.1.1.1 5000 server	Configures the server with a port 5000
routerB(config-if-serial0)#exit	Finishes configuration

In the above configuration, the routerA is used as CLIent end while the routerB is used as the server end; both of the bridge port numbers are set as 5000. The s2 port of MprouterA and the s2 port of MprouterB connect to the TCP/IP network. The port s3 and port s0 are used as the interface of the bridge-connection to connect user equipment, and then they enable the user equipment to transmit data transparently via the TCP/IP network.

The command "show interface" allows users to examine the connection status of the bridge.

For example:

```
routerA#show interface serial3
serial (unit number 3):
     Flags: (0x80f0) DOWN POINT-TO-POINT MULTICAST RUNNING
     Type: HDLC
     Metric is 0
     Maximum Transfer Unit size is 1500
     0 packets received; 0 packets sent
     0 multicast packets received
     0 multicast packets sent
     5 input errors; 0 output errors
     0 collisions; 0 dropped
      hdlc version: v1.27
    hdlc bridge client: 6.1.1.1,5000, connect  The bridge is
at the status of connected.
      rxFrames 1744, rxChars 74436
      txFrames 1738, txChars 74410
      rxNoOctet 0, rxAbtErrs 0, rxCrcErrs 0
      rxOverrun 0, rxLenErrs 0, txUnderrun 0
      DCD=up  DSR=up  DTR=up  RTS=up  CTS=up  TxC=up
     rate=128000 bps
```

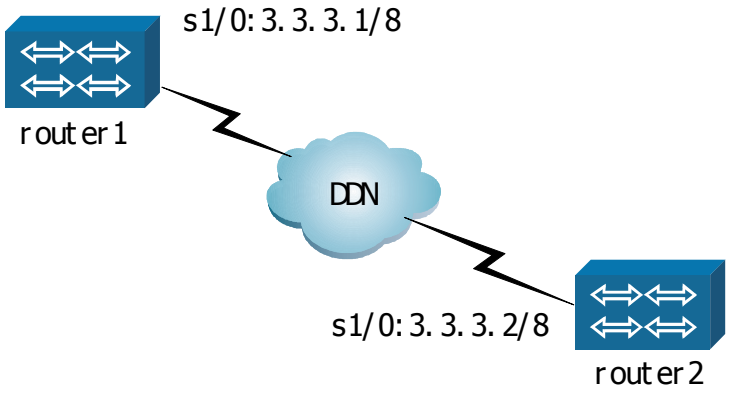
Configuring HDLC Bridge Ethernet

Signamax router forwards data between HDLC and Ethernet interface via configuring HDLC bridge Ethernet, used router as bridge.

```
Configuration command:
router(config-if-XXX)#
```

Command	Description
bridge-group <bridge-group number>	Add network interface to bridge group
no bridge-group <bridge-group number>	Delete network interface from bridge group

Configuration example:



Router1 connects router2 via s1/0, with HDLC protocol;
Router1 s1/0(3.3.3.1) connects router2 s1/0 (3.3.3.2);
The f0 of router1 and router2 connect to the same Ethernet network.

Router1 configuration

Command	Description
router1(config)#int s1/0	Enter s1/0 interface mode
router1(config-if-serial1/0)#ip add 3.3.3.1 255.0.0.0	Configure ip address
router1(config-if-serial1/0)#physical-layer sync	Configure synchronous mode
router1(config-if-serial1/0)#clock rate 128000	Configure clock
router1(config-if-serial1/0)#encapsulation hdlc	Encapsulate HDLC protocol
router1(config-if-serial1/0)#bridge-group 1	Add s1/0 to network bridge group 1
router1(config)#int f0	Enter f0 interface mode
router1(config-if-fastethernet0)#bridge-group 1	Add f0 to network group 1

Router2 configuration:

Command	Description
router2(config)#int s1/0	Enter s1/0 interface mode
router2(config-if-serial1/0)#encapsulation hdlc	Encapsulate HDLC protocol
router2(config-if-serial1/0)# physical-layer sync	Configure synchronous mode
router2(config-if-serial1/0)#ip add 3.3.3.2 255.0.0.0	Configure ip address
router2(config-if-serial1/0)#bridge-group 1	Add s1/0 to network bridge group 1
router2(config)#int f0	Enter f0 interface mode
router2(config-if-fastethernet0)# bridge-group 1	Add f0 to network group 1

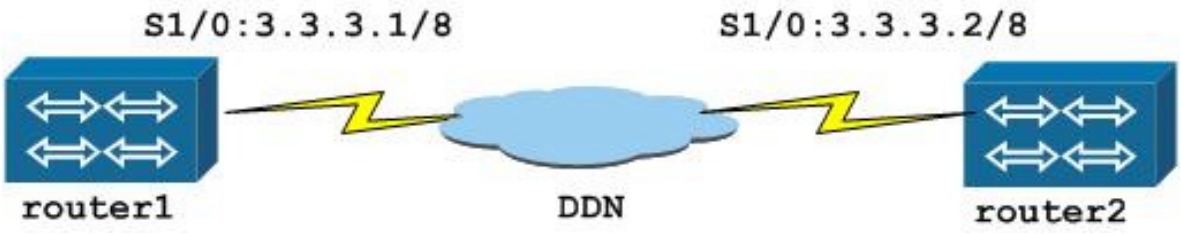
The HDLC Bridge Ethernet should be after IP address configuration on HDLC interface.

SLIP Protocol

SLIP is a kind of protocol widely used at present to transmit IP datagrams on a serial line. While it is a very practical standard while not an Internet standard. It is only a protocol used to encapsulate IP datagrams, and only defines the sequence of characters in the IP datagram that is encapsulated in the link layer frame format and is sent over a serial line, without providing the functions such as dynamical IP address distribution, datagram type identity, error checking/correction and data compression etc.

Configuration Example

SLIP configuration is simple, which generally comprises about several procedures: configuring the physical layer to asynchronous mode, the link layer encapsulating SLIP and peer IP address.



router1 and router2 connect to each other via serial port s0 and both run the SLIP protocol.

The configuration is as follows:

Router1 configuration:

Command	Task
router1(config)#int s0	Enters the interface configuration mode
router1(config-if-serial0)#phy async	The physical layer works in the asynchronous mode
router1(config-if-serial0)#enc slip	Encapsulates SLIP
router1(config-if-serial0)#ip address 3.3.3.1 255.255.255.0	Local IP address
router1(config-if-serial0)#peer ip address 3.3.3.2	Designates the IP address of the opposite terminal
router1(config-if-serial0)#speed 9600	Speed is 9600
router1(config-if-serial0)#databit 8	8 data bits
router1(config-if-serial0)#stopbit 1	1 stop bit
router1(config-if-serial0)#parity none	Parity none
router1(config-if-serial0)#flowctrl none	Without flow control

Router 2 configuration

Command	Task
Router2(config)#int s0	Enters the interface mode
Router2(config-if-serial0)#phy async	Configures the working mode as asynchronous
Router2(config-if-serial0)#enc slip	Encapsulates SLIP protocol
Router2(config-if-serial0)#speed 9600	Speed is 9600
Router2(config-if-serial0)#stopbit 1	1 stop bit
Router2(config-if-serial0)#databit 8	8 data bits
Router2(config-if-serial0)#ip address 3.3.3.2 255.255.255.0	Configures the IP address
Router2(config-if-serial0)#peer ip address 3.3.3.1	Designates the IP address of the opposite terminal
Router2(config-if-serial0)#parity none	Parity none
Router2(config-if-serial0)#flowctrl none	Without flow control

Peer ip add A.B.C.D is used to designate the IP address of the opposite side.

TCP/IP Packet Header Compression

TCP packet header compression uses the van Jacobson algorithm, which is defined in the RFC 1144. It is suitable for the TCP/IP data stream with small packets (for example, the telnet session packet). TCP/IP packet header compression reduces additional costs because of transferring the big TCP/IP packet headers in WAN.

TCP/IP packet header compression is geared toward protocols and it only compresses TCP/IP packet headers. So the frame header of the second layer will not be changed. The data frame whose TCP/IP packet header has been compressed will be transmitted on the WAN link.

In other words, TCP/IP packet header compression is more useful with the mini-type packets that only have several bytes (such as a telnet packet). The packet header compression protocols supported by Signamax routers are: X25 protocol, Frame-relay protocol, PPP protocol and HDLC protocol.

This kind of packet can also be applied to the dial-up WAN link protocol. Because data compression will bring additional process, packet header compression is usually used on the low-speed link, for example, the 64Kb/S link.

The configuration commands are as follows:

router (config-if-XXX)#？

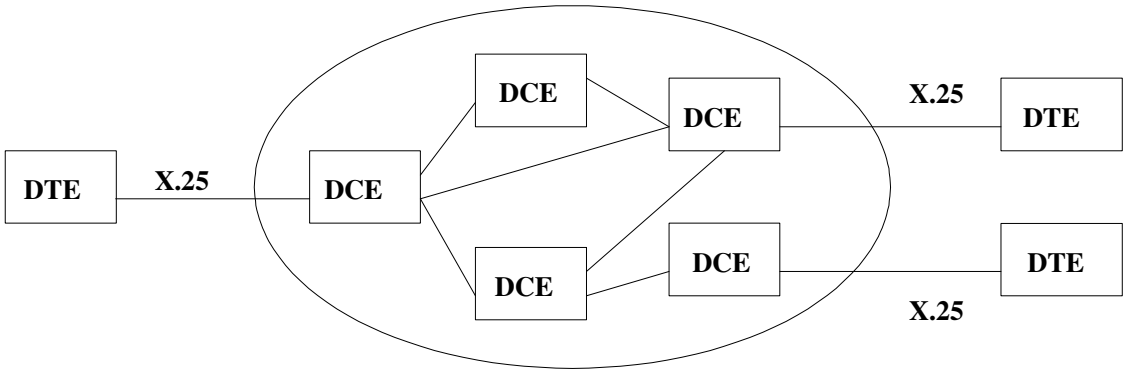
Command	Description
enc ppp	Encapsulate ppp. (ROUTER supports the TCP packet-header compression of x25.frame-relay.hdlc.ppp)
ip tcp header-compression	Encapsulates TCP packet header compression
Ip tcp header-compression passive	The function of the keyword "passive" is that the TCP packets will be compressed if received packets of the interface are compressed. If the parameter "passive" is not designated, the router will compress all the data streams

X.25 Protocol

This section introduces how to configure X.25 protocol on a Signamax router and how to run various X.25 parameters so as to achieve the seamless integration of a Signamax router in a X.25 network.

Overview

When the MP2600 router is used to connect with X.25 network or another router encapsulating X.25 via a leased line, the X.25 protocol and LAPB protocol need to be configured on the WAN port of the router.



Basic X.25 Configuration

Command	Description	Config mode
encapsulation x25 [dce | dte]	*encapsulate X.25 protocol	config-if-××
x25 address x121-address	*configure X.121 address	config-if-×× | config-x25
x25 {dce | dte}	*configure X.25 mode	config-if-×× | config-x25
x25 hic virtual-circuit-number	Configure the highest input virtual circuit number	config-if-×× | config-x25
x25 hoc virtual-circuit-number	Configure highest output virtual circuit number	config-if-×× | config-x25
x25 htc virtual-circuit-number	Configure highest dual-directional virtual circuit number	config-if-×× | config-x25
x25 lic virtual-circuit-number	Configure lowest input virtual circuit number	config-if-×× | config-x25
x25 loc virtual-circuit-number	Configure lowest output virtual circuit number	config-if-×× | config-x25
x25 ltc virtual-circuit-number	*configure lowest dual-directional virtual circuit number	config-if-×× | config-x25
x25 idle minutes	Configure virtual circuit idle time	config-if-×× | config-x25
x25 ips packet-size	Configure max input packet size	config-if-×× | config-x25
x25 ops packet-size	Configure max output packet size	config-if-×× | config-x25
x25 modulo packet-numbering-modulus	Configure number modulus	config-if-×× | config-x25
x25 t20 seconds	Configure restarting request retransmission timer	config-if-×× | config-x25
x25 t21 seconds	Configure call request retransmission timer	config-if-×× | config-x25
x25 t22 seconds	Configure reset request retransmission timer	config-if-×× | config-x25
x25 t23 seconds	Configure clear request retransmission timer	config-if-×× | config-x25
x25 win incoming-window-size	Configure incoming window size	config-if-×× | config-x25
x25 wout outgoing-window-size	Configure outgoing window size	config-if-×× | config-x25
x25 map ip ip-address x121-address	*configure IP address and	config-if-××

[broadcast / negotiate-disable]	X.121 address mapping	
x25 map compressedtcp ip-address x121-address [passive / negotiate-disable]	Configure TCP/IP header compression	config-if-××
x25 map qllc vmac-address x121-address [broadcast / negotiate-disable]	Configure QLLC VMAC address X.121address mapping	config-if-××
x25 pvc pvc-number ip ip-address [x121-address / broadcast]	*configure PVC and IP address mapping	config-if-××
x25 pvc pvc-number compressedtcp ip-address [x121-address / broadcast]	Configure TCP/IP header Compression	config-if-××
x25 pvc pvc-number qllc vmac-address [x121-address]	Configure PVC and QLLC VMAC address mapping	config-if-××
x25 pvc pvc-number1 interface intf-name pvc pvc-number2	*configure PVC local switch	config-if-××
x25 pvc pvc-number1 xot ip-address interface intf-name pvc pvc-number2	Configure PVC switch by XOT	config-if-××
encapsulation lapb [dce | dte]	Encapsulate LAPB protocol	config-if-××
lapb {dce | dte}	Configure interface LAPB mode	config-if-×× | config-x25
lapb K window-size	Configure windows size	config-if-×× | config-x25
lapb modulo frame-numbering-modulus	Configure frame numbering modulus	config-if-×× | config-x25
lapb N1 bytes	Configure information frame max bytes number	config-if-×× | config-x25
lapb N2 tries	Configure frame retransmission max times	config-if-×× | config-x25
lapb T1 seconds	Configure retransmission timer	config-if-×× | config-x25
lapb T2 seconds	Configure explicit acknowledge deferral timer	config-if-×× | config-x25
lapb T4 seconds	Configure keepalive timer	config-if-×× | config-x25
x25 routing	*enable X.25 switch function	config
x25 route x121-address interface intf-name [dlci dlci-number]	*configure X.25 route	config
x25 route x121-address xot ip-address	*configure X.25 route by XOT	config
xot keeplive enable	Enable XOT keepalive function	config
xot keeplive t1 seconds n1 times t2 seconds t3 seconds n3 times	Configure XOT keepalive parameter	config
x25 profile x25-profile-name [dce | dte]	*set up a X.25 Profile	config
x25-profile x25-profile-name	*connect X.25 Profile and	config-fr-dlci

	PVC	
x3 parameter:value [parameter:value]	Configure X.3 PAD parameter	config | enable
pad cud call-user-data	Configure PAD call user data	config
pad x121-address	*PAD connection	enable
terminal x121-address template-name COM TERM [initiative]	Apply terminal template to X.3 PAD	config

"*" before command means it has configuration example description.

Configuration mode is: enable, config, config-if-××(interface name) and config-××(protocol name) etc.

X.25 Configuration

Router1 configuration:

Command	Task
Router1#configure terminal	
Router1(config)#interface s0/0	Enters port S0/0
Router1(config-if-serial0/0)#physical-layer sync	The physical layer works in the synchronous mode
Router1(config-if-serial0/0)#encapsulation x25	Encapsulates the data link layer protocol X.25
Router1(config-if-serial0/0) x25 dte	Configures X.25 as DTE mode
Router1(config-if-serial0/0)x25 address 200	The X.121 address is 200
Router1(config-if-serial0/0)x25 map ip 3.3.3.2 100	Establishes the map between the IP address of the opposite terminal and the X.121 address
Router1(config-if-serial0/0)#ip address 3.3.3.1 255.255.255. 0	Configures the IP address of port S0

Router1(config-if-serial0/0)#end	

Router2 configuration:

Command	Task
Router2#configure terminal	
Router2(config)#interface s0/0	
Router2(config-if-serial0/0)#physical-layer sync	
Router2(config-if-serial0/0)#encapsulation x25	
Router2(config-if-serial0/0) x25 dce	Configures X.25 as DCE mode
Router2(config-if-serial0/0)x25 address 100	The X.121 address is 100
Router2(config-if-serial0/0)x25 map ip 3.3.3.1 200	Establishes the map between the IP address of the opposite terminal and the X.121 address
Router2(config-if-serial0/0)#ip address 3.3.3.2 255.255.255. 0	Configures the IP address of the port S0
Router2(config-if-serial0)#end	

Debugging/Monitoring X.25

Displays status information of an interface of local router:

```
show interface serial <serial-number>
serial (unit number 0):
Flags: (0x80e1) UP MULTICAST RUNNING
Type: RFC877_X25
Internet address: 10.1.1.1
Netmask 0xff000000 Subnetmask 0xffffff00
Metric is 0
Maximum Transfer Unit size is 1500
10 packets received; 10 packets sent
0 multicast packets received
0 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped
X.25 DTE,address 100, state R1, modulo 8, timer 0
Defaults: idle VC timeout 1 Minutes
ietf encapsulation
input/output window sizes 2/2, packet sizes 128/128
Timers: T20 10, T21 10, T22 10, T23 10
Channels: PVC none, SVC 1-1024
RESTARTs 0/1 CALLs 1+0/0+1 DIAGs 0/0
LAPB DTE, state CONNECT modulo 8, k 7, N1 1550, N2 10
T1 3s, T2 1s, interfaceoutage (partial T3) 9s, T4 15s
vs:5, vr:4, txNr:4, rxNr:5, retxCnt:0, retxqIn:5, retxqOut:5
IFRAMEs 13/12 RNRs 0/0 REJs 0/0 SABM/Es 36/1 FRMRs 0/0 DISCs
0/0
txQueue: priority 0: cnt=0 max=20 sMax=1
rxFrames 995, rxChars 12377
txFrames 748, txChars 11693
rxNoOctet 7, rxAbtErrs 3, rxCrcErrs 0
```

```
rxOverrun 0, rxLenErrs 0, txUnderrun 0
DCD=up  DSR=up  DTR=up  RTS=up  CTS=up  TxC=up
```

Displays virtual circuit status information of an interface of local router

```
show x25 vc
serial3:
  vc No.1024: R1-P4-D1  SVC calling  FRI FEB 20 20:25:37 1970
      local  X.121 address: 1124
      remote X.121 address: 1125 (112.255.4.5)
      flow-state: ready (D1), sWin:2, rWin:2
      sMaxPktSize:128, rMaxPktSize:128
      vr:4, vs:0, nr:3, ns:0, lastNr:0, noRspDataCnt:0
      stxQueue: priority 0: cnt=0    max=32   sMax=2    qw=3
qwMax=10
      txQueue: priority 0: cnt=0    max=300  sMax=8    qw=4
qwMax=10
```

Other debugging/monitoring commands:

Command	Description
show x25 map	Displays address mapping table from protocol address to X.121 address
show x25 vc	Displays detail of the appointed virtual circuit that has been established
debug x25 serial-number all	Displays all contents for the received/sent packets on the interface
debug x25 serial-number head	Displays partial contents for received/sent packets contents for
debug x25 serial-number vc	Displays all contents for received/sent packet on the VC number
debug lapb serial-number all	Displays all contents for received/sent LAPB frames on the interface
debug lapb serial-number head	Displays partial contents for received/sent LAPB frames on the interface

X.25 Sub-interface

A sub-interface is a virtual interface that is capable of connecting to some networks via a physical interface. For the routing protocol using the split-horizon rule, sub-interface is needed to decide which host needs routing updates. In a WAN environment, if sub-interface (X.25) is used, other routers that are connected via the same physical interface may not receive the route update information.

Compared with the routers connected via the different physical interfaces, the sub-interface can be used and it can be regarded as a separate interface. Then the host can be connected to different sub-interfaces of the same physical interface. The route process regards each sub-interface as an independent route update source; so all the sub-interfaces can be fit for receiving route update information.

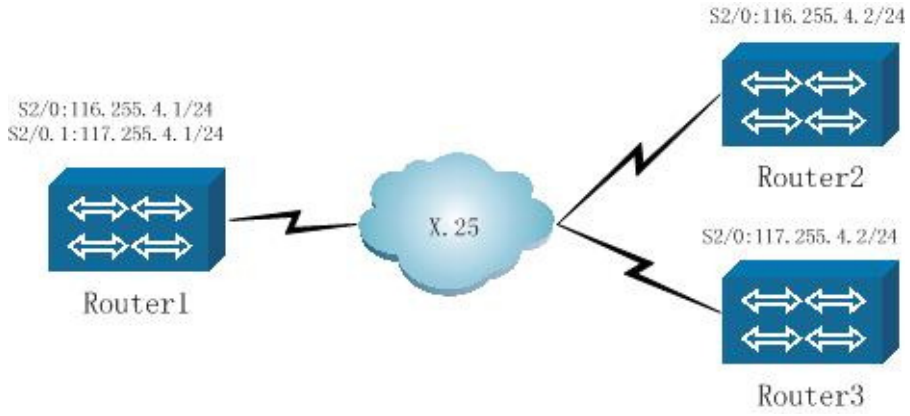
A sub-interface has two types: point to point and point to multipoint. The default is point to multipoint. At the time, X.25 of Signamax routers only support the point-to-multipoint sub-interface.

Configuring a X.25 sub-interface:

When the sub-interface is configured, X.25 should be configured on the main interface. And the x25 address x121-address also needs to be configured (if the sub-interface uses the map mapping) or x25 ltc ltc-number is configured (if the sub-interface uses the pvc mapping), and the ip-address is configured on the main interface.

If a sub-interface wants to be up, the main interface should be up first. If the main interface is shutdown, it is natural that the sub-interface will be down.

X.25 Sub-interface Configuration Example



X.25 sub-interface configuration example

The above figure represents how to configure a sub-interface on router1 so as to connect the whole X.25 network. Router2 corresponds with the main interface of router1 while router3 corresponds with the sub-interface of router1.

Router1 configuration:

Command	Task
Router1#configure terminal	
Router1(config)#interface serial2	Enters the serial port 2
Router1(config-if-serial2)#physical-layer sync	Physical layer synchronous
Router1(config-if-serial2)#clock rate 64000	Speed 64K
Router1(config-if-serial2)#encapsulation x25	Encapsulates the X.25 protocol on the data link layer
Router1(config-if-serial2)#x25 address 11625541	X121 address
Router1(config-if-serial2)#x25 map ip 116.255.4.2 11625542	The map of opposite IP address and opposite X121 address
Router1(config-if-serial2)#ip address 116.255.4.1 255.255.255.0	The IP address of the local main interface
Router1(config-if-serial2)#x25 dte	The working mode of X.25 is DTE
Router1(config-if-serial2)#exit	
Router1(config)interface serial2.1	Enters the sub-interface S2.1
Router1(config-sub-if-serial2.1)#x25 map ip 117.255.4.2 11725542	The map of opposite IP address and opposite X121 address
Router1(config-sub-if-serial2.1)#ip address 117.255.4.1 255.255.255.0 Router1(config-sub-if-serial2.1)#exit	The IP address of the local sub-interface

Configuration of router2 (router3)

Command	Task
Router2(config)#interface serial2	The tasks are the same as the one of router1
Router2(config-if-serial2)#physical-layer sync	
Router2(config-if-serial2)#clock rate 64000	
Router2(config-if-serial2)#encapsulation x25	
Router2(config-if-serial2)#x25 dte	
Router2(config-if-serial2)#x25 address 11625542	
Router2(config-if-serial2)#x25 map ip 116.255.4.1 11625541	
Router2(config-if-serial2)#ip address 116.255.4.2 255.255.255.0	
Router2(config-if-serial2)#exit	

X.25 Switching Function

The router can be used as a local or a remote switch, and it can switch X.25 data streams via TCP. Which is called XOT (X.25 Over TCP) usually.

SVC Switching

In order to enable the switching function of X.25, we can input the command "X25 routing" in the global configuration mode.

router(config)#

Command	Task
router (config)#x25 routing	Configures it as an X.25 switch

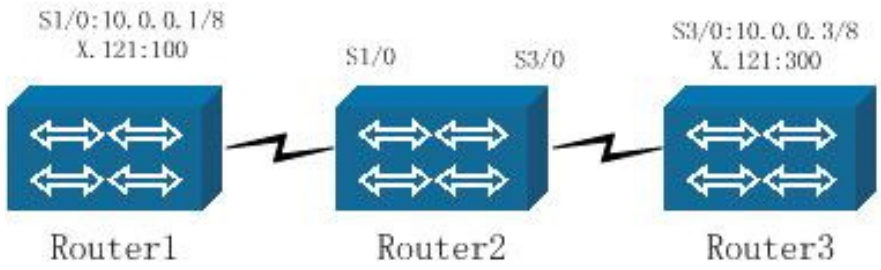
X.25 data streams can be routed between local serial ports. In this situation, the static routing command is needed to map X.121 address to the serial port. The router permits the X.25 interface connected to different ports to perform Switched Virtual Circuit (SVC) connection, and this is called local X.25 connection.

Remote X.25 switching enables the X.25 interface connected with different routers to establish the switched virtual circuit (SVC) and permanent virtual circuit (PVC). Remote X.25 switching is achieved via using tunnel technology for all X.25 calls and data streams between routers on the TCP connection. In order to enable remote switching, users can use the command "X25 router":

router (config)#x25 route X.121 address interface type number

Syntax	Task
X.121 address	X.121 address of the destination
Type number	Type and number of the interface to the destination

An example of X.25 switching function:



As shown in the figure above, we premise that router3 is used as the X.25 switch, and that router2 and router4 perform communication between them via the X.25 switching function of router3.

The X.121 address of the serial-port s2 of router2 is 200 while the X.121 address of the serial-port s3 of router4 is 100. We also need to configure the IP addresses of router2 and router4 by manually.

Router1 configuration:

Command	Task
router2(config)#int s2/0	Enters the interface mode
router2(config-if-serial2/0)#physical-layer sync	Encapsulates it as the synchronous mode
router2(config-if-serial2/0)#encapsulation x25	Encapsulates the X.25 protocol
router2(config-if-serial2/0)#x25 dte	Configures the X.25 as DTE mode (default)
router2(config-if-serial2/0)#x25 address 200	Configures X.121 address
router2(config-if-serial2/0)#x25 map ip 10.0.0.2 100 broadcast	Configures map mapping
router2(config-if-serial2/0)#ip address 10.0.0.1 255.0.0.0	Configures IP address
router2(config-if-serial2/0)#exit	Configuration has been finished

Router2 configuration:

Command	Task
router3(config)#x25 routing	Configures it as an X.25 switch
router3(config)#x25 route 100 interface serial 3/0	Configures related X.121 address to which data stream is transmitted and related port
router3(config)#x25 route 200 interface serial 2/0	Configures related X.121 address to which data stream is transmitted and related port
router3(config)#int s2/0	Enters the interface s2 mode
router3(config-if-serial2/0)#clock rate 128000	Configures the clock
router3(config-if-serial2/0)#encapsulation x25	Encapsulates X.25 protocol
router3(config-if-serial2/0)#x25 dce	Configures X.25 as the DCE mode
router3(config-if-serial2/0)#int s3/0	Enters the interface S3
router3(config-if-serial3/0)#physical-layer sync	Configures it as the synchronization mode
router3(config-if-serial3/0)#clock rate 128000	Configures the clock
router3(config-if-serial3/0)#encapsulation x25	Configures X.25 protocol
router3(config-if-serial3/0)#x25 dce	Configures X.25 as the DCE mode

Router3 configuration:

Command	Task
router2(config)#int s3/0	Enters the interface mode
router2(config-if-serial3/0)#physical-layer sync	Encapsulates it as the synchronization mode
router2(config-if-serial3/0)#encapsulation x25	Encapsulates X.25 protocol
router2(config-if-serial3/0)#x25 dte	Configures X.25 as DTE mode (default)
router2(config-if-serial3/0)#x25 address 100	Configures the X.121 address
router2(config-if-serial3/0)#x25 map ip 10.0.0.1 200 broadcast	Configures the map mapping
router2(config-if-serial3/0)#ip address 10.0.0.2 255.0.0.0	Configures the IP address
router2(config-if-serial3/0)#exit	Configuration finished

PVC Switching Function

```
router (config-if-serial3)#x25 pvc Circuit number
interface type number pvc number1
```

Configuring commands: (in interface configuration mode):

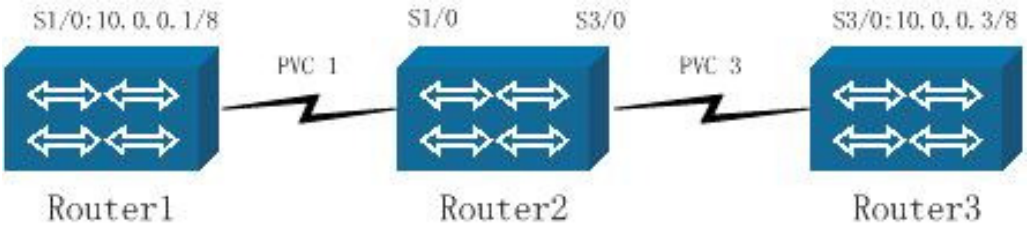
Command	Task
Circuit number	The PVC number that will be applied to the local interface
Interface	Designates the keywords needed by an interface
Type	The type of the remote interface
Number	The remote interface number
PVC	The keywords needed to configure switching PVC
Number1	The PVC number that will be used for the remote side

The configuring commands of XOT:

```
router (config-if-serial3)#x25 pvc Circuit number xot address
interface type string pvc number
```

The configuring commands: (in the interface configuration mode):

Command	Task
Circuit number	The PVC number used to connect equipment
Xot	Indicates that two PVCs will be connected via a TCP/IP LAN that uses XOT
Address	The IP address of the connected equipment
Interface serial	Indicates that the interface is a serial port
String	The definition of serial interface, which can be a number or a character string
PVC	Designates a line of PVC
Number	Designates the PVC number of the destination address



X.25 PVC switching configuration example

The PVC number between router1and router2 is 1; the PVC number between router3 and router2 is 3, router2 X.25 switch.

Router1 configuration

Command	Description
router1 (config)#int s1/0	Enter interface mode
router1 (config-if-seral1/0)#physical-layer sync	Configure as synchronous mode
router1 (config-if-serial1/0)#encapsulation x25	Encapsulate X.25 protocol
router1 (config-if-serial1/0)#x25 dte	Configure as X.25 DTE mode
router1 (config-if-serial1/0)#x25 ltc 16	Configure ltc parameter
router1 (config-if-serial1/0)#x25 pvc 1 ip 10.0.0.3	Mapping local PVC number to peer IP address
router1 (config-if-serial1/0)#ip address 10.0.0.1 255.0.0.0	Configure IP address

Router2 configuration

Command	Description
router2 (config)#x25 routing	Configure X.25 switch
router2 (config)#int s1/0	Enter s2/0 mode
router2 (config-if-serial1/0)#physical-layer sync	Configure as synchronous mode
router2 (config-if-serial1/0)#clock rate 128000	Configure clock
router2 (config-if-serial1/0)#encapsulation x25	Encapsulate X.25 protocol
router2 (config-if-serial1/0)#x25 dce	Configure as X.25 DCE mode
router2 (config-if-serial1/0)#x25 ltc 16	Configure ltc value
router2 (config-if-serial1/0)#x25 pvc 1 interface serial 3/0 pvc 3	Configure PVC switching
router2 (config-if-serial1/0)#int s3/0	Enter s3/0
router2 (config-if-serial3/0)#physical-layer sync	Configure as synchronous mode
router2 (config-if-serial3/0)#clock rate 128000	Configure clock
router2 (config-if-serial3/0)#encapsulation x25	Encapsulate X.25 protocol
router2 (config-if-serial3/0)#x25 ltc 16	Configure ltc value
router2 (config-if-serial3/0)#x25 dce	Configure as X.25 DCE mode
router2 (config-if-serial3/0)#x25 pvc 3 interface serial 1/0 pvc 1	Configure PVC switching
router2 (config-if-serial3/0)#exit	Configuration completed

Router3 configuration

Command	Description
router3 (config)#int s3/0	Enter interface mode
router3 (config-if-serial3/0)#physical-layer sync	Configure as synchronous mode
router3 (config-if-serial3/0)#encapsulation x25	Encapsulate X.25 protocol
router3 (config-if-serial3/0)#x25 dte	Configure as X.25 DTE mode
router3 (config-if-serial3/0)#x25 ltc 16	Configure ltc parameter
router3 (config-if-serial3/0)#x25 pvc 3 ip 10.0.0.1	Mapping local PVC number to peer IP address
router3 (config-if-serial3/0)#ip address 10.0.0.3 255.0.0.0	Configure IP address

X.25 GRE Function

When using x25 route x121-address interface intf-name to configure X.25 routing, the GRE becomes effective. All called address is started with serial x121-addres, and forwarded via the interface, for example, x25 route 123 int s1/0 and so all calls with the address beginning with 123 (such as 1234, 12345 etc.) will be forwarded via s1/0.

Annex G (X.25 over Frame-Relay)

Configuration Commands

1) x.25 profile
Use the command x.25 profile to create a X.25 Profile; or, use the negation of the command to cancel related X.25 Profile.

x25 profile name [dte | dce]

Syntax	Description
profile	Specify the keyword of the x25 profile
name	The name of the x25 profile
dte	(Optional)The x25 profile serves as DTE
dce	(Optional)The x25 profile serves as DCE

(By default) There exists no name, the x.25 profile serves as DTE.

(Command mode) the global configuration mode.

Enter the X.25 configuration mode after creating the X.25 Profile. In the mode, use the following configuration commands to configure X.25 parameters of the X.25profile.

The usage and meaning of these configuration commands are the same as that of those commands that are used to encapsulate X.25 interface and configure X.25 parameters.

Syntax	Description
x25 address	Configure the X.121 address
x25 modulo	Configure the window mode
x25 hic	Configure the maximal one-way ingress virtual circuit number
x25 hoc	Configure the maximal one-way egress virtual circuit number
x25 htc	Configure the maximal two-way virtual circuit number
x25 ltc	Configure the minimal two-way virtual circuit number
x25 t20	Configure restarting request retransmission timer
x25 t21	Configure call request retransmission timer
x25 t22	Configure reset request retransmission timer
x25 t23	Configure clear request retransmission timer
x25 hold-queue	Configure the maximal number of packets a virtual circuit can save before transmitting data
x25 idle	Configure the idle period of clearing a SVC
x25 nvc	Configure the maximal number of protocol virtual circuits that with the host are enabled
x25 ips	Configure the maximal length of an ingress packet
x25 ops	Configure the maximal length of an egress packet
x25 win	Configure the value of the in-window
x25 wout	Configure the value of the out-window

Enter the X.25 configuration mode after creating the X.25 Profile. In the mode, use the following configuration commands to configure LAPB parameters of the X.25profile. The usage and meaning of these configuration commands are the same as that of those commands that are used to encapsulate X.25 interface and configure LAPB parameters.

Syntax	Description
lapb k	Configure the maximal number of uncertain frames, namely window size
lapb modulo	Configure LAPB basic (mode 8)/extended (mode16) protocol mode
lapb N1	Configure the maximal number of bits contained in a frame
lapb N2	Configure the maximal times of data packet retransmission
lapb T1	Configure the value of the retransmission timer
lapb T2	Configure the value of the acknowledgement timer
lapb T4	Configure the value of the idle timer

x.25-profile
Use the command x.25-profile to relate a X.25 Profile with some frame-relay PVC on a frame-relay interface; or, use the negation of the command to cancel the relation.

```
frame-relay interface-dlci number
x25-profile name
no x25-profile name
```

Syntax	Description
Number	The DLCI number of the frame-relay PVC related with X.25 profile
Name	The name of X.25 profile related with PVC

(By default) There exists no relation.
(Command mode)the frame-relay DLCI configuration mode.

Use the following command to send out a X.25 call via the frame-relay network:

`x25 route address interface serial-interface dlci number`

Syntax	Description
Address	The X.121 destination address
serial-interface	Route the selected call to the specified frame-relay serial interface
Number	The frame-relay DLCI number used to transmit the call

Configuring X.25 over Frame-relay Network

Annex G configuration example

A connection between Router1 and Router2 is established via a X.25 packet switching network; the interconnection between Router2 and Router3 is realized via a frame-relay switching network; and the connection between Router3 and Router4 is established via a X.25 packet switching network. By means of Annex.G, X.25 packets between Router1 and Router4 are transmitting over the frame-relay network.

Router1 is configured as follows.

Syntax	Description
RouterA#configure terminal	
RouterA(config)# interface serial1/0	Enter the interface S1/0configuration mode
RouterA(config-if-serial1/0)# physical-layer sync	
RouterA(config-if-serial1/0)# clock rate 64000	Configure the clock rate
RouterA(config-if-serial1/0)# encapsulation x25	Encapsulate X.25 on the interface
RouterA(config-if-serial1/0)# x25 address 70	Configure the X.25 address
RouterA(config-if-serial1/0)# x25 map ip 192.168.1.2 71	Configure the X.25 address map
RouterA(config-if-serial1/0)# ip address 192.168.1.1 255.255.255.0	Configure the IP address
RouterA(config-if-serial1/0)#exit	

2) Router2 is configured as follows.

Syntax	Description
RouterB# configure terminal	
RouterB(config)# x25 routing	
RouterB(config)# x25 profile name1 dce	Create a X.25 Profile and set it as DCE
RouterB(config-x25)#exit	
RouterB(config)# interface serial1/0	Enter the interface S1/0 configuration mode
RouterB(config-if-serial1/0)# physical-layer sync	
RouterB(config-if-serial1/0)# encapsulation x25 dce	Encapsulate X.25 on the interface
RouterB(config-if-serial1/0)# interface serial2/0	Enter the interface S2/0 configuration mode
RouterB(config-if-serial2/0)# physical-layer sync	
RouterB(config-if-serial2/0)# encapsulation frame-relay	Encapsulate frame-relay on the interface
RouterB(config-if-serial2/0)# frame-relay lmi-type ansi	Configure frame-relay LMI type
RouterB(config-if-serial2/0)# frame-relay interface-dlci 100	Configure the DLCI number
RouterB(config-fr-dlci)# x25-profile name1	Relate X.25 Profile (name1) to the specified PVC
RouterB(config-fr-dlci)# exit	Exit the DLCI configuration mode
RouterB(config-if-serial2/0)#exit	
RouterB(config)# x25 route 71 interface serial2/0 dlci 100	Transmit a X.25 call over the specified frame-relay PVC
RouterB(config)# x25 route 70 interface serial1/0	Transmit a X.25 packet

Router3 is configured as follows.

Syntax	Description
RouterC# configure terminal	
RouterC(config)# x25 routing	
RouterC(config)# x25 profile name2 dte	Create a X.25 Profile and set it as DTE
RouterC(config-x25)#exit	
RouterC(config)# interface serial2/0	Enter the interface S2/0 configuration mode
RouterC(config-if-serial2/0)# physical-layer sync	
RouterC(config-if-serial2/0)# encapsulation x25 dce	Encapsulate X.25 on the interface
RouterC(config-if-serial2/0)# interface serial1/0	Enter the interface S1/0 configuration mode
RouterC(config-if-serial1/0)# physical-layer sync	
RouterC(config-if-serial1/0)# encapsulation frame-relay	Encapsulate frame-relay on the interface
RouterC(config-if-serial1/0)# frame-relay lmi-type ansi	Configure frame-relay LMI type
RouterC(config-if-serial1/0)# frame-relay interface-dlci 200	Configure the DLCI number
RouterB(config-fr-dlci)# x25-profile name2	Relate X.25 Profile (name1) to the specified PVC
RouterB(config-fr-dlci)# exit	Exit the DLCI configuration mode
RouterC(config-if-serial1/0)#exit	
RouterC(config)# x25 route 70 interface serial1/0 dlci 200	Transmit a X.25 call over the specified frame-relay PVC
RouterC(config)# x25 route 71 interface serial2/0	Transmit a X.25 packet

Router4 is configured as follows:

Syntax	Description
RouterD# configure terminal	
RouterD(config)# interface serial2/0	Enter the interface S2/0 configuration mode
RouterD(config-if-serial2/0)# physical-layer sync	
RouterD(config-if-serial2/0)# clock rate 64000	Configure the clock rate
RouterD(config-if-serial2/0)# encapsulation x25	Encapsulate X.25 on the interface
RouterD(config-if-serial2/0)# x25 address 71	Configure the X25 address
RouterD(config-if-serial2/0)# x25 map ip 192.168.1.1 70	Configure the X25 address map
RouterD(config-if-serial2/0)# ip address 192.168.1.2 255.255.255.0	Configure the IP address
RouterD(config-if-serial2/0)#exit	

X.25 PAD Function

The PAD is a telnet-like function, which is used to login a remote X.25 host. The destination address is a X.121 address instead of IP address.

Command	Description
Router# pad x.121 address	Login a remote X.25 host

PAD Configuration example

Router1 and router2 is connected directly throuth X.25

Router1 configuration:

Command	Description
Router1(config)#interface s1/0	Enters the interface mode
Router1(config-if-serial1/0)#encapsulation x25	Encapsulates X.25 protocol
Router1(config-if-serial1/0) x25 dte	Configures X.25 as DTE mode
Router1(config-if-serial1/0)x25 address 100	Configure X.121 address as 200

Router2 configuration:

Command	Description
Router2(config)#interface s1/0	
Router2(config-if-serial1/0)#clock rate 128000	Configure the clock rate
Router2(config-if-serial1/0)#encapsulation x25	
Router2(config-if-serial1/0)x25 dce	
Router2(config-if-serial1/0)x25 address 200	Configure X.121 address to 200
Router2(config-if-serial1/0)#end	Configuration has been finished
Router2#pad 100	PAD to peer
Router1>	Login

XOT (X.25 Over TCP/IP)

Signamax router may be configured as an X.25 remoter switch, switching X.25 data flow via TCP connection, and this is XOT(X.25 Over TCP) technology. XOT switching comprises SVC XOT and PVC XOT.

```
x25 route xot
```

Configure an XOT routing to realize SVC XOT remote switching, and no is used to delete a configured XOT routing.

```
x25 route x121-address xot ip-address
no x25 route x121-address
```

Synt ax	Description
x121-address	X.121 address
ip-address	Remote router IP address

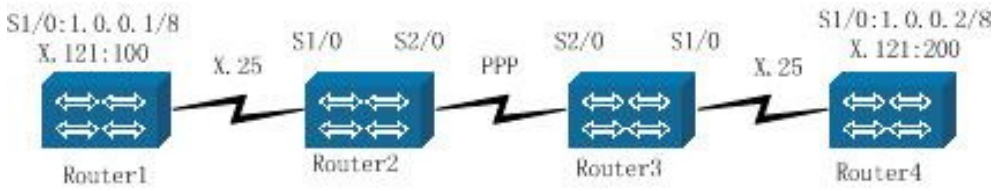
(Default status)not configure XOT routing

```
x25 pvc xot
Configure PVC XOT remote switching, no is used to delete the switching.
x25 pvc pvc-number1 xot ip-address interface intf-name pvc pvc-number2
no x25 pvc pvc-number1
```

Syntax	Description
pvc-number1	Local PVC number
ip-address	Remote router IP address
intf-name	Remote router X.25 interface name
pvc-number2	Remote PVC number

(Default status)no PVC XOT remote switching

XOT Configuration Example



Router1 and router2 are running on X.25 protocol, router3 and router4 are also running on X.25 protocol. But router2 and router3 are running on PPP protocol. This is an example of SVC XOT remote switching.

Router1 configuration:

Command	Description
router1(config)#int s1/0	Enter interface mode
router1(config-if-serial/0)#physical-layer sync	Configure synchronous mode
router1(config-if-serial1/0)#encapsulation x25	Encapsulate X.25 protocol
router1(config-if-serial1/0)#x25 dte	Configure X.25 DTE mode
router1(config-if-serial1/0)#x25 address 100	X.121 address 100
router1(config-if-serial1/0)#x25 map ip 1.0.0.2 200	Set up peer IP address and X.121 address mapping
router1(config-if-serial1/0)#ip address 1.0.0.1 255.0.0.0	Configure IP address

Router2 configuration:

Command	Description
router2(config)#x25 routing	Configure X.25 switch
router2(config)#int s2/0	Enter s2/0, configuring TCP/IP network interface
router2(config-if-serial2/0)#physical-layer sync	Configure synchronous mode
router2(config-if-serial2/0)#encapsulation ppp	Encapsulate PPP protocol
router2(config-if-serial2/0)#ip address 10.0.0.1 255.0.0.0	Configure IP address
router2(config-if-serial2/0)#int s1/0	Enter s3/0
router2(config-if-serial1/0)#physical-layer sync	Configure synchronous mode
router2(config-if-serial1/0)#clock rate 128000	Configure clock
router2(config-if-serial1/0)#encapsulation x25	Encapsulate X.25 protocol
router2(config-if-serial1/0)#x25 dce	Configure X.25 DCE mode
router2(config-if-serial1/0)#exit	Exit to interface configuration mode
router2(config)#x25 route 100 interface s1/0	Configure X.25 routing
router2(config)#x25 route 200 xot 10.0.0.2	Configure XOT routing

Router3 configuration

Command	Description
router3(config)#x25 routing	Configure X.25 switch
router3(config)#int s2/0	Enter s2/0, configuring TCP/IP network interface
router3(config-if-serial2/0)#physical-layer sync	Configure synchronous mode
router3(config-if-serial2/0)#encapsulation ppp	Encapsulate PPP protocol
router3(config-if-serial2/0)#clock rate 128000	Configure clock
router3(config-if-serial2/0)#ip address 10.0.0.2 255.0.0.0	Configure IP address
router3(config-if-serial2/0)#int s1/0	Enter s3/0
router3(config-if-serial1/0)#physical-layer sync	Configure synchronous mode
router3(config-if-serial1/0)#clock rate 128000	Configure clock
router3(config-if-serial1/0)#encapsulation x25	Encapsulate X.25 protocol

router3(config-if-serial1/0)#x25 dce	Configure X.25 DCE mode
router3(config-if-serial1/0)#end	Exit to interface configuration mode
router3(config)#x25 route 200 interface s1/0	Configure X.25 routing
router3(config)#x25 route 100 xot 10.0.0.1	Configure XOT routing

Router4 configuration:

Command	Description
router4(config)#int s1/0	enter interface mode
router4(config-if-serial1/0)#physical-layer sync	Configure synchronous mode
router4(config-if-serial1/0)#encapsulation x25	Encapsulate X.25 protocol
router4(config-if-serial1/0)#x25 dte	Configure X.25 DTE mode
router4(config-if-serial1/0)#x25 address 200	X.121 address 200
router4(config-if-serial1/0)#x25 map ip 1.0.0.1 100	Set up peer IP address and X.121 address mapping
router4(config-if-serial1/0)#ip address 1.0.0.2 255.0.0.0	Configure IP address

Frame Relay Protocol

Frame relay is a protocol standardized by ANSI and CCITT, and it can provide remarkable performance/price ratio to bursting out traffic (for example, LAN inter-connection and SNA).

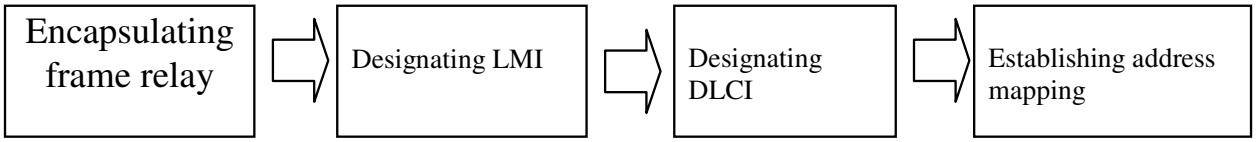
Frame relay is a kind of interface protocol between the Customer Premise Equipment (CPE), such as a router or Front End Processor, and a WAN sending data to remote CPE.

Configure Frame Relay Command

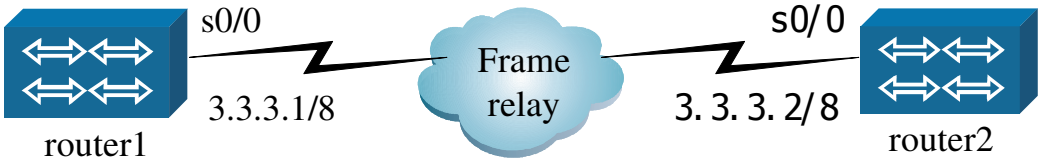
Command	Description	Configuration mode
encapsulation frame-relay [cisco]	Interface link layer protocol encapsulates frame relay	config-if-××
frame-relay class name	Connect a mapping type with interface	config-if-××
frame-relay congestion-management	Enable DE rule on interface	config-if-××
frame-relay de-goup de-list-number dlci	Enable DE bit drop rule on DLCI	config-if-××
frame-relay interface-dlci dlci [switched]	Distribute DLCI to interface or sub-interface	config-if-××
frame-relay intf-type {dce | dte | nni}	Configure frame relay interface type	config-if-××
frame-relay inverse-arp [interval time | ip dlci | update]	Configure frame relay Inverse Address Resolution Protocol	config-if-××
frame-relay ip rtp header-compression [passive]	Configure RTP header compression	config-if-××
frame-relay ip tcp header-compression [passive]	Configure TCP/IP header compression	config-if-××
frame-relay lmi-n391dte keep-exchanges	Configure full status polling counter	config-if-××
frame-relay lmi-n392dce threshold	Configure DCE error threshold value	config-if-××
frame-relay lmi-n392dte threshold	Configure DTE error threshold value	config-if-××
frame-relay lmi-n393dce events	Configure DCE monitoring event counter	config-if-××
frame-relay lmi-n393dte events	Configure DTE monitoring event counter	config-if-××
frame-relay lmi-t392dce seconds	Configure DCE timer	config-if-××
frame-relay lmi-type {ansi | lmi | q933a}	Configure local management interface(LMI)	config-if-××
frame-relay map ip ipaddress dlci [cisco | ietf] [broadcast] [compress [passive] | nocompress | rtp header-compress [passive] | tcp header-compress [passive]]	Configure local PVC and remote IP address static mapping	config-if-××
frame-relay route in-dlci interface name out-dlci	Configure PVC switching static routing	config-if-××
frame-relay traffic-shaping	Enable traffic shaping on interface	config-if-××

keepalive [seconds]	Configure keepalive check time interval	config-if-××
frame-relay de-list list-number protocol ip {fragments | gt size | list access-list-number | lt size | tcp port | udp port}	Define DE list	config
frame-relay switching	Configure router executing switching function in FR network	config
map-class frame-relay map-class-name	Designate PVC mapping type to define QoS	config
frame-relay cir bps	Configure PVC CIR	config-map-class
frame-relay custom-queue-list list-number	Designate user queue list for PVC	config-map-class
frame-relay fragment {bytes | should-encap-mulproto}	Configure frame relay packet fragment size	config-map-class
frame-relay priority-group list-number	Designate priority group of PVC	config-map-class
frame-relay traffic-rate average [peak]	Designate traffic rate of PVC	config-map-class
service-policy output policy-name	Designate QoS service strategy of PVC	config-map-class
class name	Configure a mapping type connecting PVC	config-fr-dlci
vlan-bridge vlan-interface	Configure frame relay bridging between VLAN interface and point-to-point FR sub-interface	config-if-××

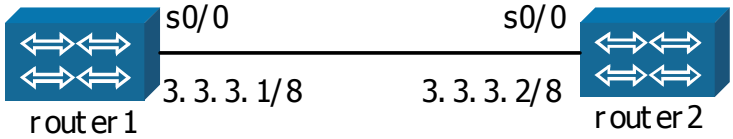
Frame Relay Configuration Example



Network connection:



Back-to-back connection:



S0/0 port (3.3.3.1) of local router1 connects to S0/0 port (3.3.3.2) of the peer router2.

Router1 configuration:

Command	Task
Router1#configure terminal	
Router1(config)#interface s0/0	Enters S0/0 port
Router1(config-if-serial0/0)#physical-layer sync	Configures the working mode of physical layer as synchronization mode
Router1(config-if-serial0/0)#encapsulation frame-relay intf-type dte	Encapsulates frame relay of link layer protocol
Router1(config-if-serial0/0)#frame-relay intf-type dte	Works in frame relay DTE mode
Router1(config-if-serial0/0)#frame-relay lmi-type ansi	Designates frame relay lmi type: it should be same with the switcher of telcom
Router1(config-if-serial0/0)#frame-relay interface-dlci 18	The local dlci number: it is provided by telecommunication office
Router1(config-if-serial0/0)#frame-relay map ip 3.3.3.2 18 broadcast	Frame relay mapping, the peer terminal IP address and the local dlci number
Router1(config-if-serial0/0)#ip address	IP address of the port S0/0

3.3.3.1 255.255.255.0	
Router1(config-if-serial0)#exit	

Router2 configuration:

Command	Task
Router2#configure terminal	
Router2(config)#interface s0/0	
Router2(config-if-serial0/0)#physical-layer sync	Configures working mode of physical layer as the synchronization mode
Router2(config-if-serial0/0)#encapsulation frame-relay	Encapsulates frame relay of link layer protocol
Router2(config-if-serial0/0)#frame-relay lmi-type ansi	Designates the frame relay type lmi: it should be same with the switch in telecom
Router2(config-if-serial0/0)#frame-relay intf-type dte	Work in the frame relay DTE mode
Router2(config-if-serial0/0)#frame-relay interface-dlci 20	The local-end number dlci: it is provided by telecommunication office
Router2(config-if-serial0/0)#frame-relay map ip 3.3.3.1 20 broadcast	Frame relay mapping, the peer terminal IP address, the dlci number of local end
Router2(config-if-serial0)#ip address 3.3.3.2 255.255.255.	IP address of S0/0 port
Router2(config-if-serial0)#exit	

Frame Relay Debugging, Monitoring

Users examine the PVC status of frame relay, and "ACTIVE" indicates that the PVC is in usable status. Users can also examine all the frame relay interfaces or a given one to determine the given PVC status and the statistic number of received/sent packets.

Displaying all status information of virtual connection (of interface) on the local router

```
show frame-relay pvc [interface serial number]

PVC statistics for interface serial0 (Frame Relay DTE)
DLCI = 17, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = seri
   al0

       input pkts 10          output pkts 10          in bytes 1040
       out bytes 1040        dropped pkts 0          in FECN pkts 0
       in BECN pkts 0       out FECN pkts 0        out BECN pkts 0
       in DE pkts 0          out DE pkts 0
```

Displaying information of frame relay mapping:

```
show frame-relay map
Serial2(up):ip 10.1.2.66  dlci 65,static,broadcast,
IETF, status ACTIVE
```

Other debugging/monitoring commands

Command	Description
show frame-relay lmi [interface serial number]	Displays LMI statistic of frame relay
show frame-relay inarp [interface serial number]	Displays InARP information
show frame-relay inarp ip rtp header-compression	
debug frame-relay lmi [interface serial number]	Displays LMI running data of frame relay
debug frame-relay packet [interface serial number]	Displays data operation beared by frame relay
debug frame-relay log [interface serial number]	Displays frame relay events and error indication

The physical layer should be in synchronous mode

The IP addresses of the ports of two connected routers should be in the same sub-network

When showing interface shows that the interface is "UP"and showing frame map shows that status is"ACTIVE", it is indicated that frame relay has connected with the WAN port and can begin to transmit data

Frame Relay Inverse Address Resolution Protocol

The main function of Inverse Address Resolution Protocol is to resolve the protocol address of the opposite equipment connected with each virtual circuit, which comprises the IP address, IPX address etc. At the present time Signamax routers only support IP addresses).

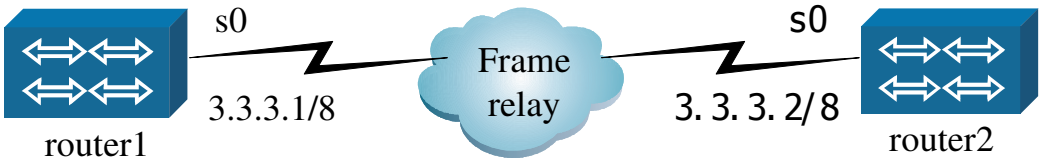
If the protocol address of the opposite equipment connected to the virtual circuit is known, the mapping between the opposite terminal protocol address and DLCI can be created locally, and then the manual configuration can be avoided.

Description of the basic instructions of frame relay Inverse Address Resolution Protocol

router(config-if)#

Command	Description
frame-relay inverse-arp	Permits the sending of InARP (Inverse Address Resolution Protocol) request (the default).
frame-relay inverse-arp interval	Configures the time interval of sending InARP (Inverse Address Resolution Protocol) request (the default value is 60 seconds).
frame-relay inverse-arp ip <DLCI NUMBER>	Permits the sending of InARP (Inverse Address Resolution Protocol) request on a virtual circuit.
frame-relay inverse-arp update	Updates the dynamic mapping periodically.

Following illustration is a typical configuration example of frame relay Inverse Address Resolution Protocol.



The port S0 (3.3.3.1) of the local router router1 connects to the port S0 (3.3.3.2) of the opposite router router2.

Router1 configuration

Router1(config-if-serial0)# encapsulation frame-relay	
Router1(config-if-serial0)# frame-relay lmi-type ansi	The type of LMI
Router1(config-if-serial0)# frame-relay inverse-arp	Permits the sending frame relay InARP (the default)
Router1(config-if-serial0)#ip address 3.3.3.1 255.0.0.0	Local-end IP address
Router1(config-if-serial0)#frame-relay inverse-arp update	Updates the dynamic mapping periodically
Router1(config-if-serial0)#frame-relay interface-dlci 16	Configures the DLCI number

Router2 configuration

Router2(config-if-serial0)# encapsulation frame-relay	
Router2(config-if-serial0)# frame-relay lmi-type ansi	The type LMI.
Router2(config-if)# frame-relay inverse-arp	Permits the sending of the frame relay InARP (the default)
Router2(config-if-serial0)#ip address 3.3.3.2 255.0.0.0	Local IP address.
Router2(config-if-serial0)#frame-relay inverse-arp update	Updates the dynamic mapping periodically.
Router2(config-if-serial0)#frame-relay interface-dlci 16	Configures the DLCI number.

Debugging/monitoring of frame relay Inverse Address Resolution Protocol (InARP):

Displaying packets receiving/sending status of frame relay Reverse Address Resolution Protocol

```
show frame-relay inarp
Frame Relay Inarp statistics for interface serial2:
InARP requests sent 5, InARP replies sent 0
InARP request recvd 0, InARP replies recvd 4
```

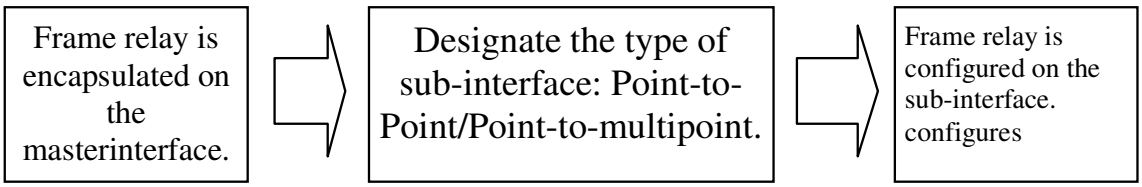
Displaying information of frame relay mapping:

```
show frame-relay map
serial0 (up): ip 3.3.3.2, dlci 16, dynamic,
IETF, status ACTIVE
```

The word dynamic among the above information indicates that the mapping is established dynamically via the Inverse Address Resolution Protocol (InARP).

Frame Relay Sub-interface

The configuration process of a frame relay sub-interface:



A sub-interface inherits the properties of a main interface, so before the sub-interface is configured, the frame relay should be encapsulated on the main interface. [LMI]

The configuration of frame relay point-to-point interface:
router(config)#

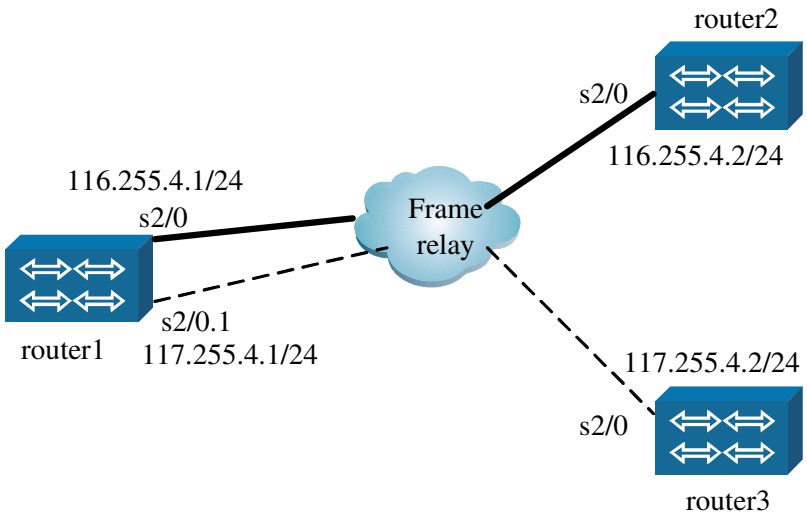
Command	Description
interface Serial <serialnumber.subnumber> point-to-point	Configure the sub-interface as the point-to-point mode
frame-relay interface-dlci number	Configure the number of the data link connection identifier (DLCI)
frame-relay ip rtp header-compression	Configure frame relay using RTP header compression (optional)
ip route peer-address A.B.C.D	Designate IP address of the opposite terminal (It is used in dynamic routing interaction)

The configuration of frame relay point-to-multipoint sub-interface

router(config)#

Command	Description
interface Serial <serialnumber.subnumber> point-to-multipoint	Configure the sub-interface as point-to-multipoint mode
frame-relay interface-dlci number	Configure the number of the data link connection identifier (DLCI)
frame-relay ip rtp header-compression	Configure frame relay using RTP header compression (optional)
frame-relay map ip ip_address dlci [broadcast|cisco|ietf]	Configure the frame relay MAP mapping

Frame Relay Sub-interface Configuration Example



The above example explains how to configure the sub-interface on the router A so as that the whole frame relay network can be connected. The router2 connects to the main interface of router1 while the router router3 connects to the sub-interface of router1.

Router1 configuration

Command	Task
Router1#configure terminal	
Router1(config)#interface s2	
Router1(config-if-serial2)#physical-layer sync	Synchronization
Router1(config-if-serial2)#clock rate 64000	Clock
Router1(config-if-serial2)#intf-type dte	Works in DTE mode of frame relay
Router1(config-if-serial2)#frame-relay lmi-type q933a	Designates LMI type as q933a
Router1(config-if-serial2)#frame-relay intf-type dte	
Router1(config-if-serial2)#frame-relay interface-dlci 102	The DLCI number
Router1(config-if-serial2)#frame-relay map ip 116.255.4.2 102 broadcast	Configures frame relay mapping
Router1(config-if-serial2)#ip address 116.255.4.1 255.255.255.0	Local-end IP address
Router1(config-if-serial2)#exit	
Router1(config)#interface serial2.1 multipoint	The mode of the sub-interface is point-to-multipoint
Router1(config-sub-if-serial2.1)#frame-relay interface-dlci 202	DLCI number is 202, which is provided by telecommunication office
Router1(config-sub-if-serial2.1)#frame-relay map ip 117.255.4.2 202 broadcast	Configures the frame relay mapping of the sub-interface
Router1(config-sub-if-serial2.1)#ip address 117.255.4.1 255.255.255.0	IP address of the sub-interface
Router1(config-sub-if)#end	

Router2 configuration (router3)

Command	Task
Router2# con t Router2(config)#interface serial2	
Router2(config-if-serial2)#physical-layer sync	
Router2(config-if-serial2)#clock rate 64000	
Router2(config-if-serial2)#encapsulation frame-relay	Encapsulates frame relay
Router2(config-if-serial2)#frame-relay lmi-type q933a	Designates LMI type as q933a
Router2(config-if-serial2)#frame-relay interface-dlci 101	The DLCI number is 101
Router2(config-if-serial2)#frame-relay map ip 116.255.4.1 101 broadcast	Configures the frame relay mapping
Router2(config-if-serial2)#ip address 116.255.4.2 255.255.255.0	IP address
Router2(config-if-serial2)#exit	

Frame Relay Switch

Commands

Signamax routers supports the function of frame relay switching. Frame relay switches makes the router able to encapsulate the data frame of frame relay into IP datagrams.

```
router(config)#frame-relay switching
```

Configuring it as a frame relay switch

```
router(config)#
```

Command	Description
Frame-relay swithig	Configures it as a frame relay switch

Configure the router, via the commmand frame-relay switching to execute the switch function in frame relay network.

When the router runs as a Router(config)#frame-relay switching switch, data stream can be exchanged between two serial ports of the router via the command frame-relay. The router executes PVC data exchange between two serial ports.

router(config-if-XXX)#frame-relay route in-dlci out-interface out-dlci

The command frame-relay switching

```
Router(config-if-XXX)#
```

Command	Description
In-dlci	The DLCI number of packets received by the interface
Out-interface	The interface used by the router to transmit packets
Out-dlci	The DLCI number used by the router to transmit packets via the designated outward interface

The interface configuration can be applied to frame relay switch via the command frame-relay intf-type. The type of frame relay switch is decided by the functions of the router in frame relay network.

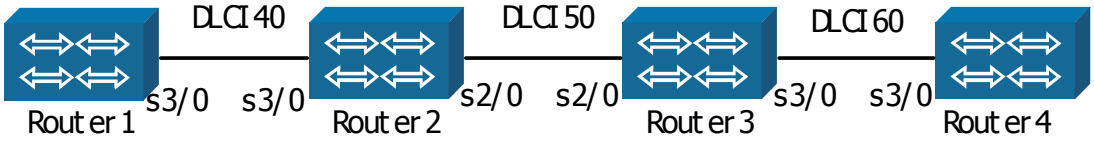
```
router(config-if-XXX)#frame-relay intf-type [dte |dce
|nni]
```

The command Frame-relay intf-type

```
Router(config-if-XXX)#
```

Command	Description
Dte	The interface of the router is used to connect a frame relay network
Dce	The interface of the router connectes with a router, and the local router is used as a frame relay switch
Nni	The router is used as a switch. The interface is connected with another switch and supports the network-to-network interface (NNI)

Frame Relay Serving as Switch



router2 and router3 serve as frame relay switches while router1 and router4 serve as DTE interfaces. When the data stream from router1 arrives at the port s3 of router2, the data stream with DLCI number 40 will be handed to the output port s2; at the same time, DLCI number 50 will be used in the source identifier.

Data stream is transmitted to the port s2of router3. Similarly, the data stream with DLCI number 50 is handed to the output port s3 again, so the data stream arrives at router4. The data from router4 can arrive at the destination router1 according to the same principle, too.

Router1 configuration:

Command	Task
router1(config)#int s3	Enters the interface mode
router1(config-if-serial3)#physical-layer sync	Configures it as the synchronization mode
router1(config-if-serial3)#encapsulation frame-relay	Encapsulates the protocol frame-relay
router1(config-if-serial3)#frame-relay lmi-type ansi	Configures LMI type
router1(config-if-serial3)#frame-relay interface-dlci 40	Configures DLCI number
router1(config-if-serial3)#frame-relay map ip 1.0.0.2 40 broadcast	Configures MAP mapping
router1(config-if-serial3)#ip address 1.0.0.1 255.0.0.0	Configures IP address

router1(config-if-serial3)#exit	Configuration has been finished

Router2 configuration:
Router(config-if-serial2)#

Command	Task
Configuration of the interface S3	
router2(config)#frame-relay switching	Configures it as the frame relay switch mode
router2(config)#int s3	Enters the interface mode
router2(config-if-serial3)#physical-layer sync	Configures it as the synchronization mode
router2(config-if-serial3)#clock rate 128000	Configures the clock
router2(config-if-serial3)#encapsulation frame-relay	Encapsulates the protocol frame-relay
router2(config-if-serial3)#frame-relay lmi-type ansi	Configures the LMI mode
router2(config-if-serial3)#frame-relay intf-type dce	Configures it as a frame relay switch to connect with another router
router2(config-if-serial3)#frame-relay route 40 interface serial2 50	Configures the direction for switch to transmit data
router2(config-if-serial3)#exit	Configuration has been finished
The configuration of the interface S2:	
router2(config-if-serial2)#physical-layer sync	Configures it as the synchronization mode
router2(config-if-serial2)#encapsulation frame-relay	Encapsulates the protocol frame-relay
router2(config-if-serial2)#frame-relay lmi-type ansi	Configures LMI mode
router2(config-if-serial2)#frame-relay intf-type nni	Configures it as the switch mode (NNI) to connect with another switch
router2(config-if-serial2)#frame-relay route 50 interface serial3 40	Configures the direction for switch to transmit data
router2(config-if-serial2)#exit	Configuration has been finished

Configuration of router3:
Router(config-if-serial2)#

Command	Task
Configuration of the interface S3	
Router3(config)#frame-relay switching	Configures it as the frame relay exchange mode
Router3(config)#int s3	Enters the interface mode
Router3(config-if-serial3)#physical-layer sync	Configures it as the synchronization mode
Router3(config-if-serial3)#clock rate 128000	Configures clock
Router3(config-if-serial3)#encapsulation frame-relay	Encapsulates the protocol frame-relay.
Router3(config-if-serial3)#frame-relay lmi-type ansi	Configures LMI mode.
Router3(config-if-serial3)#frame-relay intf-type dce	Configures it as a frame relay switch

	to connect with another router.
Router3(config-if-serial3)#frame-relay route 60 interface serial2 50	Configures the direction for switch to transmit data.
router2(config-if-serial3)#exit	Configuration has been finished.
The configuration of the interface S2:	
Router3(config-if-serial2)#physical-layer sync	Configures it as the synchronization mode.
Router3(config-if-serial2)#encapsulation frame-relay	Encapsulates the protocol frame-relay.
Router3(config-if-serial2)#frame-relay lmi-type ansi	Configures LMI mode.
Router3(config-if-serial2)#frame-relay intf-type nni	Configures it as the switch mode (NNI) to connect with another switch.
Router3(config-if-serial2)#frame-relay route 50 interface serial3 60	Configures the direction for switch to transmit data.
Router3(config-if-serial2)#Clock rate 128000	Configures clock.
Router3(config-if-serial2)#exit	Configuration has been finished.

The configuration of router4:

Command	Task
router1(config)#int s3	Enters the interface mode.
router1(config-if-serial3)#physical-layer sync	Configures it as the synchronization mode.
router1(config-if-serial3)#encapsulation frame-relay	Encapsulates the protocol frame-relay.
router1(config-if-serial3)#frame-relay lmi-type ansi	Configures LMI type.
router1(config-if-serial3)#frame-relay interface-dlci 60	Configures DLCI number.
router1(config-if-serial3)#frame-relay map ip 1.0.0.1 60 roadcast	Configures MAP mapping.
router1(config-if-serial3)#ip address 1.0.0.2 255.0.0.0	Configures the IP address.
router1(config-if-serial3)#exit	Configuration has been finished

The DLCI numbers between switches do not need to be configured in ports.

Different LMI types can be configured on different ports and the same LMI type is unnecessary. But the LMI between two routers should be the same.

Examine whether the function of switch works well via the command show frame-relay route. If S2 and S3 are showed as active, this indicates that the function of switch works well.

Frame-relay Traffic Shaping

map-class frame-relay

Use the command map-class frame-relay to specify a map type for some PVC to define Quality of Service (QoS); or, use the negation of the command to delete related map type.

```
map-class frame-relay map-class-name
no map-class frame-relay map-class-name
```

Command	Task
frame-relay	The keyword of the specified map type.
map-class-name	The name of the map type.

(By default) The command is disabled. And no default name is defined.
(Command mode)The global configuration mode.

frame-relay traffic-rate

Use the command frame-relay traffic-rate to specify the egress flow rate for the PVC related with some map type; or, use the negation of the command to restore the default flow rate.

```
frame-relay traffic-rate average [ peak ]
no frame-relay traffic-rate average [ peak ]
```

Command	Task
Average	The average rate (by bit per second), equivalent to the specified CIR.
Peak	(Optional)the peak rate (by bit per second), equivalent to CIR + Be/Tc = CIR(1 + Be/Bc) = CIR + EIR

(By default) If the peak rate is omitted, the adopted default value is the line rate.

(Command mode)the map type configuration mode.

frame-relay adaptive-shaping

Use the command frame-relay adaptive-shaping to specify the rate adjust mode for the PVC related with some map type; or, use the negation of the command to deny the rate adjust.

```
frame-relay adaptive-shaping { becn | foresight}
```

```
no frame-relay adaptive-shaping
```

Command	Task
Becn	Perform the rate adjust according to BECN message.
Foresight	Perform the rate adjust according to foresight message.

(By default) The command is disabled.
(Command mode)the map type configuration mode.

frame-relay custom-queue-list
Use the command frame-relay custom-queue-list to specify the custom-queue for the PVC related with some map type; or, use the negation of the command to restore the default value of the PVC queue.

```
frame-relay custom-queue-list list-number
no frame-relay custom-queue-list list-number
```

Command	Task
list-number	The list-number of the queue.

(By default) The default queue is FIFO (First In First Out).
(Command mode)the map type configuration mode.

frame-relay priority-group
Use the command frame-relay priority-group to specify the priority queue for the PVC related with some map type; or, use the negation of the command to restore the default value of the PVC queue.

```
frame-relay priority-group list-number
no frame-relay priority-group list-number
```

Com mand	Task
list-number	The list-number of the queue.

(By default) The default queue is FIFO.
(Command mode)the map type configuration mode.

frame-relay traffic-shaping
Use the command frame-relay traffic-shaping to enable traffic shaping for all PVC of a frame-relay interface; or, use the negation of the command to disable the function of traffic shaping.

```
frame-relay traffic-shaping
no frame-relay traffic-shaping
```

(By default) The command is disabled.
(Command mode)the interface configuration mode.

frame-relay class
Use the command frame-relay class to relate a map type with an interface or a sub-interface; or, use the negation of the command to cancel the relation.

```
frame-relay class name
no frame-relay class name
```

Command	Task
name	The name of the map class related with the interface/sub-interface.

(By default) There exists no relation.
(Command mode)the interface configuration mode.

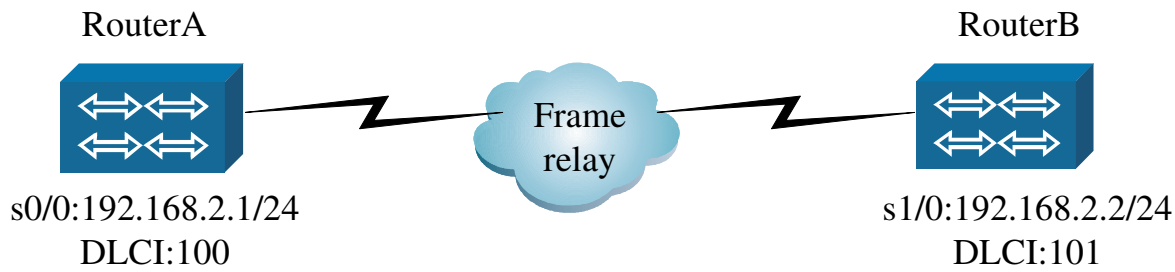
class
Use the command to relate a map type to some PVC; or, use the negation of the command to cancel the relation.

```
class name
no class name
```

Command	Task
Name	The name of the map class related with the PVC.

(By default) There exists no relation.
(Command mode)the DLCI configuration mode.

Frame relay traffic shaping configuration example:



An interconnection between RouterA (the port s0/0 192.168.2.1) and RouterB (the port s1/0 192.168.2.2) is established via a frame-relay network. The frame-relay traffic shaping policy is adopted to limit data transmission rate over the specified PVC between RouterA and RouterB and provide high priority service for Telnet data transmission between RouterA and RouterB.

RouterA is configured as follows.

Syntax	Description
RouterA#configure terminal	
RouterA(config)# priority-list 1 protocol ip high tcp 23	Configure a priority queue and set QoS of Telnet as high.
RouterA(config)# map-class frame-relay name	Establish a map for PVC.
RouterA(config-map-class)# frame-relay traffic-rate 9600 128000	Specify the egress flow rate and peak rate for the PVC related with the map type.
RouterA(config-map-class)# frame-relay priority-group 1	Specify the priority queue for the PVC related with the map type.
RouterA(config-map-class)# exit	
RouterA(config)# interface serial0/0	Enter the interface S0/0 configuration mode.
RouterA(config-if-serial0/0)# physical-layer sync	
RouterA(config-if-serial0/0)# encapsulation frame-relay	Perform the frame-relay encapsulation.
RouterA(config-if-serial0/0)# frame-relay lmi-type ansi	Configure the LMI type .
RouterA(config-if-serial0/0)# frame-relay traffic-shaping	Make traffic shaping effective on the frame-relay interface.
RouterA(config-if-serial0/0)# frame-relay interface-dlci 100	Configure the local DLCI number.
RouterA(config-fr-dlci)# class name	Relate the map type with the specified PVC.
RouterA(config-fr-dlci)#exit	Exit the DLCI configuration mode.
RouterA(config-if-serial0/0)# frame-relay map ip 192.168.2.2 100	Configure the frame-relay address map.
RouterA(config-if-serial0/0)# ip address 192.168.2.1 255.255.255.0	Configure the IP address.
RouterA(config-if-serial0/0)# priority-group 2	Enable the PQ queue on the interface (the serial-number is not consistent with the defined one.)
RouterA(config-if-serial0/0)# end	

The simple frame-relay configuration is performed on RouterB.

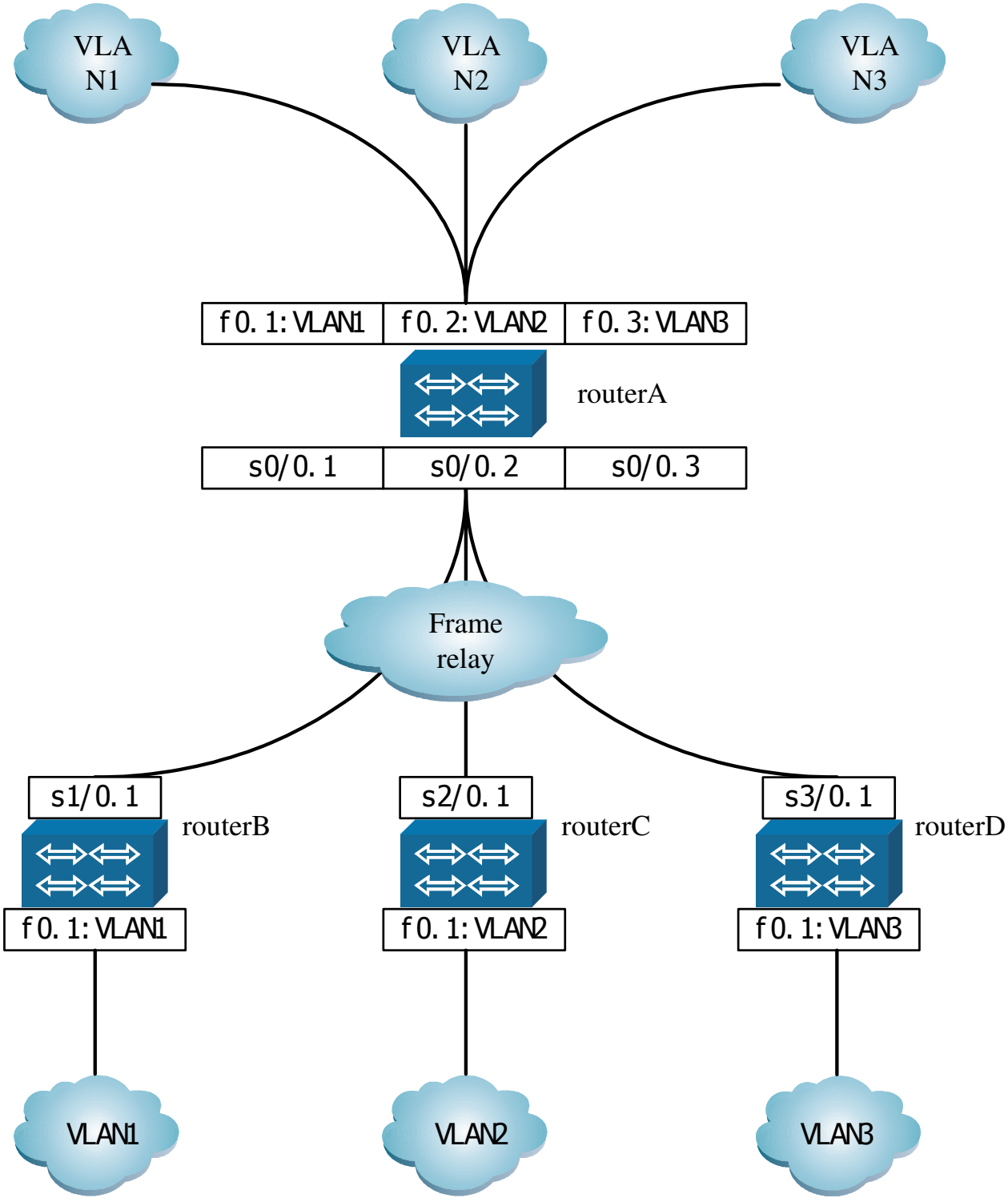
Frame-relay Bridging VLAN

vlan-bridge

Use the command vlan-bridge to make the frame-relay network bridge VLAN; or, use the negation of the command to deny bridging VLAN.
Vlan-bridge vlan-interface

Command	Task
vlan-interface	The VLAN interface to be bridged.

(By default) The command is denied.
(Command mode)The point-to-point sub-interface configuration mode.



Frame relay bridging VLAN configuration example

As shown in figure above, in the one-point-to-multi-point frame-relay network, all routers are required to adopt the point-to-point sub-interface configuration mode. The interface f0 of RouterA has three sub-interfaces that belong to three different VLANs.

And the interface S0/0 also has three sub-interfaces that are related with three different VLANs; the interface f0.1 of RouterB belongs to Vlan1 and the interface s1/0.1 is related with Vlan1; the interface f0.1 of RouterC

belongs to Vlan2 and the interface s2/0.1 is related with Vlan2; the interface f0.1 of RouterD belongs to Vlan3 and the interface s3/0.1 is related with Vlan3.

RouterA is configured as follows:

Syntax	Description
RouterA# configure terminal	
RouterA(config)# interface fastethernet0.1	Enter the sub-interface f0.1 configuration mode.
RouterA(config-if-fastethernet0.1)# encapsulation dot1q 1	Encapsulate the sub-interface to Vlan1.
RouterA(config-if-fastethernet0.1)# interface fastethernet0.2	Enter the sub-interface f0.2 configuration mode.
RouterA(config-if-fastethernet0.2)# encapsulation dot1q 2	Encapsulate the sub-interface to Vlan2.
RouterA(config-if-fastethernet0.2)# interface fastethernet0.3	Enter the sub-interface f0.3 configuration mode.
RouterA(config-if-fastethernet0.3)# encapsulation dot1q 3	Encapsulate the sub-interface to Vlan3.
RouterA(config-if-fastethernet0.3)# interface serial0/0	Enter the interface s0/0 configuration mode.
RouterA(config-if-serial0/0)# physical-layer sync	
RouterA(config-if-serial0/0)# encapsulation frame-relay	Perform the frame-relay encapsulation for the interface S0/0.
RouterA(config-if-serial0/0)# frame-relay lmi-type ansi	Set the LMI type.
RouterA(config-if-serial0/0)# interface serial0/0.1 point-to-point	Enter the sub-interface s0/0.1 configuration mode.
RouterA(config-if-serial0/0.1)# frame-relay interface-dlci 100	Configure the local DLCI number.
RouterA(config-if-serial0/0.1)# vlan-bridge fastethernet0.1	Make S0/0.1 relate with F0.1 and bridge related VLAN.
RouterA(config-if-serial0/0.1)# interface serial0/0.2 point-to-point	Enter the sub-interface s0/0.2 configuration mode.
RouterA(config-if-serial0/0.2)# frame-relay interface-dlci 200	Configure the local DLCI number.
RouterA(config-if-serial0/0.2)#vlan-bridge fastethernet0.2	Make S0/0.2 relate with F0.2 and bridge related VLAN.
RouterA(config-if-serial0/0.2)# interface serial0/0.3 point-to-point	Enter the sub-interface s0/0.3 configuration mode.
RouterA(config-if-serial0/0.3)# frame-relay interface-dlci 300	Configure the local DLCI number.
RouterA(config-if-serial0/0.3)#vlan-bridge fastethernet0.3	Make S0/0.3 relate with F0.3 and bridge related VLAN.

RouterB is configured as follows.

Syntax	Description
RouterB# configure terminal	
RouterB(config)# interface fastethernet0.1	Enter the sub-interface f0.1 configuration mode
RouterB(config-if-fastethernet0.1)# encapsulation dot1q 1	Encapsulate the sub-interface to Vlan1
RouterB(config-if-fastethernet0.1)# interface serial1/0	Enter the interface S1/0 configuration mode
RouterB(config-if-serial1/0)# physical-layer sync	
RouterB(config-if-serial1/0)# encapsulation frame-relay	Perform the frame-relay encapsulation for the interface s1/0
RouterB(config-if-serial1/0)# frame-relay lmi-type ansi	Set the LMI type
RouterB(config-if-serial1/0)# interface serial1/0.1 point-to-point	Enter the sub-interface S1/0.1 configuration mode
RouterB(config-if-serial1/0.1)# frame-relay interface-dlci 101	Configure the local DLCI number
RouterB(config-if-serial1/0.1)# vlan-bridge fastethernet0.1	Make S1/0.1 relate with F1.1 and bridge related VLAN
RouterB(config-if-serial1/0.1)# end	

RouterC is configured as follows.

Syntax	Description
RouterC# configure terminal	
RouterC(config)# interface fastethernet0.1	Enter the sub-interface f0.1 configuration mode
RouterC(config-if-fastethernet0.1)# encapsulation dot1q 2	Encapsulate the sub-interface to Vlan2
RouterC(config-if-fastethernet0.1)# interface serial2/0	Enter the interface S2/0 configuration mode
RouterC(config-if-serial2/0)# physical-layer sync	
RouterC(config-if-serial2/0)# encapsulation frame-relay	Perform the frame-relay encapsulation for the interface S2/0
RouterC(config-if-serial2/0)# frame-relay lmi-type ansi	Set the LMI type
RouterC(config-if-serial2/0)# interface serial2/0.1 point-to-point	Enter the sub-interface S2/0.1 configuration mode
RouterC(config-if-serial2/0.1)# frame-relay interface-dlci 201	Configure the local DLCI number
RouterC(config-if-serial2/0.1)# vlan-bridge fastethernet0.1	Make S2/0.1 relate with f0.1 and bridge related VLAN
RouterC(config-if-serial2/0.1)# end	

RouterD is configured as follows.

Syntax	Description
RouterD# configure terminal	
RouterD(config)# interface fastethernet0.1	Enter the sub-interface f0.1 configuration mode
RouterD(config-if-fastethernet0.1)# encapsulation dot1q 3	Encapsulate the sub-interface to Vlan3
RouterD(config-if-fastethernet0.1)# interface serial3/0	Enter the interface S3/0 configuration mode
RouterD(config-if-serial3/0)# physical-layer sync	
RouterD(config-if-serial3/0)# encapsulation frame-relay	Perform the frame-relay encapsulation for the interface s3/0
RouterD(config-if-serial3/0)# frame-relay lmi-type ansi	Set the LMI type
RouterD(config-if-serial3/0)# interface serial3/0.1 point-to-point	Enter the sub-interface S3/0.1 configuration mode
RouterD(config-if-serial3/0.1)# frame-relay interface-dlci 301	Configure the local DLCI number
RouterD(config-if-serial3/0.1)# vlan-bridge fastethernet0.1	Make S3/0.1 relate with F0.1 and bridge related VLAN
RouterD(config-if-serial3/0.1)# end	

Vlan-bridge is required to adopt the point-to-point sub-interface configuration mode.

Frame-Relay PVC Compression

Frame Relay PVC Compression Configuration Command

frame-relay map ip ipaddress dlci tcp header-compress [passive]

Use TCP/IP header compression function on frame relay PVC via this command.

Command	Task
passive	Passive mode header compression

(Default status)disable compression

frame-relay map ip ipaddress dlci rtp header-compress [passive]

Use RTP header compression function on frame relay PVC via this command.

Command	Task
passive	Passive mode header compression

(Default status)disable compression

frame-relay map ip ipaddress dlci compress [passive]
Use TCP/IP and RTP header compression function on frame relay PVC via this command.

Command	Task
passive	Passive mode header compression

(Default status)disable compression

frame-relay map ip ipaddress dlci nocompress
Disable TCP/IP and RTP header compression function on frame relay PVC via this command.

(Default status)disable compression

frame-relay ip tcp header-compress

Use TCP/IP header compression function on frame relay all PVC via this command. No format is used to disable this function.

```
frame-relay ip tcp header-compress [passive]
no frame-relay ip tcp header-compress
```

Command	Task
passive	Passive mode header compression.

(Default status)disable compression

frame-relay ip rtp header-compress
Use RTP header compression function on frame relay all PVC via this command. No format is used to disable this function.

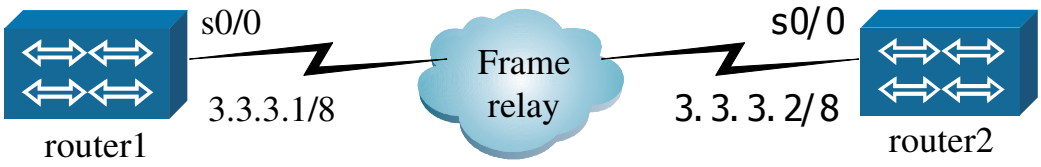
```
frame-relay ip rtp header-compress [passive]
no frame-relay ip rtp header-compress
```

Command	Task
passive	Passive mode header compression

(Default status)disable compression

Frame Relay PVC Compression Example

TCP/IP Header Compression over Frame Relay PVC



Router1 is configured as follows :

Command	Task
RouterA# configure terminal	
RouterA(config)# interface serial0/0	Enter the interface Serial0/0 configuration mode
RouterA(config-if-serial0/0)# physical-layer sync	
RouterA(config-if-serial0/0)# encapsulation frame-relay	Enable frame-relay encapsulation for the interface S0/0
RouterA(config-if-serial0/0)# frame-relay lmi-type ansi	Set the type as LMI
RouterA(config-if-serial0/0)# frame-relay interface-dlci 100	Configure the local DLCI number
RouterA(config-if-serial0/0)# frame-relay map ip 3.3.3.2 100 tcp header-compress	Configure the TCP/IP header compression on DLCI=100 PVC
RouterA(config-if-serial0/0)# ip address 3.3.3.1 255.0.0.0	Configure the interface IP address

Router2 is configured as follows:

Command	Task
RouterB# configure terminal	
RouterB(config)#interface serial0/0	Enter the interface S0/0 configurationo mode
RouterB(config-if-serial0/0)# physical-layer sync	
RouterB(config-if-serial0/0)# clock rate 128000	
RouterB(config-if-serial0/0)# encapsulation frame-relay	Enable the frame-relay encapsulatin for the interface s0/0
RouterB(config-if-serial0/0)# frame-relay lmi-type ansi	Set the type as LMI
RouterB(config-if-serial0/0)# frame-relay interface-dlci 100	Configure the local DLCI number
RouterB(config-if-serial0/0)# frame-relay map ip 3.3.3.1 100 tcp header-compress	Configure the TCP/IP header compression on DLCI=100 PVC
RouterB(config-if-serial0/0)# ip address 3.3.3.2 255.0.0.0	Configure the interface IP address

Examine whether the data packet is being compressed via command show frame-relay ip tcp header-compress.

RTP header compression example on frame relay PVC:

Router1 is configured as follows:

Command	Task
RouterA# configure terminal	
RouterA(config)# interface serial0/0	Enter the interface Serial0/0 configuration mode
RouterA(config-if-serial0/0)# physical-layer sync	
RouterA(config-if-serial0/0)# encapsulation frame-relay	Enable frame-relay encapsulation for the interface S0/0
RouterA(config-if-serial0/0)# frame-relay lmi-type ansi	Set the type as LMI
RouterA(config-if-serial0/0)# frame-relay interface-dlci 100	Configure the local DLCI number
RouterA(config-if-serial0/0)# frame-relay map ip 3.3.3.2 100 rtp header-compress	Configure the TCP/IP header compression on DLCI=100 PVC
RouterA(config-if-serial0/0)# ip address 3.3.3.1 255.0.0.0	Configure the interface IP address

Router2 is configured as follows :

Command	Task
RouterB# configure terminal	
RouterB(config)#interface serial0/0	Enter the interface Serial0/0 configuration mode
RouterB(config-if-serial0/0)# physical-layer sync	
RouterB(config-if-serial0/0)# clock rate 128000	
RouterB(config-if-serial0/0)# encapsulation frame-relay	Enable frame-relay encapsulation for the interface S0/0
RouterB(config-if-serial0/0)# frame-relay lmi-type ansi	Set the type as LMI
RouterB(config-if-serial0/0)# frame-relay interface-dlci 100	Configure the local DLCI number
RouterB(config-if-serial0/0)# frame-relay map ip 3.3.3.1 100 rtp header-compress	Configure the TCP/IP header compression on DLCI=100 PVC
RouterB(config-if-serial0/0)# ip address 3.3.3.2 255.0.0.0	Configure the interface IP address

Monitoring of RTP Compression over Frame-Relay PVC:

Use the command show frame-relay ip rtp header-compress to show RTP compression information about whether the tranmitted data is compressed and related compression statistics.

The command frame-relay ip tcp header-compress/ frame-relay ip rtp header-compres is valid to all PVCs (except the PVCs for which the RTP compression has bee configured singly).

It can be examined by the command show frame-relay ip tcp header-comress/show frame-relay ip rtp header-compress that the RTP compression has been configured on PVC and its type is inherited.

For a single PVC on which the RTP has been configured, it can be known by the command that its compression type is enabled.

DE Bit Support on Frame-Relay

Configuration Command

frame-relay de-list

To enable the DE bit list in the frame-relay network, use the command frame-relay de-list, or else, use the negation of the command to disable it.

```
frame-relay de-list list-number protocol ip {fragments | gt
size| list access-list-number
| lt size| tcp port| udp port}
```

Command	Description
List-number	DE list number
Size	Packet size
Access-list-number	Access list number
Port	The port number of the destination address

(By default) disabled
(Command mode)the globe configuration mode.

frame-relay de-group

To eable DE bit discarding rule on DLCI, use the command frame-relay de-group, or else, use the negation of the command to disable it.

Frame-relay de-goup de-list-number dlci

Command	Description
De-list-number	DE list number
Dlci	DLCI number

(By default) disabled
(Command mode)the interface configuration mode

frame-relay congestion-management

To enable the DE rule on an interface, use the command frame-relay congestion-management, or else, use the negation of the command to disable it.

```
(By default) disabled.
```

(Command mode)the interface configuration mode

Configuration Examples

An example of the configuration command DE-list frame-relay de-list

```
define DE list 1 for IP fragment packets    / Set DE bit for
packets of the IP fragment.

frame-relay de-list 1 protocol ip fragment
define DE list 2 for port 500 of UDP packets  / Set DE bit
for UDP packets whose port number is 500.

frame-relay de-list 2 protocol ip udp 500
```

An example of the configuration command de-group frame-relay de-group

```
Enable DE list 1 on PVC 100   /Enable the rule de-list 3 on
DLCI-number=100 PVC for setting DE bit.

frame-relay de-group 1 100
```

Only one kind of rule can be set in each DE-list. Multiple de-lists canbe enabled on each PVC, and one de-list can also be used in different PVCs. To enable DE, it is necessary to configure the command frame-relay congestion-management on the interface. DE cannot take effect until traffic-shapping is configured.

Monitoring DE bit over Frame-Relay

Use the command show frame-relay PVC to show the statistics of received/transmitted packets for which DE bit has been configured.

Frame-Relay Fragment

frame-relay fragment

To enable frame-relay fragment function, use the command frame-relay fragment number, or else, use the negation of the command to disable it. Abour related details, refer to FRF.12.

frame-relay fragment number

Command	Description
Number	Fragment size(By byte)

(By default) disabled
(Command mode)the map-class configuration mode .

```
frame-relay fragment should-encap-mulproto
```

After the frame fragment function is configured, to perform the multilink encapsulation for network-layer packet whose size is less than the frame fragment, use the command frame-relay fragment should-encap-mulproto, or else, use the negation of the command to disable it.

(By default) disabled
(Command mode)the map-class configuration mode

It is unnecessary to configure the command. The command need be enabled only when opposite equipment performs the multilink encapsulation for network-layer packet whose size is less than the frame fragment or implements the strict order-limit to network-layer data.

The frame fragment function cannot take effect until the traffic-shapping is enabled.

Virtual Ethernet Bridge Protocol

Overview

Virtual Ethernet bridge protocol is a special bridge protocol of Signamax. The protocol creates a virtual Ethernet interface, and then makes data bridge between WAN interface and virtual Ethernet interface.

After encapsulating this protocol, Ethernet frame can be sent and accepted. Because of the existence of virtual Ethernet interface, Ethernet frame is sent and accepted via virtual ehternet interface.

Configuration Command

Command	Description	Config mode
interface virtualethernet unit[.subunit]	Set up a virtual Ethernet interface	config
encapsulation virtualethernet virtualethernet unit	Encapsulate virtual Ethernet bridge protocol on WAN interface	config-if-××
veth-macaddr macaddress	Designate virtual Ethernet interface MAC address	config-if-××

interface virtualethernet
Use this command to set up a virtual Ethernet interface. No is used to delete the interface.

```
interface virtualethernet unit[.subunit]
no interface virtualethernet unit[.subunit]
```

Command	Description
unit	Virtual Ethernet interface unit number, and range is 0～255, the system supports 256 virtual Ethernet interfaces
subunit	Virtual Ethernet interface unit number, and range is 0～1023,each virtual Ethernet interface supports 1023 sub-interface (sub-interface 0 is main interface)

(Default status)no virtual Ethernet interface is set up

encapsulation virtualethernet virtualethernet
Encapsulate virtual Ethernet bridge protocol on WAN interface, to send and accept Ethernet frame.

```
encapsulation virtualethernet virtualethernet unit
```

Command	Description
unit	Virtual Ethernet interface unit number, and range is 0～255,the system supports 256 virtual Ethernet interfaces

(Default status)encapsulate link layer protocol HDLC by default.

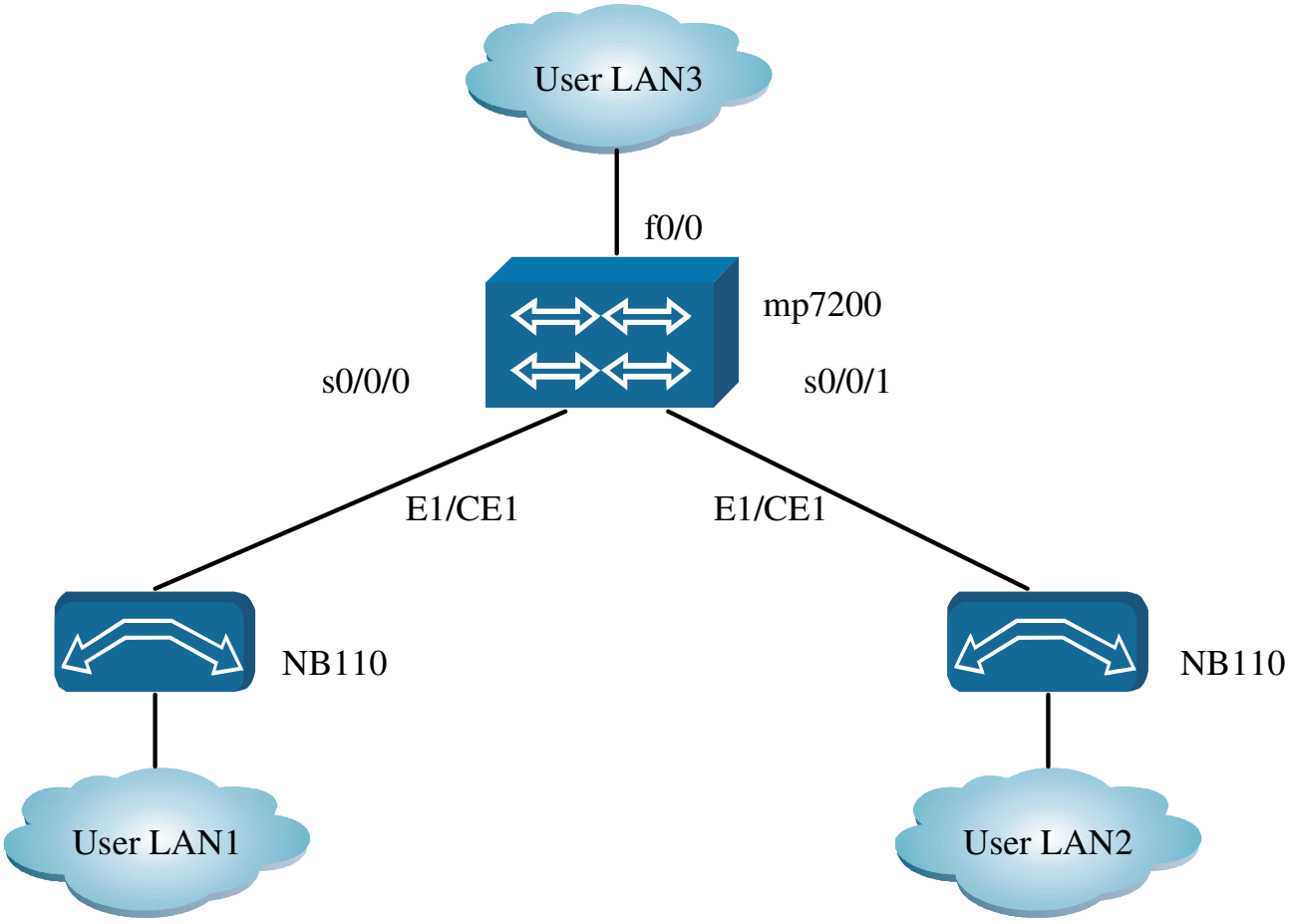
veth-macaddr
designate virtual Ethernet interface MAC address. No is used to renew MAC address.

```
veth-macaddr macaddress
no veth-macad(Default status)create MAC address by system
```

Command	Description
macaddress	MAC address

Configuration Example

Virtual Ethernet bridge protocol configuration comprises setting vrtual Ethernet interface and encapsulating virtual Ethernet interface.



Virtual-ethernet protocol configuration example

MP7200 connects NB110 via E1/CE1, via virtual Ethernet bridge protocol. Seeing from all LAN users, it seems NB110 is some virtual Ethernet interface on MP7200, which provides all the functions by Ethernet protocol.

MP7200 configuration:

Command	Description
mp7200(config)#int virtualethernet0	Create virtual Ethernet interface and enter interface mode
mp7200(config-if- virtualethernet0)# ip address 3.1.1.1 255.0.0.0	Configure IP address of interface
mp7200 (config-if- virtualethernet0)#exit	Exit to interface configuration mode
mp7200(config)#int virtualethernet1	Create virtual Ethernet interface and enter interface mode
mp7200(config-if- virtualethernet0)# ip address 4.1.1.1 255.0.0.0	Configure IP address of interface
mp7200 (config-if- virtualethernet0)#exit	Exit to interface configuration mode
mp7200(config)#int s0/0/0	Enter E1/CE1 interface mode
mp7200(config-if-serial1/0)#physical-layer sync	Configure synchronous mode of interface
mp7200(config-if-serial1/0)#encapsulation virtualethernet virtualethernet 0	Encapsulate virtual-ethernet protocol, and bridge WAN interface and virtualethernet0
mp7200(config-if-serial1/0)#exit	Exit to interface configuration mode
mp7200(config)#int s0/0/1	Enter E1/CE1 interface mode
mp7200(config-if-serial1/0)#physical-layer sync	Configure synchronous mode of interface
mp7200(config-if-serial1/0)#encapsulation virtualethernet virtualethernet 1	Encapsulate virtual-ethernet protocol, and bridge WAN interface and virtualethernet0
mp7200(config-if-serial1/0)#exit	Exit to interface configuration mode

After encapsulating virtual Ethernet bridge protocol, the above layer protocol cannot be showed. The IP address etc. configurations should be done on virtual Ethernet interface. Virtual Ethernet interface MAC address system is created random.

If the there is a conflict between the address and MAC interface, you can modify MAC address. After the modification, the interface will be DOWN and UP to send ARP update. This will be happen after restartup of saving configuration.

Network Protocol

Signamax's MP Series routers supports Internet network protocols. The Internet Protocol is the protocol based on packets and is used to exchange data via a computer network. IP is the foundation of all other protocols in the Internet protocol stack. IP deals with addressing, fragmenting, reassembling and disassembling of the protocol information; datagrams.

As the network layer protocol, IP processes address routing and controls the transmission of data packets. As network layer protocols, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are established on the IP layer.

TCP is a connection-based protocol, which provides the reliable data transmission service while UDP is connectionless protocol, which provides unreliable data transmission service.

MP series routers support all the demands prescribed in the RFC of Internet Protocol (IP), which comprises the services such as IP, ICMP, IGMP, TCP, and UDP etc.

IP Address Configuration

IP Addressing

An IP address is a 32-bit number assigned to every device which runs the IP protocol and connects to the Internet. IP addresses are used to designate a network connection IP addresses are divided into five classes for convenience, and each IP addresses is divided into two parts:

Network number - Designates the network to which each device belongs.

Host number - Designates the host number of each device on its network lists the classes and ranges of IP Addresses.

Classes and ranges of IP addresses.

Address type	Valid Ranges of IP address	Explanation
A	0.0.0.0-127.255.255.255	The network number 127 is used for loopback interface.
B	128.0.0.0-191.255.255.255	A host number, whose bits are all 1, is used for a broadcast over its network.
C	192.0.0.0-223.255.255.255	A host number, whose bits are all 1, is used for a broadcast over its network.
D	224.0.0.0-239.255.255.255	Class D addresses are used for Multicast
E	240.0.0.0-247.255.255.255	Class E addresses are reserved for later use.

Usually, IP addresses of different classes are intended for use in different network systems. For large-scale network systems, Class A addresses are used, while Class B and Class C IP addresses would most likely be used for medium and small scale network systems. Class D and E addresses are reserved for special use.

With the development of the Internet, the IP addresses become limited and class address distribution can lead to the wasting of IP addresses. To solve this problem the concept of "subnet" has emerged. A "subnet" uses several bits of a host bits of a net address as the subnet, so the same network address can span mutliple physical networks.

Signamax's MP Series routers support the following IP address features:

Supports the feature of network address with classes

Supports subnetting properties of network addresses

Supports CIDR properties of classless routing

Allocates several IP addresses to a network interface in a broadcast network (for example, Ethernet)

Permits the use of unnumbered IP addresses on a serial-port interface to save addresses.

Supports EASY IP and NAT

IP Address Configuration Command

Command	Description	Config mode
ip address ip-address mask	* configure main IP address of interface	config-if-××
ip address ip-address mask secondary	* configure secondary IP address of interface	config-if-××
no ip address	Delete all configured IP address on interface	config-if-××
ip unnumber	Configure interface using IP unnumber mechanism	config-if-××
ip address negotiated	Configure interface using IP address negotiation	config-if-××

"*" before command means it has configuration example description.

```
configuration mode is : config, config-if-××(interface name)
config-××(protocol name) etc.
```

Allocating IP Address to Interface

An interface often has a primary IP address. The following tasks should be done in the interface configuration mode to allocate a primary IP address and network mask to a network interface.

Command	Description
Ip adderss <ip-address> <mask>	Set master IP address for the interface

A subnet mask is used to identify the network number of an IP address. When a mask is used to determine a subnet in a network, the mask is regarded as a subnet mask.

Signamax MP series routers only support network masks which are composed of several continuous "1" bits with left alignment.

In addition, Signamax MP series routers supports the assigning of many IP addresses to a broadcasting/multicasting network interface. So you can assign some unlimited secondary addresses, which can be used in various occasions.

There may not be enough host addresses for a given network section. For instance, your subnet allows up to 254 host addresses for a logical subnet, however, your physical subnet has 300 actual host addresses. Two logical subnets on the physical subnet can exist after introducing secondary IP addresses to a router or an access server.

In the past, many networks used Layer-2 bridges, instead of subnets. The use of the secondary addresses can help covert the network into a subnet, which is a network based on routers. A bridge router in an old network can easily establish several subnets in this network segment.

Two subnets in a single network can be separated by another network under other conditions. You can establish a network from subnets, so that these subnets can be separated physically by another network by use of secondary addresses. a subnet cannot appear at several active interfaces at the same time.

If any router in the network segment uses a secondary address, all the other routers in the same segment should use the secondary addresses in the same network or subnet.

Management of Interface IP addresses

Command	Description
ip address 128.255.255.1 255.255.0.0 [secondary]	Allocate a primary (secondary) IP address to an interface.
no ip address 128.255.255.1 255.255.0.0 [secondary]	Disable an existing primary (secondary) IP address.

Example

The following example shows how to assign a primary IP address and two secondary IP addresses to the interface Fastethernet0:

```
router#configure  terminal

router(config)#interface Fastethernet0

router(config-if-fastethernet0)#ip address 128.255.255.1
255.255.0.0

router(config-if-fastethernet0)#ip address 128.254.255.1
255.255.0.0 secondary

router(config-if-fastethernet0)#ip address 128.253.255.1
255.255.0.0 secondary

router(config-if)#exit
```

```
router(config)#
```

Those secondary IP addresses configured for the same interface have priority according to their configuration time. At the same time, these IP addresses are not required in the same net section thereby allowing routers to forward datagrams quickly.

Enabling IP Unnumbered on Serial Port

The IP unnumbered process is a method to saving IP addresses on the Internet network. You can enable IP unnumbered on a serial-interface, instead of assigning a visible IP address to the interface.

Whenever an unnumbered interface produces a packet (for example, when updating a routing list), it will use the interface address designated by you as the source address of IP packet.

It will also that designated interface address to determine which route process is sending the updated content to this unnumbered interface. There are some limitations. They are:

A serial-port only supports Point-to-Point Protocol (PPP). The High-Level Data Link Control (HDLC), Link Access Process Balance (LAPB), Serial Line Internet Protocol (SLIP) and Channel interface will be supported in the future.

The command ping EXEC cannot be used to test and connect the interface since it has no IP address. But the Simple Network Management Protocol (SNMP) can be used to remotely monitor the status of the interface.

Do not boot network image via unnumbered serial ports.

Do not support IP security options on a unnumbered interface.

For details, please refer to RFC 1195; It is not necessary to assign an IP address to each port.

Be sure to use an unnumbered serial line among different main networks. At each end, if there are different main networks are assigned to your unnumbered any routing protocol running via serial lines will be configured not to announce subnet information.

To enable an IP process on an unnumbered serial port, the following task should be finished in the interface configuration mode:

Command	Description

Ip unnumbered <reference interface>	Enable IP unnumbered on a serial interface, and don't distribute an obvious IP address to the interface.

The specified interface, not another unnumbered one, should be another interface in the router with at least one IP address. The designated interface should also be valid.

Setting IP Address Negotiation Property on Interface

With regard to the point-to-point protocols on the data link layer supporting IP address negotiation, you can enable IP address negotiation on an interface with no IP address.

Typically, PPP running over serial lines is used to access Internet via an ISP. IP address negotiation of the serial port is enabled by the commands, which allows the local interfaces to receive the IP address assigned by the interface of the opposite terminals.

Command	Description
Ip address negotiated	Enable IP address negotiation of an interface
No ip address negotiated	Disable IP address negotiation of an interface

Examine IP Address Configuration

After configuring IP address of interface, the user examines IP address information of interface via show interface.

```
Router#sh int f0
fastethernet0:
     Flags: (0x8063) UP BROADCAST MULTICAST ARP RUNNING
     Type: ETHERNET_CSMACD
     Internet address: 129.255.222.26   IP address is 129.255.222.26
     Netmask 0xffff0000 Subnetmask 0xffff0000 network mask is 16
bits  subnet mask is 16 bits
     Broadcast address: 129.255.255.255  broadcast address
129.255.255.255
     Queue strategy: FIFO Output queue: 0/40 (/max packets)
     Metric: 0, MTU: 1500, BW: 100000 Kbps, DLY: 100 usec, VRF:
kernel
     Ethernet address is 0001.7a00.b415
     Rate:  100Mbit/s   Duplex:  full duplex
     Babbling recvive 0, babbling transmit 0, heartbeat fail 0
     Tx late collision 0, Tx retransmit limit 0, Tx underrun 0
     Tx carrier sense 0, Rx length violation 0
     Rx not aligned 0, Rx CRC error 0, Rx overrun 0
     Rx trunc frame 0, Rx too small 0, Rx alloc mbuf fail 0
```

```
5 minute input rate 48000 bits/sec4 packets/sec
5 minute output rate 7000 bits/sec2 packets/sec
109948 packets received; 114881 packets sent
22677 multicast packets received
1325 multicast packets sent
28 input errors; 0 output errors
0 collisions; 0 dropped
```

Address Resolution Configuration

Signamax MP series routers permit you to designate IP addresses via address resolution and naming service.

Address Resolution Basic Configuration Command

Command	Description	Config mode
arp [vrf vrf-name] ip-address mac-address [alias]	Configure static ARP entry	config
ip proxy-arp	*interface configures ARP proxy function	config-if-××
show arp	Display ARP entry information	enable
clear arp-cache	Update ARP entry	enable
arp timeout	Configure ARP aging time	config-if-××
host	Configure hostname mapping to IP	config
ip domain-name	Configure router domain name	config
ip name-server	Configure DNS address	config
Ip name-order	Configure domain name resolution order	config

"*" before the command means it has configuration example description.

the configuration mode is config, config-if-××(interface name) config-××(protocol name) etc.

Establishing ARP

A device may have a data link (MAC) address (which uniquely identifies an interface on a LAN), and it can also has a network address (which identifies the network and the host number in which the device is

located). In order to communicate with a device on an Ethernet network, for example, a Signamax MP series router should first decide the 48 bits MAC address of that device.

The process used to determine the MAC address from an IP address is called address resolution. The process used to determine an IP address from a MAC address is called reverse address resolution (RAR).

Signamax routers support the Address Resolution Protocol (ARP). ARP is used to associate an IP address with a MAC address. Taking an IP address as input, ARP can determine its MAC address.

Once a MAC address is determined, the IP address/MAC address association is kept in ARP cache for high-speed searches. Then IP datagrams are encapsulated into frames to be sent out onto the network.

Defining Static ARP Cache

ARP provides a dynamic mapping from an IP address to a MAC address. Because most hosts support dynamic address resolution, it is not usually necessary to add a static entry into the Address Resolution Protocol (ARP) cache. You can define one globally ---- write a permanent entry into ARP cache, if the entry is defined for necessity. MP router software will translate the 32-bit IP address into a 48-bit MAC address by that entry.

Execute the following commands in the Global configuration mode:

```
arp <ip-address> <ethernet-address> - Used to define a static
ARP cache no arp <ip-address> <ethernet-address> - Used to
delete a static ARP cache
```

Proxy ARP

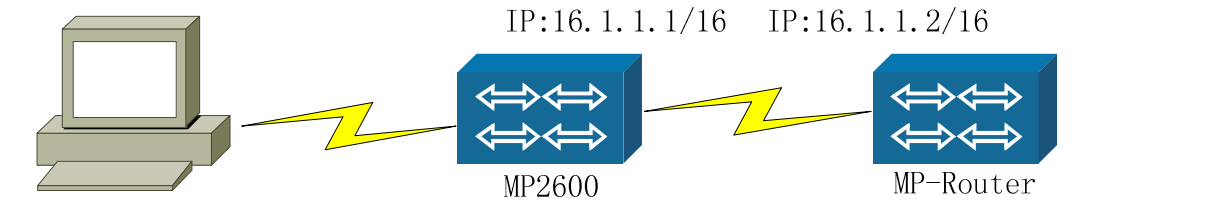
Configure the following command in interface configuration mode:

ip proxy-arp

```
ip proxy-arp
no ip proxy-arp
```

(Default status)enable ARP proxy
(command mode)interface configuration mode

The typical application and configuration:


IP:16.1.1.1/16
IP:16.1.1.2/16
MP2600
MP-Router
IP:136.1.2.99/16
IP:136.1.2.1/24
IP:136.1.3.1/24

Run and disable ARP proxy function on MP2600

Command	Description
MP2600(config-if-xxx)#ip proxy-arp	Enable ARP proxy function
MP2600(config-if-xxx)#no ip proxy-arp	Disable ARP proxy function

PC ping 136.1.3.1,if MP2600 doesn't have ARP PROXY, PING cannot be connected. The reason is as following:

To the packet in the same network, PC gets MAC address via broadcast ARP request, and then sends to destination host. In this example, the destination host address and PC address are in the same network, but physically they are not.

If there is no response for PC ARP request, PING is not connected. At this time, if MP2600 enables ARP PROXY, MP2600 gives the response to PC request via MAC address, and PING is connected.

Signamax router realized proxy is used in this condition, to proxy the same main network but different subnet packet.

Examine ARP Cache

show arp

```
show arp [vrf vrf-name] [all]
```

Command	Description
vrf-name	Display vrf-name ARP cache
All	Display ARP cache in resolution

(Default status)no
(command mode)privileged user mode

In order to display cache, use show arp to examine ARP cache content.

Update ARP Cache

Input the following command to update ARP in privileged mode.

clear arp-cache

```
clear arp-cache
```

(Default status)no
(command mode)privileged user mode

In order to update dynamic ARP, use command clear arp-cache to check each dynamic ARP, if ARP request is not response, ARP cache will be deleted; or ARP cache aging time will be updated, 20 minutes by default.

Configure ARP Cache Aging Time

Configure ARP aging time in interface mode:

arp timeout

```
arp timeout {seconds | disable}
```

Command	Description
seconds	Range is <1200-2147483>, 1200 seconds by default
disable	Disable dynamic ARP aging

(Default status)ARP 1200 seconds for aging
(command mode)interface configuration mode

Dynamic ARP detects destination host IP every 5 seconds, and ARP aging time will be updated after the detection. The total times is 4, but ARP will be invalid without detecting IP MAC. This operation will enhance network communication efficiency.

Domain Name System (DNS)

Each IP address has its related host name. Signamax Router software holds a cache that maps a host name to an IP address, which is supported by telnet, ping and theremote login. The cache accelerates the procedure translating the host name into an address.

IP provides a naming method to enable a device to be identified by its location in IP. This is a hierarchical naming method provided for domains. To trace a domain name, IP defines the conception of name server, which is used to keep a cache (or database) that holds the mapping information from a domain name to an IP addresses.

To map a domain name into an IP address, you should first identify a host name, and then specify a domain name server to enable the Domain Naming System, which is a global naming method to uniquely identify a network device on an internetwork.

Mapping IP Addresses to Host Name

Signamax routers holds a table that saves host names and their related IP addresses. The table is also called the host name-to-address mapping table. High-level protocols, such as the remote logon, use host names to identify network devices (hosts). IP addresses or routers and other network devices should be associated mutually by static or dynamic tools.

When the dynamic mapping cannot be used, addresses can be distributed to host names manually.

To specify a domain name or a host name to an address, users can execute the following commands in the global configuration mode:

```
host <host_name> <Ip_Address> Defining a mapping of host
names and IP addresses

no host <host_name> <Ip_Address>    Deleting a mapping of
host names and IP addresses
```

Designating Domain Name

You can designate a default domain name for a router. The domain name will be used by the system to finish the domain name request. You can designate either a single domain name or a series of domain names. Any IP host name without a domain name will have a specified domain name before it is added to the host table.

Execute any following task in global configuration mode in order to designate a domain name:

ip domain-name <name>	Defines a default domain name.
no ip domain-name <name>	Deletes a default domain name.

Designating Domain Name Server

Execute the following commands in the global configuration mode to specify one or hosts (up to 6) as domain name servers to provide name information service for DNS:

```
ip name-server server-address       Defines a domain name
server no
ip name-server server-address       Deletes a domain name
server.
```

Designating Domain Name Service Order

When resolving a name by use of the name service, the system will first use the default local name Cache, and then it uses DNS service to complete name resolution. Users can also designate that the system only use the DNS service (so you need not map an IP address into a host name manually) or first use the DNS service, and then use the local name CACHE to achieve name resolution.

Executing the following command in the global configuration mode:

```
ip name-order {dns-first|dns-only|local-first}
```

IP Protocol Configuration

IP Protocol Basic Configuration Command

Command	Description	Config mode
ip routing	Enable IP routing forwarding	config
ip redirect	Enable IP redirection function	config
icmp redirect-route	Enable IP receiving redirection packet	config
ip route-cache	Enable IP high speed forwarding	config-if-××
ip upper-cache	Enable IP user layer high speed forwarding	config
ip source-check	Enable IP source address check	config
ip option queue-length	Configure IP input queue length	config
ip option default-ttl	Configure sending IP packet default ttl	config
ip option fragment-ttl	Configure distributing packet regrouping ttl	config
ip option recv-checksum	Configure whether to check IP packet of Interface	config
ip option send-checksum	Configure whether send checksum of IP	config
show ip statistics	*display IP layer statistics information	enable

"*" before command means it has configuration example description.

Configuration mode is: config, config-if-××(interface name) config-××(protocol name) etc.

Enabling/Disabling IP Route Forwarding

Each Signamax router enables IP route forwarding by default. But it can be disabled under certain conditions, which can be realized under the following operations:

In the global configuration mode, users can disable IP routing forwarding by typing the command no ip routing.

In the global configuration mode, users can enable IP routing forwarding by typing the command ip routing.

Permitting/Prohibiting IP to Send Redirection Messages

Each Signamax router enables the sending of IP redirection by default. But in under certain conditions, IP redirection can be disabled. This can be accomplished by the following commands (in the global configuration mode):

```
ip redirect            Enables IP to send IP redirection
no ip redirect         Disables IP to send IP redirection
```

The default setting is to permit IP redirection.
Executing the following commands in the interface configuration mode:

```
ip redirects           Enables the sending of ICMP Redirect
messages
no ip redirects        Disables the  sending ICMP Redirect
messages
```

The default setting is to permit the redirecting of an ICMP Message.

Permitting/Prohibiting IP Receiving Redirection Message

The redirection packet of icmp can result in the update of the routing table. The default setting of a Signamax Router is not to update route after the router receives the redirection icmp packet. But users can select the route update.

Executing the following commands in global configuration mode:

```
icmp redirect-route      Enables addition of an icmp redirect
route
no icmp redirect-route   Disables addition of an icmp redirect
route
```

The default setting is to prohibit the routing update.

IP Fast Forwarding

The IP fast forwarding is realized via route cache mechanism. The purpose of the route cache is to reduce the repeated searching of a routing table and to accelerate the packets sending speed via using previous cache searching results. But under certain circumstances, users can choose to enable/disable the following two places to process route cache.

Fast Forwarding Route Cache

Before sent to IP layer to deal, some packets received by interface can be transferred directly if they match the route that stored in the cache.

Executing the following commands in the interface configuration mode:

```
ip route-cache                Enables fast-switching cache
for outgoing packets
no ip route-cache             Disables fast-switching cache
for outgoing packets
```

The default setting is to permit cache for outgoing packets.

Socket Route Cache

When there are packets sent down from the user layer, if the destination is the same each time and the route is UP, the route in the cache can be used without searching the routing table. Only one route, which is the result of recently searching the routing table, is stored in cache. Execute the following commands in the global configuration mode:

```
ip upper-cache                Enables the use of upper route
cache
no ip upper-cache       Disables the use of upper route cache
```

The default setting is to permit the use of upper route cache.

Enable/disable IP source address check

Enable IP source address check(RFC1812) of Signamax router by default. But in some special condition, the user disables IP source address check function, to be completed via the following operation:

Execute the command in global configuration mode:

ip source-check

```
ip source-check
no ip source-check
```

(Default status)IP source address check by default
(command mode)global configuration mode

The command is not existed in V3.4.x and IOS.

Configuring IP Protocol Attributes

Configure IP Protocol Input Queue

Configure the following command in global mode:

ip option queue-length

```
ip option queue-length {queue-length}
no ip option queue-length {queue-length }
default ip option queue-length
```

Command	Description
queue-length	IP input queue length, and the range is <30-600>

(Default status)200 by default
(command mode)global configuration mode

Command no and default is used to renew the default value.

Configure Default Time-To-Live (TTL) of Sending Data Packet

Configure the following command in global mode:

ip option default-ttl

```
ip option default-ttl {time-to-live}
```

```
no ip option default-ttl {time-to-live}
default ip option default-ttl
```

Command	Description
time-to-live	IP packet time-to-live, and the range is <1-255>

(Default status)64 by default
(command mode)global configuration mode

Command no and default is used to renew the default value.

Time-to-live is not the real time, but the skip times of packets. When ttl is 0, the router will drop this IP packet.

Configure Default Time-To-Live (TTL) of Sending IP Data Packet

Configure the command in global mode:

ip option fragment-ttl

```
ip option fragment-ttl {time-to-live}
no ip option fragment-ttl {time-to-live}
default ip option fragment-ttl
```

Command	Description
time-to-live	IP fragment packet living time before regrouping, and the range is <1-255>

(Default status)60 by default
(command mode)global configuration mode

Command no and default is used to renew the default value.

Enable IP recv-checksum

Configure the following command in global mode:

ip option recv-checksum

```
ip option recv-checksum
no ip option recv-checksum
default ip option recv-checksum
```

(Default status)enable recv-checksum
(command mode)global configuration mode

No is used to disable the option, and default is used to renew the default value.

Enable IP send-checksum

Configure the following command in global mode:

ip option send-checksum

```
ip option send-checksum
no ip option send-checksum
default ip option send-checksum
```

(Default status)enable send-checksum
(command mode)global configuration mode

No is used to disable the option, and default is used to renew the default value.

Observe IP Statistics

```
router#show          ip statistics

Statistics for IP protocol:

total 1356                          Number of the total received/sent packets
Badsum          0                   Number of packets that have bad checksums
Tooshort        0                   Number of packets that are too short
Toosmall        0                   Number of packets that are too small
Badhlen         0                   Number of packets with bad header lengths
badlen          0                   Number of packets that have bad lengths
infragments     0                   Number of the received fragment packets
fragdropped     0                   Number of packets discarded when fragment
fragtimeout     0                   Number of packets when fragmented overtime
forward         0                   Number of packets forwarded
cantforward     1312                Number of packets that cannot be forwarded
redirectsent    0                   Number of redirected transmissions
unknownprotocol 16                  Number of packets with unknown protocols
nobuffers       0                   Number of packets having no buffers
reassembled     0                   Number of datagram reassembly
outfragments    0                   Number of fragmented packets transmitted
noroute         0                   The times of without routing
```

ICMP Protocol

In the Internet Protocol stack, the Internet Control Message Protocol (ICMP) provides services such as controls, error reports and network tests, etc. for other protocols in the Internet stack. The Signamax router supports RFC792, RFC950 and RFC1122.

ICMP Basic Configuration Command

Command	Description	Config mode
ip mask-reply	ICMP subnet mask requesting for reply	Config
icmp redirect-route	ICMP redirection acceptance option	config
ip icmp source-quench	ICMP source disabled option	Config
show ip icmpstate	*display ICMP statistics	enable

"*" before command means it has configuration example description.

configuration mode is: config, config-if-××(interface name) config-××(protocol name) etc.

Configuring ICMP Options

Subnet Mask Option

Configure in global configuration mode:

ip mask-reply

ip mask-reply
no ip mask-reply

(Default status)not enable this option
(command mode)global configuration mode

Redirection Packet Option

Configure in global configuration mode:

icmp redirect-route

icmp redirect-route
no icmp redirect-route

(Default status)not enable this option
(command mode)global configuration mode

Source Quench Option

Configure in global configuration mode:

ip icmp source-quench

ip icmp source-quench
no ip icmp source-quench

(Default status)not enable this option
(command mode)global configuration mode

Displaying ICMP Statistics

```
router#sh ip icmp

Statistics for ICMP protocol

16 calls to icmp error                    The times for system to call ICMP to send error
                                          messages
0 error not generated because             The number of ICMP errors generated due to
old message was icmp                      timeout

Output histogram:                         output information
destination unreachable: 16               The times of the unreachable destination

0 message with bad code fields            The number of packets with bad code field
0 message < minimum length>
0 bad checksum                            The numbers of packets with bad checksum
0 message with bad length                 The numbers of packets with bad length

Input histogram:                          The input information
Destination unreachable: 16               The times of unreachable destination
0 message response generated              The number of the response messages
```

TCP Protocol

The Transmission Control Protocol (TCP) provides a highly reliable datagrams transmission service between application programs. Signamax Routers support RFC793, RFC813, RFC879, RFC896 and RFC1122.

TCP Protocol Basic Command Configuration

Command	Description
ip tcp recvbuffers [1024-65536](default: 4096)	Set the TCP receive buffer size
ip tcp sendbuffers [1024-65536](default: 4096)	Sets the send buffer size
ip tcp retransmits [1-100](default: 3)	Sets the retransmit threshold
ip tcp segment-size [256-4028](default: 512)	Configures the size of the maximum TCP segment
ip tcp round-trip [1-100](defult: 3)	Configure the maximum TCP round trip time

ip tcp idle-timeout[3-144000](default: 14400)	Configure the idle time of the connection that is before the first testing of keeping alive
ip tcp init-timeout[2-30000](default: 150)	Configure the value of the connection establishment
ip tcp keep-count[3-20](default: 8)	Configure the maximum keeping alive times when the opposite terminal has no response
ip tcp selective-ack	Configure TCP selective acknowledgement options as per RFC2018

Configure TCP Properties

Configure TCP recvbuffers size

ip tcp recvbuffers

ip tcp recvbuffers {buffer-size}
no ip tcp recvbuffers
default ip tcp recvbuffers

Command	Description
buffer-size	TCP input buffer size, and the range is <1024-65536>

(Default status)8192 by default
(command mode)global configuration mode

No and default is used to renew accepting buffer value.

Configure TCP sendbuffers size

ip tcp sendbuffers

ip tcp sendbuffers {buffer-size}
no ip tcp sendbuffers
default ip tcp sendbuffers

Command	Description
buffer-size	TCP output buffer size, and the range is <1024-65536>

(Default status)8192 by default
No and default is used to renew sending buffer value.

Configure TCP max retransmits times

ip tcp retransmits

ip tcp retransmits {retransmits-count}
no ip tcp retransmits
default ip tcp retransmits

Command	Description
retransmits-count	TCP max retransmits times, and the range is <1-100>

(Default status)3 times by default
(command mode)global configuration mode

No and default is used to renew retransmits times.

Configure TCP max segment-size

ip tcp segment-size

ip tcp segment-size {segment-size}
no ip tcp segment-size
default ip tcp segment-size

Command	Description
segment-size	TCP max packet segment size, and the range is <256-4028>

(Default status)512 bytes by default
(command mode)global configuration mode

No and default is used to renew max packet segment size

Configure TCP max round-trip time

ip tcp round-trip

ip tcp round-trip {round-trip}
no ip tcp round-trip
default ip tcp round-trip

Command	Description
round-trip	TCP max round-trip time, and the range is <1-100> seconds.

(Default status)3 seconds by default
(command mode)global configuration mode

No and default is used to renew max packet segment size default value.

Configure idle time

ip tcp idle-timeout

ip tcp idle-timeout { idle-time}
no ip tcp idle-timeout
default ip tcp idle-timeout

Command	Description
idle-time	TCP idle time, and the range is <3-144000> seconds.

(Default status)14400 seconds (2 hours) by default.
(command mode)global configuration mode

No and default is used to renew connecting idle time default value.

Configure timer value

ip tcp init-timeout

ip tcp init-timeout {init-time}
no ip tcp init-timeout
default ip tcp init-timeout

Command	Description
Init-timeout	TCP setting connection timer, and the range is <2-30000>

(Default status)150 by default, unit is 0.5 second.
(command mode)global configuration mode

No and default is used to renew timer default value.

Configure max keepalive testing times

ip tcp keep-count

ip tcp keep-count { keep-count }
no ip tcp keep-count
default ip tcp keep-count

Command	Description
keep-count	TCP keepalive times, and the range is <3-20>

(Default status)8 times by default.
(command mode)global configuration mode

No and default is used to renew keepalive testing times default value.

Configure TCP Using MTU Discovery

ip tcp path-mtu-discovery

ip tcp path-mtu-discovery [age-timer {minute | infinite}]
no ip tcp path-mtu-discovery

Command	Description
age-timer	Define PMTU aging time, and the unit is minute.
minute	Range is <10-30>
infinite	PMTU not aging

(Default status)not enable PMTUD,PMTU default aging time is 10 minutes.
(command mode)global configuration mode

Displaying TCP Statistics

The command show Ip tcp provides the detailed TCP statistics.

routerr#show ip tcp

Statistics for the TCP protocol:

0 packet sent	The total number of sending packets
0 data packet (0 byte)	The packets number (byte number)
0 data packet (0 byte) retransmitted	The resent packets number (byte number)
0 ack-only packet (0 delayed)	The acknowledge packets number
0 URG only packet	The urgent packets number
0 window probe packet	The window probe packets number
0 window update packet	The window update packets number
0 control packet	The control packets number
0 packet received	The total received packets number
0 ack (for 0 byte)	The acknowledge packets number (byte)
0 duplicate ack	The duplicate-acknowledge packets number
0 ack for unsent data	The number of the packets asked not to be sent
0 packet (0 byte) received in-sequence (byte)	The number of packets received in sequence
0 completely duplicate packet (0 byte)	The completely duplicate packet number (byte)

0 packet with some dup. Data (0 byte duped) The partial duplicate packet number (byte)

0 out-of-order packet (0 byte) The out-of-order packets number (byte)

0 packet (0 byte) of data after window The number of the packets outside of the window (byte)

0 window probe The window probe packets number

0 window update packet ---The window update packets number

0 packet received after close ---The number of the received packets after closing connection.

0 discarded for bad checksum ---The number of the packets discarded because of bad checksum

0 discarded for bad header offset field ---The number of the packets discarded because of bad header offset field

0 discarded because packet too short ---The number of the packets discarded because of too short

0 connection request ----The number of the local TCP connection requests

0 connection accept ----The number of connections received by the local TCP

0 connection established ----The established TCP connections number (including accepts).

0 connection closed (including 0 drop) ----The closed TCP connections number

0 embryonic connection dropped ----The discarded connections number

0 segment updated rtt (of 0 attempt) ----No packet used to update round trip time
0 retransmit timeout ----The times of retransmission for timeout

0 connection dropped by reXmit timeout ---The number of discarded connections for timeout resending
0 persist timeout ---The persist timer don't timeout
0 keepalive timeout ---The number of keepalive timeouts.
0 keepalive probe sent ---The number of keepalive probes sent.
0 connection dropped by keepalive ---The number of connections dropped by keepalive
0 pcb cache lookup failed ---The times of examining protocol control module failure

UDP Protocol

The User Datagram Protocol (UDP) provides the basic service of data transmission between application programs. Signamax MP series routers support RFC768.

UDP Basic Command Configuration

Command	Description
ip udp default-ttl [1-255]	Set Time-To-Live of UDP packets
ip udp recvbuffers [1024-65536]	Set UDP receiving buffer size
ip udp sendbuffers [1024-65536]	Set UDP sending buffer size
ip udp recv-checksum	Enable UDP receiving checksum
ip udp send-checksum	Enable UDP sending checksum

Configuring UDP Protocol Attributes

Configure Time-To-Time Live of Sending UDP Data Packet

ip udp default-ttl

ip udp default-ttl {time-to-live}
no ip udp default-ttl
default ip udp default-ttl

Command	Description
time-to-live	UDP TTL,and the range is <1-255>

(Default status)30 by default
(command mode)global configuration mode

No and default is used to renew TTL default value.

Configure UDP Accepting recvbuffers size

ip udp recvbuffers

ip udp recvbuffers {buffer-size}
no ip udp recvbuffers
default ip udp recvbuffers

Command	Description
buffer-size	UDP input buffer size, and the range is <1024-65536>

(Default status)41600 bytes
(command mode)global configuration mode

No and default is used to renew accepting buffer value.

Configure UDP sendbuffers size

ip udp sendbuffers

ip udp sendbuffers {buffer-size}
no ip udp sendbuffers
default ip udp sendbuffers

Command	Description
buffer-size	UDP output buffer size, and the range is <1024-65536>

(Default status)9216 bytes
(command mode)global configuration mode

No and default is used to renew sending buffer value.

Configure UDP accepting recv-checksum

ip udp recv-checksum

ip udp recv-checksum
no ip udp recv-checksum
default ip udp recv-checksum

(Default status)enable
(command mode)global configuration mode

No and default is used to renew default value.

Configure UDP send-checksum

ip udp send-checksum

ip udp send-checksum
no ip udp send-checksum
default ip udp send-checksum

(Default status)enable

(command mode)global configuration mode

No and default is used to renew default value.

Displaying UDP Statistic Information

The command show Ip udp displays detailed UDP statistics

router# show ip udp

Statistics for the UDP protocol:

32 total packets	Total number of input and output packets
16 input packets	Total number of input packets
16 output packets	Total number of output packets
0 incomplete header	Number of packets with incomplete UDP headers
0 bad data length field	Number of packets with bad UDP data length field
0 bad checksum	Number of packets with bad UDP checksum
0 broadcasts received with no ports	Number of the broadcast packets received with no ports
0 full socket	Number of broadcast packets received with full socket
16 pcb cache lookups failed	Number of PCB Cache lookups failed
16 pcb hash lookups failed	Number of PCB Hash lookups failed

Socket Interface

A socket is a mechanism that network application programs use to access lower layer network resources. Signamax MP series routers supports the standard socket interface mechanism and a series of socket applications. The command Show Ip Sockets can be used to display the usage situation of the TCP/UDP connection used by the system, and can helpful to troubleshoot.

router#show ip sockets

```
Active Internet connections (including servers)
PCB       Proto      Recv-Q    Send-Q    Local Address     Foreign Address    (state)
--------  -----      ------    ------    ------------------    ------------------   -------
990320  TCP   0    0         128.255.1.8.23          128.255.111.100.10
ESTABLISHED
99029c  TCP   0    0         128.255.1.8.23                                  128.255.1.6.1057
ESTABLISHED
98ff84    TCP    0            0         0.0.0.0.23                        0.0.0.0
LISTEN
9903a4  UDP   0            0         0.0.0.0          0.0.0.0
98fdf8    UDP   0            0         0.0.0.0          0.0.0.0
98ff00    UDP   0            0         0.0.0.0.1024     0.0.0.0
```

Each line represents one TCP/UDP connection.

Explanation of Abbreviations in the Chart:

PCB -- indicates the address of the Protocol Control Block
Proto -- indicates the protocol used by the connection: TCP or UDP
Recev-Q -- indicates the data received over the connection
Send-Q -- indicates the data sent over the connection

Local Address -- indicated the local address and port number of the connection
Foreign Address – remote address and port number of the connection
For TCP connection, (State) indicates the TCP state.

NDSP Protocol Configuration

Neighbor Device Search Protocol(NDSP) discovers adjacent devices on the network and obtains protocol address of neighboring devices and platform of those devices. NDSP is media- and protocol-independent,and run over the data link layer only.

Each device configured for NDSP sends periodic messages, known as advertisements, to a multicast address. The advertisements contain time-to-live, or holdtime, information, which indicates the length of time a receiving device should hold NDSP information before discarding it.

Each device also listens to the periodic NDSP messages sent by others in order to learn about neighboring devices and determine when their interfaces to the media go up or down.

NDSP is supported by HDLC, PPP, Frame Relay protocol on WAN interface.

Commands

You can use the following three commands to configure NDSP in global configuration mode:

Command	Description
ndsp run	Enable NDSP . The no ndsp run command is used to deactivate NDSP . The default mode leaves NDSP turned off.
ndsp timer	Specifies frequency of transmission of NDSP update. The default interval is 60 seconds.

ndsp holdtime:	Specfies the amount of time a receiving device should hold information sent by your device before discarding it. The default interval is 180 seconds.
ndsp enable	NDSP is enabled by default on all supported interfaces to send and receiver NDSP information.

NDSP is enabled by default on all supported interfaces to send and receiver NDSP information. You can disable NDSP on an interface supports NDSP by using the no ndsp enable command.

Command	Description
ndsp enable	Enabled NDSP on an interface.

Input these commands to display NDSP status:

Command	Description
Show ndsp entry	Displays information about a specific neighbor
Show ndsp neighbors	Displays type of device that has been discovered, the name of the device, the number and type of the local interface, the number of seconds the NDSP advertisement is valid for the portthe device type, the device product number, and the port ID.
Show ndsp traffic	Display s NDSP counters,including the number of packets sent and received and checksum errors.
Show ndsp version	Displays NDSP version.

Examples

If you want to run NDSP on your router, input:

```
router#configure terminal
router(config)# ndsp run
router(config)#exit
router#
```

If you don’t want to run NDSP on your router anymore, input:

```
router#configure terminal
router(config)#no  ndsp run
router(config)#exit
router#
```

Routing Configuration

This chapter introduces routing mechanisms and how to apply many kinds of mainstream routing protocols, such as Routing Information Protocol (RIP), Internal Routing Message Prococol(IRMP)Open Shortest Path First (OSPF), to configure a Signamax router to achieve a network interconnection.

Routing Overview

Internet protocol is a routable network protocol, in which a router executes the route addressing function.

Each router has a routing table, which plays a key role in transmitting packets. A routing table is created manually by network administrators or dynamically by exchanging routing information with other routers. A router locates an optimal route to a given destination from the routing table, then transmits packets following this route.

The routing table comprises network addresses, network masks, routing selective metrics, interfaces to be used and the "next hop" IP address on the way to the destination (if needed).

A route is divided into two kinds due to different destinations:

Network route, whose destination is a network

Host route, whose destination is a host

A route further divided into another two kinds depending on whether a router is connected to a destination directly or not.

Direct route, The destination network is connected directly to the router

Indirect route, The destination is connected indirectly to the router

A route is also divided into two kinds according to how the routes are generated

Static routing, which is configured manually

Dynamic routing, which is generated automatically by various dynamic routing protocols

Very often there are several routes to the same destination. A router uses a set of rules to select the optimal route. The rules used by a router to select an optimal route to share the network accessibility and state with other routers is called a routing protocol. A routing protocol comprises at the following four parts:

Transmittable network information reachable by other routers

Receivable network information reachable by other routers

The mechanism of selecting the optimal route based on the previous reachable information and to record this route to the routing table.

Responses to the changes of network topology and notification of the changes.

Signamax MP series routers supports many kinds of routing methods, which will be introduced one by one in the following sections: the configuration and usage method of static route/default route, RIPv1/v2 dynamic route, OSPF dynamic route, and IRMP dynamic route.

Configuring Static Routes/Default Routes

The static route is the route defined by the user, and it can enable the transmission between the source and the destination to adopt the path designated by the user.

This section explains how to configure the static route protocol of a Signamax router to interconnect networks.

Static Routing/Default Routing Basic Commands

Command	Description	Config mode
ip route [vrf vrf_name] destination-ip-address destination-mask {next-hop-ip-address | interface-type interface-number} [administrative-distance]	* configure a static routing	config
no ip route [vrf vrf_name] destination-ip-address destination-mask {next-hop-ip-address | interface-type interface-number} [administrative-distance]	* delete a static routing	config
router static	*enter static routing configuration mode	config
distance administration-distance	* configuration static routing	config-static

	administration distance	
default distance	* renew static routing default distance 1	config-static
ip route [vrf vrf_name] 0.0.0.0 0.0.0.0 {next-hop-ip-address | interface-type interface-number} [administrative-distance]	* configure a default routing	config
no ip route [vrf vrf_name] 0.0.0.0 0.0.0.0 {next-hop-ip-address | interface-type interface-number} [administrative-distance]	* delete a default routing	config
show ip route [vrf vrf_name] static	* display static routing	#
debug ip routing	* debug and display ip routing event	#
debug ip routing message	* debug and display ip routing event message	#

"*" before command means it has configuration example description.

Configuration mode is: config, config-if-××(interface name) config-××(protocol name) .

Configure Static Routing

The configuration of the static route comprises:

Adding/deleting configuration of the static route

Configuration of the static route administrative distance

The detailed configuring commands are:

Commands to configure static route

In global mode, use ip route to set up static routing, and no is used to delete the static routing.

•

```
ip route [vrf vrf_name] destination-ip-address destination-
mask {next-hop-ip-address | interface-type interface-number}
[administrative-distance]

no ip route [vrf vrf_name] destination-ip-address
destination-mask {next-hop-ip-address | interface-type
interface-number} [administrative-distance]
```

Syntax	Description
vrf_name	The routing has vrf attribute
destination-ip-address	Destination ip address.
destination-mask	Destination mask.
next-hop-ip-address	Next hop IP address.
interface-type	Forwarded network interface type
interface-number	Forwarded network interface number
administrative-distance	Administrative distance, and the vale is 1—255

(Default status) no static routing configuration
(command mode) global configuration mode

Delete static routing, and if there is administration distance:

```
router(config)#no ip route A.B.C.D   mask a.b.c.d|interface
[distance]
```

In practical applications, the configuration of the static route had better adopt the IP address of the next hop. In a point-to-multipoint network (for example, X.25 and FR), the configuration should adopt the IP address of the next hop. The network interface configured to transmit can be only fit for the point-to-point link (for example, HDLC).

```
(configuration example)
```

Adding a static route to the interface fasterthenet0 to reach the network 199.199.199.0

Command	Description
router1#con t router1(config)# ip route 199.199.199.0 255.255.255.0 fastethernet0	Configures the static route from the interface fastethernet0 to the network section 199.199.199.0/24.

To display the routing table of the router and checking the configuration results

```
router#sh ip route

Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF
External, M - Management

D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP

Gateway of last resort is 0.0.0.0 to network 0.0.0.0


S   0.0.0.0/0 [1/100] is directly connected, 01:00:25, fastethernet0
```

```
C    127.0.0.0/8 is directly connected, 01:30:22, lo0
C    128.255.60.0/22 is directly connected, 01:30:11, fastethernet0
S    199.199.199.0/24 [1/100] is directly connected, 00:00:06,
fastethernet0
```

Example i :

Command	Description
ip route 128.255.0.0 255.255.0.0 f0	Configure a connecting static routing
ip route 128.255.0.0 255.255.0.0 f0 210	Configure a connecting static routing, and its administration distance is 210
ip route 128.255.0.0 255.255.0.0 128.255.1.1	Configure a static routing to next hop gateway
ip route 128.255.0.0 255.255.0.0 128.255.1.1 210	Configure a static routing to next hop gateway, and the administration distance is 210:

configure static routing administration distance:

In static routing mode, use distance to configure static routing administration distance. default distance is used to renew the default value.

enter static routing configuration mode:

router static

Command	Description
router static	Enter static routing mode

(command mode)global configuration mode
(Default status)no

configure administration distance:

(command)
distance administration-distance
default distance

Command	Description
Administration-distance	Administration distance, and the value is 1—255
default distance	Renew static routing default administration distance 1.

(command mode)static routing configuration mode
(Default status)administration distance is 1

•

(configuration example)
router(config)#

Command	Description
router static	Enter static routing configuration mode
distance number	Configure administration distance, and number is the number among 1 to 255.

(command mode)global configuration mode

Configuring Default Route

Command	Description
router(config)#ip route 0.0.0.0 0.0.0.0 A.B.C.D	A.B.C.D:Indicating the default gateway IP address

The default route configuration of the router is to permit IP route transmission. But in some special situations, users can prohibit the routing function, which can be achieved in the global configuration mode via the following command to prohibit IP route transmission:

router(config)#no ip routing
In the global configuration mode, the following command can be used to permit IP route transmission:

router(config)#ip routing
The no form of this command is used to delete a default route

Display Static Routing

After configuration, execute show ip route static to display static routing and default routing information, and the user validates the configuration result via examining displaying information.

```
show ip route [vrf vrf_name] static
```

Command	Description
Static	Only displaying configured static routing and default routing
vrf_name	The vrf atrribute of the routes

(command mode)privileged user mode
(configuration example)

Command	Description
router#show ip route static	Display all static routing and default routing

```
router#show ip route static
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M -
Management
D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
S    0.0.0.0/0 [1/100] is directly connected, 01:49:55, fastethernet0
S    128.255.0.0/16 [210/100] is directly connected, 00:40:10, fastethernet0
S    192.168.0.0/16 [1/100] is directly connected, 00:38:58, fastethernet0
S    199.199.199.0/24 [1/100] is directly connected, 00:49:35, fastethernet0
```

Debug Static Routing

```
debug ip routing
debug ip routing message
```

Syntax	Description
message	Display rouging, interface, address message event.

(command mode)privileged user mode
(configuration example)

Syntax	Description
router#debug ip routing	Display routing working status

```
router(config-if-fastethernet0)#no shut
router(config-if-fastethernet0)#
02:26:26: %LINEPROTO-5-UPDOWN: Line protocol on Interface
fastethernet0, changed state to up
02:26:26: RT : add "C 128.255.60.0 255.255.252.0 128.255.60.3

fastethernet0(0,0,0, 0x0, 0x0, 0)" to kernel table success


02:26:26: %LINEPROTO-5-UPDOWN: Line protocol on Interface
fastethernet0.1, changed state to up
02:26:26: RT : add "S 0.0.0.0 0.0.0.0 128.255.60.3
fastethernet0(0,1,0, 0x0, 0x0, 0)" to kernel table success
02:26:26: RT : add "S 128.255.0.0 255.255.0.0 128.255.60.3
fastethernet0(0,210,0, 0x0, 0x0, 0)" to kernel table success
```

Command	Description
router(config)#debug ip routing message	Display all routing message

```
router(config)#int f0
router(config-if-fastethernet0)#shut
02:33:00: %LINEPROTO-5-UPDOWN: Line protocol on Interface fastethernet0,
changed state to down
02:33:00: RTMSG : Module ROUTE MSGTYPE RTM_DELETE IFName = fastethernet0 VRF
= 0 DST = 128.255.60.0 GATEWAY = 128.255.60.3 NETMASK = 255.255.252.0
02:33:00: RTMSG : Module INTERFACE MSGTYPE RTM_IFINFO IFName = fastethernet0
VRF = 0
02:33:00: %LINEPROTO-5-UPDOWN: Line protocol on Interface fastethernet0.1,
changed state to down
02:33:00:
RTMSG : Module INTrouterERFACE MSGTYPE(config-if- RTM_IFINfastethernet0)#FO
IFName = fastethernet0.1 VRF = 0
02:33:00: RTMSG : Module ROUTE MSGTYPE RTM_DELETE IFName = fastethernet0 VRF
= 0 DST = 0.0.0.0 GATEWAY = 128.255.60.3 NETMASK = 0.0.0.0
02:33:00: RTMSG : Module ROUTE MSGTYPE RTM_DELETE IFName = fastethernet0 VRF
= 0 DST = 128.255.0.0 GATEWAY = 128.255.60.3 NETMASK = 255.255.0.0
02:33:00: RTMSG : Module ROUTE MSGTYPE RTM_DELETE IFName = fastethernet0 VRF
= 0 DST = 192.168.0.0 GATEWAY = 128.255.60.3 NETMASK = 255.255.0.0
02:33:00: RTMSG : Module ROUTE MSGTYPE RTM_DELETE IFName = fastethernet0 VRF
= 0 DST = 199.199.199.0 GATEWAY = 128.255.60.3 NETMASK = 255.255.255.0
```

Configuring RIP Dynamic Routing

Routing Information Protocol (RIP) exchanges routing updates via broadcasting UDP packets. A router sends out routing updates every 30 seconds, which is called a notification.

If a router does not receive any routing updates from another router within 180 seconds or more, the routes related to that router is disabled. If the router does not receive any routing updates within 240 seconds after this, the router will delete all routes related to that router from its routing table.

RIP provides a metric, which is called a hop count, to scale different routing distances. Hop count is the number of routers passing via a route. The hop count of a directed network is 0, while the hop count of an unreachable network is 16.

If a router has a default route, RIP will notify the route from the router to a virtual network 0.0.0.0 which does not exist. RIP takes 0.0.0.0 as a network to deal with the default route.

RIP sends routing updates to the interface of the specified network interfaces. If the interfaces are not specified to a network, no RIP updating information will be sent out.

RIP (Routing Information Protocol) is a kind of distance vector routing protocol serving as the routing of the mini, simple network. This section explains how to configure Signamax Router RIP to interconnect networks.

RIP Commands

Command	Description
auto-summary	Makes Route Classify Summarization valid
default	Configures the default instruction
default-information originate [route-map routemap-name]	Configures router as the default gateway
default-metric metric	Set the default metric that RIP uses to redistribut other routing protocols routes
neighbor ip-address	Define a neighbor router exchanging routing information
network network-number	Associates the network with the RIP routing process
passive-interface interface-name	Restrains route update of the interface, so that this interface can only accept the route update information sent from the other routers but can't send any route update information
redistribute protocol-name [{as-num|process-id}] [metric metric]	Configures the route redistribution (you can choose: direct connection, IRMP, ospf, static route)
timers basic update invalid holddown flush	Adjusts the timer
version {1|2}	Designates the version of RIP
address-family ipv4 vrf vrf-name	Enable VRF in RIP
distance distance	Set RIP routes management distance
distribute-list access-list-name in/out [interface]	Configure RIP routes filtering
Maximum-paths number-paths	Configure RIP load balance max number
offset-list access-list-name in/out offset [interface]	Add offset to RIP routes metrics

RIP Configuration Commands

router rip
Enable RIP,and enter RIP routing configuration mode. No is use to disable RIP.

```
router rip
no router rip
```

(Default status)not run RIP
(command mode)global configuration mode

address-family

enable VRF in RIP,and enter RIP VRF routing configuration mode. No is used to disable that.

```
address-family ipv4 vrf vrf-name
no address-family ipv4 vrf vrf-name
```

Syntax	Description
vrf-name	Vrf name

(Default status)RIP doesn't enable VRF
(command mode)RIP protocol configuration mode.

auto-summary

Enable RIPv2 routing auto aggregation function. No is use to disable this function.

```
auto-summary
no auto-summary
```

(Default status)RIPv2 doesn't have routing auto aggregation function by default.

(command mode)RIP protocol configuration mode

default-information originate

Configured router as default gateway, and the default routing is (0.0.0.0/0). No is used to disable the function.

```
default-information originate [route-map routemap-name]
no default-information originate
```

Syntax	Description
routemap-name	route-map name

(Default status)no default gateway function.
(command mode)RIP protocol configuration mode

default-metric

Configure RIP redistributing other routing protocol routes metric default value. No is used to renew the metric value.

```
default-metric metric
no default-metric
```

Syntax	Description
metric	Metric value by default, and the range is 1-16

(Default status)RIP redistributing other routing protocol routes metric value is 1
(command mode)RIP protocol configuration mode

distance

Configure RIP routes administration distance. No is used to renew the distance.

```
distance distance
no distance distance
```

Syntax	Description
distance	Administration distance value. And the range is 1-255.

(Default status)RIP routes administration distance is 120
(command mode)RIP protocol configuration mode

distribute-list

Configure RIP routing filter. No is use to clear routing filter.

```
distribute-list access-list-name in/out [interface]
distribute-list prefix prefix-list-name in/out [interface]
no distribute-list access-list-name in/out [interface]
no distribute-list prefix prefix-list-name in/out [interface]
```

Syntax	Description
access-list-name	Standard access list name
prefix-list-name	Prefix list name

(Default status)not routing filter
(command mode)RIP protocol configuration mode

maximum-paths

Configure RIP load balance max number. No is use to renew load balance max number.

```
maximum-paths number-paths
no maximum-paths
```

Syntax	Description
number-paths	RIP supported load balance max routing numbers, and the range is 1-6

(Default status)number-paths:4
(command mode)RIP protocol configuration mode

neighbor

Define neighbor router. No is use to clear that router.

```
neighbor ip-address
no neighbor ip-address
```

Syntax	Description
ip-address	Router IP address

(Default status)no definition of neighbor router
(command mode)RIP protocol configuration mode

offset-list

Config offset on RIP routes metric, and no is used to renew RIP routes metric.

```
offset-list access-list-name in/out offset [interface]
no offset-list access-list-name in/out [offset] [interface]
```

Syntax	Description
access-list-name	Standard access list name
offset	offset value, and the range is 0～16

(Default status)use metric value by default
(command mode)RIP protocol configuration mode

network

Choose routing network list for RIP. No is used to clear the network.

```
network network-number
no network network-number
```

Syntax	Description
network-number	Connected network.

(Default status)no designation network.
(command mode)RIP protocol configuration mode

passive-interface

Designate passive interface, and this interface only accepts routing update but not send it. No is used to clear the passive attribute.

```
passive-interface interface-name
no passive-interface interface-name
```

Syntax	Description
interface-name	Passive interface name

(Default status)no designated passive interface, and all interfaces covered by network can send routing update.
(command mode)RIP protocol configuration mode

This command and neighbor command can control the router broadcast update.

redistribute

Configure RIP introducing other routing protocol routes. No is used to cancel the introducing.

```
redistribute protocol-name [{as-num|process-id}] [metric
metric]
no redistribute protocol-name
```

Syntax	Description
protocol-name	Network protocol name, introduced protocols: connected, static, ospf, irmp, bgp and snsp.
as-num	Designate autonomy system number.
process-id	Designate process id.
metric	Designate introduced routing metric value.

(Default status)not introduce other protocol routing
(command mode)RIP protocol configuration mode

1. if not designate metric,use default-metric designated default metric.
2. when redistributing irmp, designate as-num ; when redistribute ospf, designate process-id.

timers

Adjust RIP network timer. No is used to renew default timer.

```
timers basic update invalid holddown flush
no timers basic
```

Syntax	Description
update	Update sending rate (second)
invalid	Invalid time segment of routing. This value should be 3 times of update.
holddown	Restrain routing time segment (second).

flush	Clear the routing segment (second). The designated time segment should be more than invalid value.

```
(Default status)update:30 seconds, invalid:180 seconds,
holddown:180 seconds, flush:240 seconds.
```

(command mode)RIP protocol configuration mode

If holddown is 0, the routing has no block.

version

Designate router RIP version.

version {1|2}

Syntax	Description
1	Designate RIP version 1.
2	Designate RIP version 2.

(Default status)RIP global version 1
(command mode)RIP protocol configuration mode

ip rip authentication mode

Designate RIP version 2 packet authentication check mode. No authentication is used to checking.

```
ip rip authentication mode {text|md5}
no ip rip authentication {text|md5}
```

Syntax	Description
text	Text check.
md5	Packet MD5 check

(Default status)no authentication check.
(command mode)interface configuration mode

This command should be used together with ip rip authencation key.

ip rip authentication key

designate check authentication key to RIP version 2.

```
ip rip authentication key {0|7} string
```

Syntax	Description
0	Not deal with string

7	Encrypt to string
string	Authentication word. And the range is 1~16 characters.

(Default status)no authentication key.
(command mode)interface configuration mode

This command should be used together with ip rip authencation mode.

ip rip receive version

designate accepted RIP version on interface. No is used to make the interface be accord with instance version.

```
ip rip receive version {1|2|12}
no ip rip receive version
```

Syntax	Description
1	Only accept RIP version 1
2	Only accept RIP version 2
12	Accept RIP version 1 and 2

(Default status)confirm according to instance version.
(command mode)interface configuration mode

ip rip send version

designate sending RIP version. No is used to make the interface be accord with version.

```
ip rip send version {1|2|12}
no ip rip send version
```

Syntax	Description
1	Only send RIP version 1
2	Only send RIP version 2
12	Send RIP version 1 and 2

(Default status)confirm according to version.
(command mode)interface configuration mode

ip split-horizon

designate enabling split horizon. No is used to cancel the function.

```
ip split-horizon
no ip split-horizon
```

(Default status)enable split horizon.
(command mode)interface configuration mode

RIP Configuration Example

RIP Startup Configuration

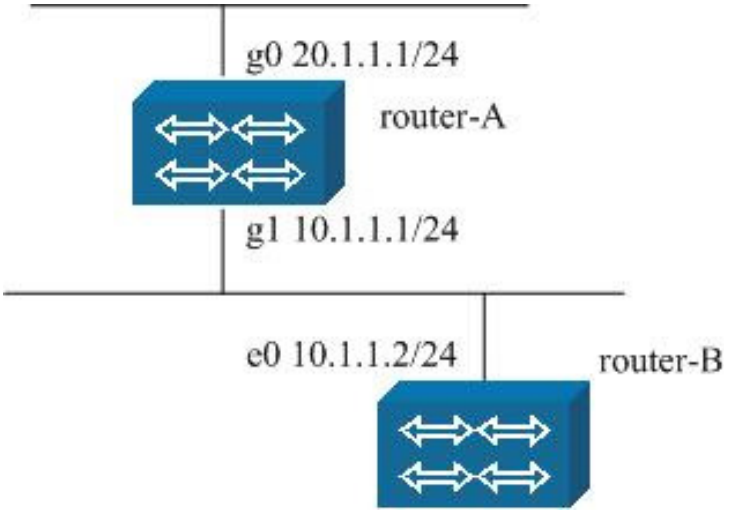


Figure 8-1

Router-A g1 connects Router-B e0, and the addresses are 10.1.1.1 and 10.1.1.2. and meanwhile, Router-A g0 connects to another LAN 20.1.1.0/24.

Router-A configuration:

Command	Description
router-A#configure terminal	Enter global configuration mode
router-A(config)# interface gigaethernet0	Enter g0
router-A(config-if-gigaethernet0)# ip address 20.1.1.1 255.255.255.0	Configure ip address
router-A(config-if-gigaethernet0)# interface gigaethernet1	Enter g1
router-A(config-if-gigaethernet1)# ip address 10.1.1.1 255.255.255.0	Configure ip address
router-A(config-if-gigaethernet1)#exit	Exit to global configuration mode
router-A(config)#router rip	Enter RIP configuration mode
router-A(config-rip)# network 20.0.0.0	Designate RIP running network number
router-A(config-rip)# network 10.0.0.0	Same as above
router-A(config-rip)#version 2	Configure RIP version

Router-B configuration:

Command	Description
router-B#configure terminal	Enter global configuration mode
router-B(config)# interface ethernet0	Enter e0
router-B(config-if- ethernet0)# ip address 10.1.1.2 255.255.255.0	Configure ip address
router-B(config)#router rip	Enter RIP configuration mode
router-B(config-rip)# network 10.0.0.0	Designate RIP running network number
router-B(config-rip)#version 2	Configure RIP version

After above configuration, Router-A and Router-B start running RIP. Run command show ip route rip on Router-B.

```
R        20.1.1.0/24 [120/2] via 10.1.1.1, 00:00:06, ethernet0
```

RIP Routing Collecting Configuration

On Router-A:

Command	Description
router-A#configure terminal	Enter global configuration mode
router-A(config)# interface gigaethernet0	Enter g0
router-A(config-if-gigaethernet0)# ip address 20.1.1.1 255.255.255.0	Configure ip address
router-A(config-if-gigaethernet0)# interface gigaethernet1	Enter g1
router-A(config-if-gigaethernet1)# ip address 10.1.1.1 255.255.255.0	Configure ip address
router-A(config-if-gigaethernet1)#exit	Exit to global configuration mode
router-A(config)#router rip	Enter RIP configuration mode
router-A(config-rip)# network 20.0.0.0	Designate RIP running network number
router-A(config-rip)# network 10.0.0.0	Same as above
router-A(config-rip)# version 2	Configure RIP version
router-A(config-rip)# auto-summary	Enable auto collection

Router-B configuration is same as 8.3.3.1. Run command show ip route rip on Router-B.

```
R        20.0.0.0/8 [120/2] via 10.1.1.1, 00:00:07, ethernet0
```

RIP Default Routing Notification

On Router-A:

Command	Description
router-A#configure terminal	Enter global configuration mode
router-A(config)# interface gigaethernet0	Enter g0
router-A(config-if-gigaethernet0)# ip address 20.1.1.1 255.255.255.0	Configure ip address
router-A(config-if-gigaethernet0)# interface gigaethernet1	Enter g1
router-A(config-if-gigaethernet1)# ip address 10.1.1.1 255.255.255.0	Configure ip address
router-A(config-if-gigaethernet1)#exit	Exit to global configuration mode
router-A(config)#router rip	Enter RIP configuration mode
router-A(config-rip)# network 10.0.0.0	Designate RIP running network number
router-A(config-rip)# version 2	Configure RIP version
router-A(config-rip)# default-information originate	Notify default routing

Router-B configuration is same as 8.3.3.1. Examine default routing information on Router-B via show ip route rip.

```
R    0.0.0.0/0 [120/2] via 10.1.1.1, 00:00:02, ethernet0
```

RIP Administration Distance Adjustment

Router-A configuration is same as 8.3.3.1.

On Router-B:

Command	Description
router-B#configure terminal	Enter global configuration mode
router-B(config)# interface ethernet0	Enter e0
router-B(config-if- ethernet0)# ip address 10.1.1.2 255.255.255.0	Configure ip address
router-B(config)#router rip	Enter RIP configuration mode
router-B(config-rip)# network 10.0.0.0	Same as above
router-B(config-rip)# version 2	Configure RIP version

router-B(config-rip)# distance 100	Adjust RIP routing administration distance as 100

```
show ip route rip on Router-B:
R       20.1.1.0/24 [100/2] via 10.1.1.1, 00:00:06, ethernet0
```

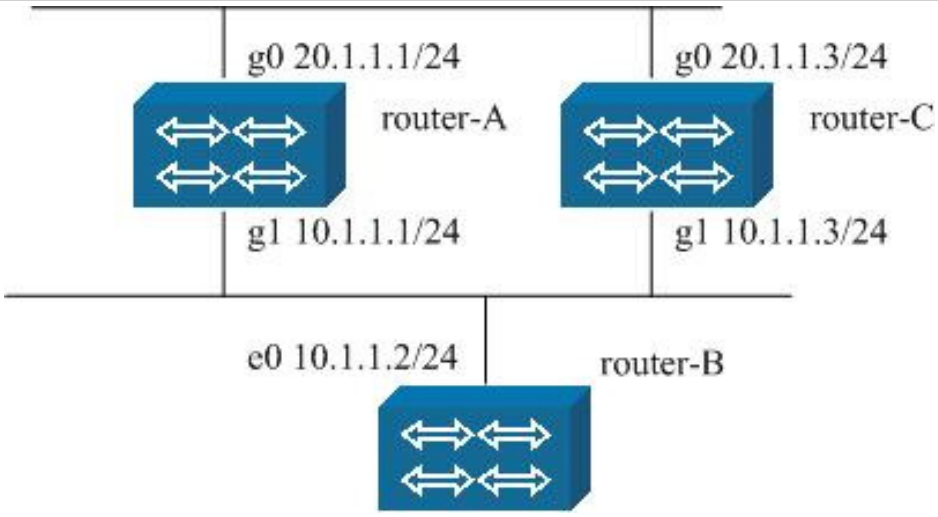
RIP Routing Filter Configuration

Router-A configuration is as 8.3.3.1.
On Router-B:

Command	Description
router-B#configure terminal	Enter global configuration mode
router-B(config)# interface ethernet0	Enter e0
router-B(config-if- ethernet0)# ip address 10.1.1.2 255.255.255.0	Configure ip address
router-B(config)#ip access-list standard 10	Configure standard access list
router-B(config-std-nacl)# deny 20.1.1.0 0.0.0.255	Configure rule deny 20.1.1.0/24
router-B(config)#router rip	Enter RIP configuration mode
router-B(config-rip)# network 10.0.0.0	Same as above
router-B(config-rip)# version 2	Configure RIP version
router-B(config-rip)# distribute-list 10 in e0	Use access list on e0

On Router-B show ip rotue rip,there is no 20.1.1.0/24 RIP routing.

RIP Load Balance Number Configuration



In topology, Router-B can reach LAN via Router-A or Router-C.
Router-A and Router-B configuration are same as 8.3.3.1.

Router-C configuration:

Command	Description
router-C#configure terminal	Enter global configuration mode
router-C(config)# interface gigaethernet0	Enter g0
router-C(config-if-gigaethernet0)# ip address 20.1.1.3 255.255.255.0	Configure ip address
router-C(config-if-gigaethernet0)# interface gigaethernet1	Enter g1
router-C(config-if-gigaethernet1)# ip address 10.1.1.3 255.255.255.0	Configure ip address
router-C(config-if-gigaethernet1)#exit	Exit to global configuration mode
router-C(config)#router rip	Enter RIP configuration mode
router-C(config-rip)# network 20.0.0.0	Designate RIP running network number
router-C(config-rip)# network 10.0.0.0	Same as above
router-C(config-rip)#version 2	Configure RIP version

```
On Router-B show ip route rip,you can examine load balance
routing.
R       20.1.1.0/24 [100/2] via 10.1.1.1, 00:00:06, ethernet0
[100/2] via 10.1.1.3, 00:00:06, ethernet0
```

Configure maximum-path on Router-B to disable RIP load balance function.

Command	Description
router-B#configure terminal	Enter global configuration mode
router-B(config)# interface ethernet0	Enter e0
router-B(config-if- ethernet0)# ip address 10.1.1.2 255.255.255.0	Configure ip address
router-B(config)#router rip	Enter RIP configuration mode
router-B(config-rip)# network 10.0.0.0	Same as above
router-B(config-rip)# version 2	Configure RIP version
router-B(config-rip)# maximum-paths 1	RIP uses only one path to disable load balance.

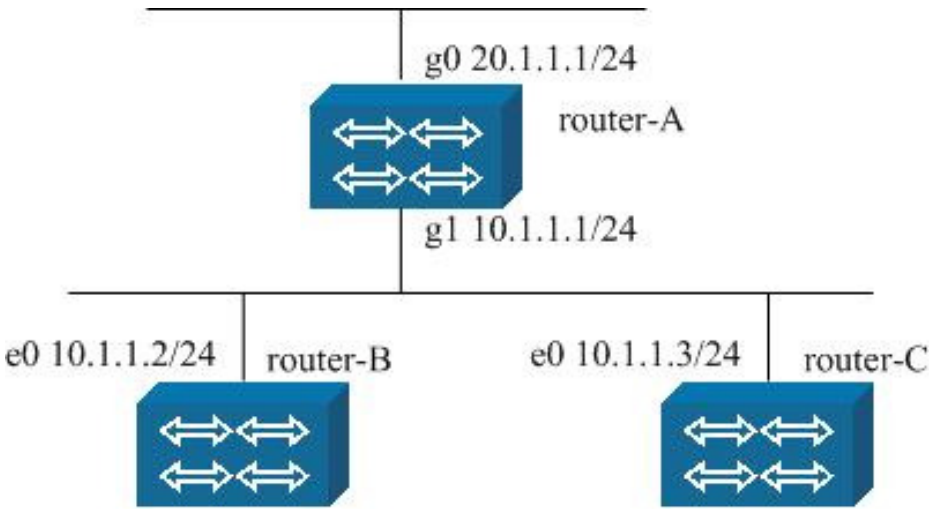
On Router-B show ip route rip,you can examine one routing information.

RIP Passive Interface Configuration

On Router-A:

Command q	Description
router-A#configure terminal	Enter global configuration mode
router-A(config)# interface gigaethernet0	Enter g0
router-A(config-if-gigaethernet0)# ip address 20.1.1.1 255.255.255.0	Configure ip address
router-A(config-if-gigaethernet0)# interface gigaethernet1	Enter g1
router-A(config-if-gigaethernet1)# ip address 10.1.1.1 255.255.255.0	Configure ip address
router-A(config-if-gigaethernet1)#exit	Exit to global configuration mode
router-A(config)#router rip	Enter RIP configuration mode
router-A(config-rip)# network 20.0.0.0	Designate RIP running network number
router-A(config-rip)# network 10.0.0.0	Same as above
router-A(config-rip)# version 2	Configure RIP version
router-A(config-rip)# passive-interface gigaethernet1	Configure g1 as passive interface

RIP Unicast Neighbor Configuration



Router-C configuration:

Command	Description
router-C#configure terminal	Enter global configuration mode
router-C(config)# interface ethernet0	Enter e0
router-C(config-if- ethernet0)# ip address 10.1.1.3 255.255.255.0	Configure ip address
router-C(config)#router rip	Enter RIP configuration mode
router-C(config-rip)# network 10.0.0.0	Same as above
router-C(config-rip)# version 2	Configure RIP version

Router-A and Router-B configurations are same as above.

Router-A configuration:

Command	Description
router-A#configure terminal	Enter global configuration mode
router-A(config)# interface gigaethernet0	Enter g0
router-A(config-if-gigaethernet0)# ip address 20.1.1.1 255.255.255.0	Configure ip address
router-A(config-if-gigaethernet0)# interface gigaethernet1	Enter g1
router-A(config-if-gigaethernet1)# ip address 10.1.1.1 255.255.255.0	Configure ip address
router-A(config-if-gigaethernet1)#exit	Exit to global configuration mode
router-A(config)#router rip	Enter RIP configuration mode
router-A(config-rip)# network 20.0.0.0	Designate RIP running network number
router-A(config-rip)# network 10.0.0.0	Same as above
router-A(config-rip)# version 2	Configure RIP version
router-A(config-rip)# passive-interface gigaethernet1	Configure g1 as passive interface
router-A(config-rip)# neighbor 10.1.1.2	Designate 10.1.1.2 as unicast neighbor

Router-A only updates packet to 10.1.1.2 unicast.

RIP Routing Using Excursion Configuration

The configuration of Router-B is as following:

Command	Description
router-B#configure terminal	Enter global configuration mode
router-B(config)# interface ethernet0	Enter e0
router-B(config-if- ethernet0)# ip address 10.1.1.2 255.255.255.0	Configure ip address
router-B(config)#ip access-list standard 10	Configure standard access list
router-B(config-std-nacl)# permit 20.1.1.0 0.0.0.255	Configure rule permitting 20.1.1.0/24
router-B(config)#router rip	Enter RIP configuration mode
router-B(config-rip)# network 10.0.0.0	Configure RIP running network number
router-B(config-rip)# version 2	Configure RIP version
router-B(config-rip)# offset-list 10 in 2 e0	Use access list on e0

Router-A configuration is same as 8.3.3.1.

```
R  20.1.1.0/24 [120/4] via 10.1.1.1, 00:00:06, ethernet0
```

RIP Routing Redistributing Configuration

Configure static routing on Router-A.

Command	Description
router-A#configure terminal	Enter global configuration mode
router-A(config)# interface gigaethernet0	Enter g0
router-A(config-if-gigaethernet0)# ip address 20.1.1.1 255.255.255.0	Configure ip address
router-A(config-if-gigaethernet0)# interface gigaethernet1	Enter g1
router-A(config-if-gigaethernet1)# ip address 10.1.1.1 255.255.255.0	Configure ip address
router-A(config-if-gigaethernet1)#exit	Exit to global configuration mode
router-A(config)# ip route 5.1.1.0 255.255.255.0 20.1.1.5	Configure static routing
router-A(config)#router rip	Enter RIP configuration mode
router-A(config-rip)# network 20.0.0.0	Designate RIP running network number
router-A(config-rip)# network 10.0.0.0	Same as above

router-A(config-rip)#version 2	Configure RIP version
router-A(config-rip)#redistribute static	Configure RIP redistributing static routing

Router-B configuration is same.

```
Router-B studies routing 5.1.1.0/24 via RIP.
R 5.1.1.0/24 [120/2] via 10.1.1.1, 00:00:06, ethernet0
```

RIP Redistributing Default Consumption Configuration

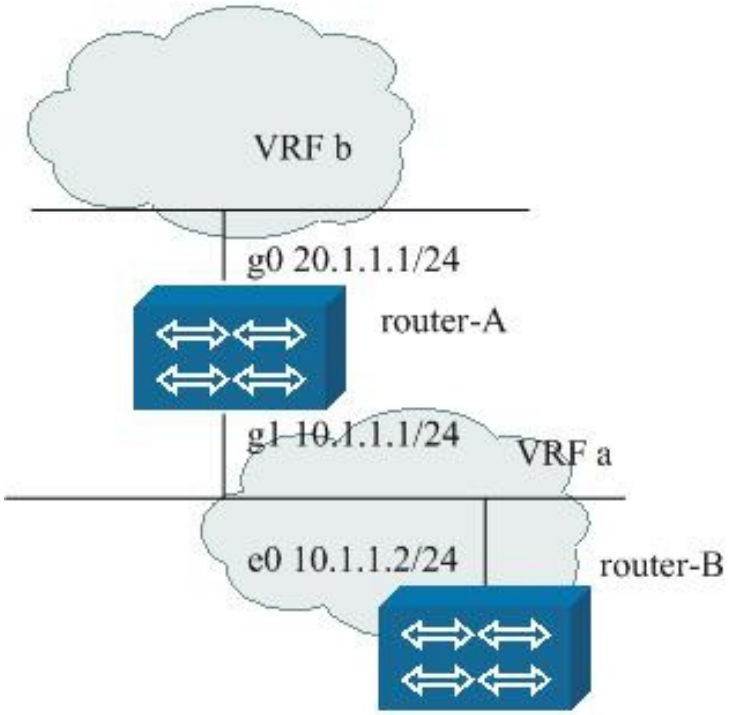
The consumption value is 1. default-metric can modify this value.
On the basis of 8.3.3.10, configure default-metric on Router-A.

Command	Description
router-A#configure terminal	Enter global configuration mode
router-A(config)# interface gigaethernet0	Enter g0
router-A(config-if-gigaethernet0)# ip address 20.1.1.1 255.255.255.0	Configure ip address
router-A(config-if-gigaethernet0)# interface gigaethernet1	Enter g1
router-A(config-if-gigaethernet1)# ip address 10.1.1.1 255.255.255.0	Configure ip address
router-A(config-if-gigaethernet1)#exit	Exit to global configuration mode
router-A(config)# ip route 5.1.1.0 255.255.255.0 20.1.1.5	Configure static routing
router-A(config)#router rip	Enter RIP configuration mode
router-A(config-rip)# network 20.0.0.0	Designate RIP running network number
router-A(config-rip)# network 10.0.0.0	Same as above
router-A(config-rip)# version 2	Configure RIP version
router-A(config-rip)# default-metric 5	Configure RIP redistributing default consumption value 5
router-A(config-rip)# redistribute static	Configure RIP redistributing static routing

Router-B studied 5.1.1.0/24 consumption is 6.

RIP Enables VRF Example

router-A is PE equipment, and the LAN is in VRF a and VRF b. So use RIP in both of them.



Router-A configuration:

Command	Description
router-A#configure terminal	Enter global configuration mode
router-A(config)# ip vrf a	Configure VRF a
router-A(config-vrf)# rd 1:1	Configure RD
router-A(config-vrf)# exit	Exit to global configuration mode
router-A(config)# ip vrf b	Configure VRF b
router-A(config-vrf)# rd 2:2	Configure RD
router-A(config-vrf)# exit	Exit to global configuration mode
router-A(config)# interface gigaethernet0	Enter g0
router-A(config-if-gigaethernet0)# ip vrf forwarding b	Enable g0 running in VRF b
router-A(config-if-gigaethernet0)# ip address 20.1.1.1 255.255.255.0	Configure ip address
router-A(config-if-gigaethernet0)# interface gigaethernet1	Enter g1
router-A(config-if-gigaethernet0)# ip vrf forwarding a	Enable g1 running in VRF a

router-A(config-if-gigaethernet1)# ip address 10.1.1.1 255.255.255.0	Configure ip address
router-A(config-if-gigaethernet1)#exit	Exit to global configuration mode
router-A(config)#router rip	Enter RIP configuration mode
router-A(config-rip)# address-family ipv4 vrf a	Enable RIP VRF a example
router-A(config-rip-af)# network 10.0.0.0	Designate RIP running network number
router-A(config-rip-af)# version 2	Configure RIP version
router-A(config-rip-af)# exit	Exit to RIP configuration mode
router-A(config-rip)# address-family ipv4 vrf b	Enable RIP VRF b example
router-A(config-rip-af)# network 20.0.0.0	Designate RIP running network number
router-A(config-rip-af)# version 2	Configure RIP version
router-A(config-rip-af)# exit	Exit to RIP configuration mode

Router-B configuration is same

Configuring RIP Authentication

Enable MD5 authentication on Router-A and Router-B.

Router-A configuration:

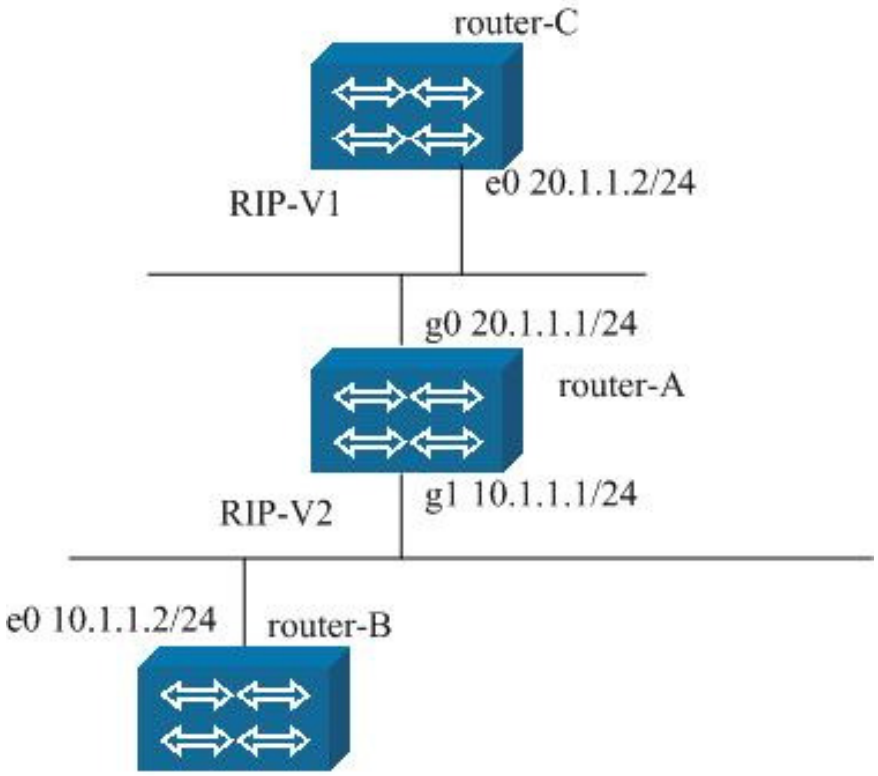
Command	Description
router-A#configure terminal	Enter global configuration mode
router-A(config)# interface gigaethernet0	Enter g0
router-A(config-if-gigaethernet0)# ip address 20.1.1.1 255.255.255.0	Configure ip address
router-A(config-if-gigaethernet0)# interface gigaethernet1	Enter g1
router-A(config-if-gigaethernet1)# ip address 10.1.1.1 255.255.255.0	Configure ip address
router-A(config-if-gigaethernet1)# ip rip authentication mode md5	Designate RIP authentication type is MD5
router-A(config-if-gigaethernet1)# ip rip authentication key 0 signamax	Designate RIP authentication password
router-A(config-if-gigaethernet1)#exit	Exit to global configuration mode
router-A(config)#router rip	Enter RIP configuration mode
router-A(config-rip)# network 20.0.0.0	Designate RIP running network number
router-A(config-rip)# network 10.0.0.0	Same as above

router-A(config-rip)#version 2	Configure RIP version

Router-B configuration:

Command	Description
router-B#configure terminal	Enter global configuration mode
router-B(config)# interface ethernet0	Enter e0
router-B(config-if- ethernet0)# ip address 10.1.1.2 255.255.255.0	Configure ip address
router-A(config-if- ethernet0)# ip rip authentication mode md5	Designate RIP authentication type MD5
router-A(config-if- ethernet0)# ip rip authentication key 0 signamax	Designate RIP authentication password
router-B(config)#router rip	Enter RIP configuration mode
router-B(config-rip)# network 10.0.0.0	Designate RIP running network number
router-B(config-rip)#version 2	Configure RIP version

RIP version sending and accepting configuration



Router-A and Router-B run RIP V2, but Router-A and Router-C only run RIP V1. and this time designate router-A version number on interface.

Router-A configuration:

Command	Description
router-A#configure terminal	Enter global configuration mode
router-A(config)# interface gigaethernet0	Enter g0
router-A(config-if-gigaethernet0)# ip address 20.1.1.1 255.255.255.0	Configure ip address
router-A(config-if-gigaethernet0)# ip rip receive version 1	Designate g0 accepting version 1 RIP packet
router-A(config-if-gigaethernet0)# ip rip send version 1	Designate g0 sending version 1 RIP packet
router-A(config-if-gigaethernet0)# interface gigaethernet1	Enter g1
router-A(config-if-gigaethernet1)# ip address 10.1.1.1 255.255.255.0	Configure ip address
router-A(config-if-gigaethernet1)#exit	Exit to global configuration mode
router-A(config)#router rip	Enter RIP configuration mode
router-A(config-rip)# network 20.0.0.0	Designate RIP running network number
router-A(config-rip)# network 10.0.0.0	Same as above
router-A(config-rip)#version 2	Configure RIP version

Router-B configuration is same as 8.3.3.1.

Router-C configuration:

Command	Description
router-C#configure terminal	Enter global configuration mode
router-C(config)# interface ethernet0	Enter e0
router-C(config-if- ethernet0)# ip address 20.1.1.2 255.255.255.0	Configure ip address
router-C(config)#router rip	Enter RIP configuration mode
router-C(config-rip)# network 20.0.0.0	Designate RIP running network number
router-C(config-rip)#version 1	Configure RIP version

RIP Monitoring/Debugging

Command	Tas k
debug ip rip event	Traces RIP events and messages.
show ip route rip	Show the routing information of RIP has learned

Configuring OSPF Dynamic Routing

Open Shortest Path First (OSPF) is an internal gateway protocol (IGP) used to determine a route in a single Autonomous System (AS). It is more complex, powerful, widely used anmd efficient than RIP. This section explains how to configure OSPF dynamic route protocol for a Signamax router to interconnect networks.

Configure OSPF Commands

Command	Description	Config mode
router ospf process-id [vrf vrfname]	Enable or enable OSPF process from vrf.	config
network network-id wildmask area area-id	*Configure OSPF process and designate OSPF interface (network-id OSPF process network number; Wildmask reverse mask; area-id area id)	config-ospf
area area-id range ip-address netmask [advertise|not-advertise]	Configure area routing aggregation	config-ospf
area area-id default-cost	Configure OSPF STUB or NSSA area default	config-ospf

	cost.	
area transit_area_id virtual-link address	Configure virtual neighbor, and establish virtual link.the address means neighbor' router ID	config-ospf
cost reference-bandwidth bandwidth-value	Configure bandwidth value to account the cost (choose from 1_4294967)	config-ospf
default-information originate {metric metic-value|metric-type metric-type-value}	Configure redistributing default routing	config-ospf
distance {distance-value|ospf {external distance-value |inter-area distance-value | intra-area distance-value }}	Configure external routing management distance. inter-area area routing management distance. intra-area area inner routing management distance	config-ospf
distribute-list access-list-num in/out	Routing filter (the parameter is used to designate access list number)	config-ospf
LeaveOverflowInterval <1-4294967295>	Configure leave overflow time interval(choose from 1_4294967295)	config-ospf
neighbor ip-address	Configure neighbor router (in NBMA network type)	config-ospf
Max {External_LSA number|Sumnet_LSA area-id number}	Configure external lsa or area lsa max number	config-ospf
passive-interface interface	Configure OSPF passive interface	config-ospf
Redistribute {bgp as-number/connected / irmp irmp-number/ rip /snsp /static /ospf process-id}	Configure routing redistribution (BGP, connected, IRMP, RIP, SNSP, static routing and other OSPF process)	config-ospf
router-id ip-address	Configure OSPF router Router ID	config-ospf
summary-address ip-address netmask [tag tag-value]	Configure external route summary function	config-ospf
ip ospf authentication-key 0/7 password	Configure simple text authentication	config-if-XX
ip ospf message-digest-key key_id md5 0/7 password	Configure MD5 authentication	config-if-XX
ip ospf cost cost-value	Configure interface OSPF cost	config-if-XX
ip ospf dead-interval dead-value	Configure neighbor dead time interval	config-if-XX

ip ospf hello-interval hello-value	Configure interface sending HELLO packet time interval	config-if-XX
ip ospf demand-circuit	Configure interface OSPF demand circuit function	config-if-XX
ip ospf network broadcast|non-broadcast|point-to-point|point-to-multipoint	Configure OSPF interface network type (broadcast network/point to point network/point to multipoint network)	config-if-XX
ip ospf poll-interval poll-value	OSPF neighbor poll time interval(only effective to NBMA network)	config-if-XX
ip ospf priority priority-value	Configure OSPF interface priority	config-if-XX
ip ospf retransmit-interval retran-value	Configure retransmit interval	config-if-XX
ip ospf transmit-delay trans-value	Configure link status sending delay time	config-if-XX

Commands Configuring OSPF

Configuration of OSPF is comprised of three sections:

Creating OSPF processes and designating OSPF interfaces

OSPF route configuration mode

Configuring status of OSPF for an interface.

The detailed configuring commands are as follows:

Configuring OSPF process and designating OSPF interface

router(config)#

Command	Description
router ospf <1_65535>[vrf vrfname]	Enters configuring OSPF mode.
network A.B.C.D a.b.c.d area area_id	Configures the OSPF process and designate the OSPF interface. (A.B.C.D Use the network number of OSPF process.

	a.b.c.d inverse-mask area_id area id)

After the OSPF process is created, the process does not know which interface or network it enters; however, it can solve this problem via the command network. This command can designate an interface to a given area . The following command can be used to designate the match interface to the area 0:

router (config-ospf)#network 128.255.0.0 0.0.255.255 area 0

In the command network, all the interfaces capable of matching the pair of the addresses and the inverse mask will be placed into a given area. 0 represents the placeholder, and 1 represents an arbitrary match.

The command network has the function of auto-route summary.

When the command network can match at least one interface address, the OSPF process runs. When the last command network is canceled (by running the command no network…), the OSPF process will be deleted.

Configuring OSPF status parameters

router(config-ospf)#?

Command	Description
area area-id {stub [no-summary]|nssa}	Configure OSPF area type area-id range is 0_4294967295, and it can also identify via ip address form. stub configure area as stub area. no-summary summary-lsa do not flood to this area nssa configure area as NSSA area
area area-id default-cost default-cost	Configure OSPF STUB or NSSA area default cost
area area-id range ip-address netmask [advertise|not-advertise]	Configure OSPF area aggregation routing ip-address aggregation ip address netmask aggregation mask advertise advertised routing not-advertise not advertise this routing.
area transit_area_id virtual-link address	Configure virtual neighbor, and set up virtual link.
cost reference-bandwidth bandwidth-value	Configure bandwidth value to account cost (rang is 1_4294967)
default-information originate {metric metic-value|metric-type metric-type-value}	Configure redistribute default routing configuration
distance {distance-value|ospf {external distance-value |inter-area distance-value | intra-area distance-value }}	Configure OSPF routing administration distance external external routing administration distance inter-area inter-area routing administration distance intra-area internal area routing administration distance
distribute-list access-list-num in/out	Routing filter (the parameter is the number of standard access list)
LeaveOverflowInterval	Configure leave overflow interval
neighbor ip-address	Configure neighbor router (in NBMA network type)
Max {External_lsa number|Sumnet_lsa area-id number}	Configure external lsa or internal lsa max number.
passive-interface <interface number>	Configure OSPF passive interface
redistribute<bgp connected irmp rip snsp static ospf>	Configure routing redistribution (BGP, connected, IRMP, RIP, SNSP, static routing, other OSPF process)
router-id ip-address	Configure OSPF router Router ID
summary-address ip-address netmask [tag tag-value]	Configure external routing summary function

Similarly, the command NO can be used to prohibit the usage of the above command.

Configure the neighbor router:
In order that the OSPF router can be configured to interconnect to a no-broadcasting network, the command can be used to configure a neighbor. In the neighboring address, ip-address is the IP address of the neighboring interface.

commands configuring OSPF for an interface

```
router(config-if-xxx)#ip ospf  ?
```

Command	Description
authentication-key 0/7 password	Configures simple text authentication.
cost	Configures the OSPF cost of interface.
dead-interval	Configures the neighbor dead interval.
hello-interval	Configures the interval for interface to send HELLO packet.
message-digest-key key_id md5 0/7 password	Configures MD5 authentication.
Network broadcast/non-broadcast/point-to-point/point-to-multipoint	Configures OSPF network type (broadcasting network/no-broadcasting network/point-to-point network/point-to-multipoint network).
poll-interval	Configures time between retransmitting hello packet to dead neighbor(for NBMA)
priority	Configures the priority of the router.
retransmit-interval	Configures the declaration interval to retransmit the lost connection status.
transmit-delay	Configures the transmission delay of connection status.
demand-circuit	Configures OSPF demand circuit

On the protocol port of PPP and HDLC, the default type of OSPF network is point-to-point.

On the protocol port of frame relay and X25, the default type of OSPF network is non-broadcast.

Reset OSPF process

```
router#
```

Command	Task

clear ip ospf process	Reset OSPF process

Should reset OSPF proces with Clear command to make router-id command become effective.

STUB/NSSA/Route-Summary/Virtual-Link/Demand-Circuit Configuration Commands

area stub

Use the router configuration command area stub to configure the OSPF stub-area; or, use the command no area stub to disable the function.

```
area  area_id  stub
no  area  area_id  stub
```

Syntax	Task
area_id	The area-id of the stub-area. Its value range is from 0 to 4294967295 or an IP address is used to identify the stub-area.

(By default) No area is configured as the stub area.
(Command mode)the OSPF protocol configuration mode.

(Guide)No type 5 LSA, namely the external LSA, can be received or transmitted in the stub area. The neighborship among routers cannot be established until the command is configured on all the routers in the stub area.

1) When a stub area is configured, the area number cannot be the backbone area number. That is to say that the area number cannot be 0.

2) To cancel the stub area specified in the configuration, use the command no area area_id stub.

area nssa
An nssa area is similar to an OSPF stub area. Type 5 LSA cannot be diffused from the backbone area to the nssa area, but the external route of autonomous system can be introduced into the area by means of finite forms.

By means of redistributing type 7 external LSAintroduced into the nssa area, nssa can convert the type 7 external LSA to type 5 external LSA, which will be flooded to other areas of the autonomous system via the border router in the nssa area.

Use the command area nssa to configure an area as an nssa area (not-so-stubby area); or, use the command no area nssa to cancel the attribute nssa of the area.

```
area  area_id  nssa
no  area  area_id  nssa
```

Syntax	Task
area_id	The area-id of the nssa area. Its value range is from 0 to 4294967295 or an IP address is used to identify the nssa area.

(By default) No area is configured as the nssa area.
(Command mode)the OSPF protocol configuration mode.

(Guide)An nssa area is similar to a stub area. Type 5 LSA cannot be diffused from the backbone area to the nssa area, but the external route of autonomous system can be introduced into the area by means of finite forms.

The backbone area cannot be configured as the nssa area.

Any router in the same area should support nssa area, or else the neighborship among the routers cannot be established.

If it is possible, try not to adopt the explicit redistribution on nssa abr because the packets converted by the router are confused easily.

area range

Use the command area range to realize the route summary of areas; or, use the command no area range to disable it.

```
area  area_id  range  address  mask
no  area  area_id  range  address  mask
```

Syntax	Task
area_id	The OSPF area-id. And its value range is from 0 to 4294967295
address	The network IP address.
mask	The network IP address.mask

(By default) No route summary area range is configured.
(Command mode)the OSPF protocol configuration mode.
(Guide)Route summary is a set of routes generated by the area border router and the AS border router and will be announced to the neighbor routers.

If network numbers in an area is successive, the area border router and the AS border router can be configured to announce the route summary

that specifies the range of network numbers. The route summary can reduce the size of link-state database.

The OSPF route summary can be classified into inter-area route summary and external route summary. After configured with the command area range, the area border router summarizes the routes in the configured network segment and generates a route profile summary net lsa, which is notified by the area border router to other areas, and lsa in the network segment will not be notified any more.

The command area range can take effect on nothing but the area border router.

Use the command no area range to cancel the command route summary.

summary-address
Use the command summary-address to perform OSPF external route summary; or, use the command no summary-address to make the command out of work.

```
summary-address address mask [tag tag-value]
no summary-address address mask [tag tag-value]
```

Syntax	Description
address	The network IP address.
mask	The network IP address mask
tag-value	The tag-value of the summarized ase lsa. And its value range is from 0 to 4294967295

(By default) No the command summary-address is configured.
(Command mode)the OSPF protocol configuration mode
(Guide)When the route is redistributed from other protocols to OSPF, each route is singly announced in the external link-status announcement.

The command summary-address is used to summarize all redistributed routes covered by the special network address and mask as one route. The size of OSPF link-state database can be reduced.

Use the command summary-address to summarize external routes. And the command is used to summarize all ase lsa in the network segment and generate a summary ase lsa. Only the summary ase lsa is announced to other routers via ASBR.

1) The command can take effect on nothing but ASBR and summarize the external routes redistributed by OSPF.

2) Use the command no summary-address to cancel the summary command of the external route.

area virtual-link (Configuring a virtual link)

In OSPF, all areas should be connected directly to the backbone area. When performing network design, however, an area may be out of the backbone area or the backbone area may be isolated. To resolve the problems above, a virtual link can be adopted.

The virtual link can be applied in the following two kinds of conditions: two isolated backbone area can be connected together by means of configuring the virtual link; a third area, via an area (called transit area) connecting with the backbone area, is connected to the backbone area.

```
area  transit_area_id  virtual-link  address
no  area  transit_area_id  virtual-link  address
```

Syntax	Description
transit_area_id	The area number of virtual-link transit area. Its value range is from 0 to 4294967295, or an IP address is used to identify the area.
Address	The router ID of the virtual-link opposite end (neighbor).

(By default) No area is configured as virtual-link.
(Command mode)the OSPF protocol configuration mode.

(Guide) In OSPF, the backbone area should keep the full-connected state all along and all areas should be connected to the backbone area. If the backbone area is divided into two or more parts, then some destinations are unreachable. To ensure the prescriptions of OSPF network, a virtual-link can be employed for the isolated backbone areas and the areas that have not been connected with the backbone area.

Each virtual-link can be identified uniquely by means of the transit area and the router ID of the virtual-link opposite end.

Configuring the demand-circuit

The demand-circuit is a network whose expenditure changes with network usage. The expenditure can be based on connection time and transmitted packet bits. The typical demand-circuit comprises ISDN circuit, X.25SVC and dial-up circuit. The data link need keep open for the previous OSPF.

This will result in the needless expenses. After the demand-circuit is added, OSPF Hello message and route update information are restricted on the demand-circuit, and the data link is allowed to be close when no data is transmitted.

```
router(config-if-serial0/0)#ip ospf demand-circuit
```

Syntax	Description
demand-circuit	Enable the demand-circuit on the interface.

When the demand-circuit is enabled between routers, the demand-circuit can be configured on the interface of one side or both sides.

The demand-circuit can take effect only in the point-to-point interface type or in the point-to-multipoint interface type.

The router configured with the virtual-link should be an area border router.

The virtual-link is identified by router-id of the router on the other end.

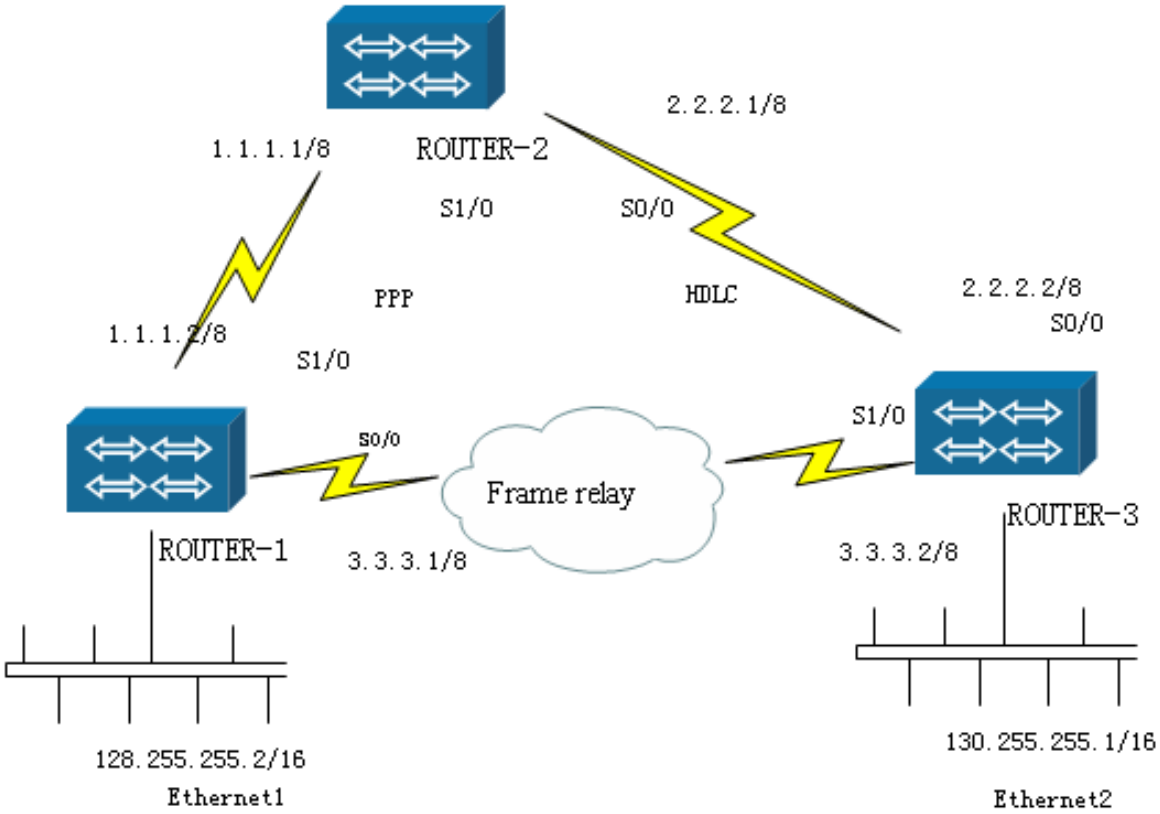
The two end routers configured with the virtual-link should be located in the same public area that is called virtual-link transit area.

The virtual-link can be regarded as one part of the backbone area or as unnumbered point-to-point network. Its cost is the spending of the link and cannot be configured.

Use the command no area virtual-link to cancel the link configuration command

The virtual-link cannot be configured via the stub area. That is to say that the virtual-link transit area cannot be the stub area.

OSPF Configuration Examples



A PPP link runs between router-1 and the interface serial1/0 of router-2, Frame Relay runs between the interface serial0/0 of router1 and the interface serial1/0 of router3, and HDLC link runs between the router2 and the interface serial0/0 of router3.

During the course of configuring OSPF dynamic routing protocol for a Signamax router to connect, the following tasks should be completed:

a) Establishing the OSPF process
b) Configuring OSPF interface parameters

The concrete configuration of Router1:

Command	Task
router-1#configure terminal	
router-1(config)#router ospf 2	Enters the mode of configuring OSPF.
router-1(config-ospf)#network 1.0.0.0 0.255.255.255 area 3 router-1(config-ospf)#network 3.0.0.0 0.255.255.255 area 3	Establishes the OSPF process and designates related OSPF interface.
router-1(config-ospf)#network 128.255.0.0 0.0.255.255 area 3	
router-1(config-ospf)# neighbor 3.3.3.2	Configures 3.3.3.2 as a neighbor.
router-1(config-ospf)#exit	
router-1(config)#int s0/0 router-1(config-if-serial0/0)# ip ospf network non-broadcast	The type of OSPF network is non-broadcast (NBMA).
router-1(config-if-serial0/0)#exit	
router-1(config)#int s1/0	The type of OSPF network is point-to-point.
router-1(config-if-serial1/0)# ip ospf network point-to-point router-1(config-if-serial1/0)#exit	
router-1(config)#int f0	The type of OSPF network is broadcasting.
router-1(config-if-fastethernet0)# ip ospf network broadcast	
router-1(config-if-fastethernet0)# end	

The concrete configuration of Router2:

Command	Task
Router-2#configure terminal	
router-2(config)#router ospf 2	Establishes an OSPF process and designate related OSPF interface.
router-2(config-ospf)#network 1.0.0.0 0.255.255.255 area 3 router-2(config-ospf)#network 2.0.0.0 0.255.255.255 area 3 router-2(config-ospf)#exit	
router-3(config)#int s0/0 router-2(config-if-serial0/0)#ip ospf network point-to-point	
router-2(config-if-serial0/0)#exit	

router-2(config)#int s1/0	
router-2(config-if-serial1/0)# ip ospf network point-to-point router-2(config-if-serial1/0)#end	

The concrete configuration of Router3:

Command	Task
router-3#configure terminal router-3(config)#router ospf 2 router-3(config-ospf)#network 2.0.0.0 0.255.255.255 area 3 router-3(config-ospf)#network 3.0.0.0 0.255.255.255 area 3 router-3(config-ospf)#network 130.255.0.0 0.0.255.255 area 3 router-3(config-ospf)# neighbor 3.3.3.1 router-3(config-ospf)#exit	Establishes an OSPF process and designates related OSPF interface.
router-3(config)#int s1/0 router-3(config-if-serial1/0)# ip ospf network non-broadcast router-3(config-if-serial1/0)#exit	
router-3(config)#int s0/0 router-3(config-if-serial0/0)# ip ospf network point-to-point router-3(config-if-serial0/0)#exit	
router-3(config)#int f0 router-3(config-if-fastethernet0)# ip ospf network broadcast router-3(config-if-fastethernet0)#end	

Debugging/Monitoring OSPF

Monitoring OSPF

Command	Description
show ip ospf interface (Displaying information of the OSPF interface)	Interface: 44.1.1.1 (serial0/0) Area 0 Cost: 1 State: BackupDR Status: the Backup designated Router Type: NBMA Type: non-broadcast (NBMA) Priority: 1 The priority of the interface: 1 Designated router: 44.1.1.2 Designated Router:44.1.1.2 Backup Designated router: 44.1.1.1 Backup designated Router:44.1.1.1 Authentication: none Authentication: none Timers:

	Hello: 30 Poll: 2:00 Dead: 2:00 Retrans: 5 Neighbors MprouterID: 111.2.2.2 Neighbor Count is 1 Neighbor number:1 Interface:142.255.255.1 (fastethernet0) Area 0 Cost: 1 State: DR Type: Broadcast Priority: 1 Designated router: 142.255.255.1 Authentication: none Timers: Hello: 10 Poll: 0 Dead: 40 Retrans: 5 Neighbor Count is 0
show ip ospf interface name (Monitoring information of an OSPF interface)	Interface: 44.1.1.1 (serial0/0) Area 0 Cost: 1 State: BackupDR Type: NBMA Priority: 1 Designated router: 44.1.1.2 Backup Designated router: 44.1.1.1 Authentication: none Timers: Hello: 30 Poll: 2:00 Dead: 2:00 Retrans: 5 Neighbors MprouterID: 111.2.2.2 Neighbor Count is 1
show ip ospf neighbor (Displaying OSPF neighbor)	Neighbor ID Pri State Dead Time Address serial 111.2.2.2 1 Full/Dr 120 44.1.1.2 serial0
show ip ospf database [process-id][adv-router [self_originate| A.B.C.D]] (Displays lists of information related to the OSPF database of self_originated or special .)	sh ip os da adv-router 33.33.33.33 OSPF Router with ID (4.4.4.4) (Process ID 2) ASE link states (AREA 0) Link ID ADV router Age Seq# CheckSum 111.1.1.1 33.33.33.33 661 80000002 1c8a Router link states (AREA 113) Link ID ADV router Age Seq# CheckSum Link Count 33.33.33.33 33.33.33.33 448 8000000d ee8c 1 Net link states (AREA 113) Link ID ADV router Age Seq# CheckSum Link Count 128.255.43.5 33.33.33.33 448 80000003

	640f 2 ASE link states (AREA 113) Link ID ADV router Age Seq# CheckSum 111.1.1.1 33.33.33.33 661 80000002 1c8a sh ip os da adv-router self_originate OSPF Router with ID (4.4.4.4) (Process ID 2) Router link states (AREA 0) Link ID ADV router Age Seq# CheckSum Link Count 4.4.4.4 4.4.4.4 1091 80000004 b4ba 1 SumNet link states (AREA 0) Link ID ADV router Age Seq# CheckSum 128.255.40 4.4.4.4 1096 80000002 128a SumASB link states (AREA 0) Link ID ADV router Age Seq# CheckSum 33.33.33.33 4.4.4.4 1091 80000001 615c Router link states (AREA 113) Link ID ADV router Age Seq# CheckSum Link Count 4.4.4.4 4.4.4.4 1091 80000008 7849 1 SumNet link states (AREA 113) Link ID ADV router Age Seq# CheckSum 138.255.43 4.4.4.4 1086 80000001 7f0e
show ip ospf database [process-id] [router/network/summary/ asbr-summary/external/ nssa-external] [adv-router [self_originate| A.B.C.D]] (displays lists of detail information related to the special type OSPF database of self_originated or special advertising router.)	show ip ospf database network OSPF Router with ID (4.4.4.4) (Process ID 2) Net link states (AREA 113)LS age : 997 options : <DC> LS_TYPE : Net Link State ID : 128.255.43.5 Advertising Router : 33.33.33.33 LS Seq Number : 0x80000003 CHECKSUM :0x640f LS length : 32 Route : Canreach Time:0 Network Mask:255.255.252 Network:128.255.40 Att_rtr number: 2 Attached Router: 33.33.33.33 Attached Router: 4.4.4.4

Show ip ospf routing (displays lists of detail information related to the routes calculated by spf .)	sh ip os routing OSPF ROUTING IN VRF 0 OSPF PROCESS 2 Routes To Area Border: AREA: 0 Router Cost AdvRouter NextHop(s) RTAB_REV 4.4.4.4 0 4.4.4.4 Myself 10 AREA: 113 Router Cost AdvRouter NextHop(s) RTAB_REV 4.4.4.4 0 4.4.4.4 Myself 11 Routes To AS Border: AREA: 0 Router Cost AdvRouter NextHop(s) RTAB_REV AREA: 113 Router Cost AdvRouter NextHop(s) RTAB_REV 33.33.33.33 1000 33.33.33.33 128.255.43.5 11 Inter AREA: Router Cost AdvRouter NextHop(s) RTAB_REV AS Intra Routes: Dest Mask LSID AdvRouter Cost Ptype NextHop(s) Area RTAB_REV 128.255.40 255.255.252 128.255.43.5 33.33.33.33 1000 2 128.255.43.4 0.0.0.113 11 138.255.43 255.255.255 138.255.43 4.4.4.4 1000 0 138.255.43.4 0.0.0.0 10 AS External Routes: Dest Mask LSID AdvRouter Cost Ptype Etype NextHop(s) Area RTAB_REV 111.1.1.1 255.255.255.255 111.1.1.1 33.33.33.33 20 5 1 128.255.43.5 0.0.0.113 11

OSPF Debugging Commands

Command	Description
debug ip ospf all	Displays all the debugging information.
debug ip ospf lsa	Traces the link status announces.
debug ip ospf events	Traces events and messages.
debug ip ospf packet hello / dd / lsr / lsu / ack / all	Traces the reception/sending of messages. hello: HELLO message dd: database description message lsr: link status request message

	lsu: link status update message ack: acknowledge message on accepting link status update all: the detailed contents of all the OSPF messages
debug ip ospf route	Traces the change of the routing table.
debug ip ospf spf	Traces the shortest path tree algorithm.
debug ip ospf state	Traces the state machine.
debug ip ospf task	Traces tasks.
debug ip ospf timer	Traces the timer.

Configuring IRMP Dynamic Route

IRMP (Internal Routing Message Protocol) is a kind of dynamic routing protocol based on link status. It overcomes the shortcomings of the Distance Vector Routing Protocol (DVRP) and does not require the heavy overhead.

IRMP supports multiple Autonomous Systems (AS), which can run independently without disturbing each other, and be fit for more large-scale networks, it is a popular routing protocol.

This chapter explains how to configure the dynamic routing protocol IRMP on Signamax routers enabling it to interconnect networks.

IRMP Commands

Command	Description	Config mode
router irmp autonomous-system	*enter IRMP routing configuration mode(autonmous system number)	config
network network-number [wild-mask]	*designate IRMP network number and reverse mask	config-irmp
auto-summary	*auto summary, only for connected routing	config-irmp
default-metric bandwidth delay reliability loading mtu	*configure IRMP introducting other protocols default parameters (bandwidth, time delay, reliability, load, mtu)	config-irmp
distance irmp distance-for-internal distance-for-external	*configure local IRMP internal and external routing administration distance	config-irmp
distribute-list access-list-name {in|out} [interface]	*filter routing information	config-irmp
distribute-list gateway prefix-list-name in [interface]		
distribute-list prefix prefix-list-name {in|out} [interface]		

distribute-list prefix prefix-list-name gateway prefix-list-name in [interface]		
maximum-paths path-num	Choose path number for load balance	config-irmp
metric weights TOS k1 k2 k3 k4 k5	Change IRMP K value. TOS is service type, only supports type0.	config-irmp
neighbor ip-address interface	*define neighbor router	config-irmp
offset-list access-list-name {in|out} offset-value [interface]	Change routing metric excursion value	config-irmp
passive-interface interface	*disable interface accepting and sending IRMP packet information	config-irmp
redistribute protocol [process-id] [route-map]	*configure routing redistribution	config-irmp
timers active-time minutes	Configure active overtime timer	config-irmp
variance metric-variance-multiplier	Configure variance multiplier	config-irmp
ip message-digest-key irmp autonomous-system key_id md5 {0|7} string	*configure authentication	config-if-××
ip hello-interval irmp autonomous-system seconds	Configure hello packet time interval	config-if-××
ip hold-time irmp autonomous-system seconds	Configure neighbor invalid time	config-if-××
ip summary-address irmp autonomous-system network-number mask	*routing summary on interface	config-if-××
ip split-horizin irmp autonomous-system	Enable horizontal split	config-if-××

Configure IRMP

Configuring IRMP routing involves these three main principles:

Establishing IRMP process and designating the IRMP interface;

Entering the IRMP route configuration mode;

Entering the interface IRMP configuration mode.

The detailed configuring commands are as follows:

Configuring IRMP process and designating IRMP interface

Router(config)#?

Command	Description
router irmp autonomous-system	Enters the IRMP route configuration mode (Autonomous System number)
network network-number [wild-mask]	Runs IRMP on an interface within the designated network range. Network number, inverse-mask

IRMP routing protocol supports many ASes (Autonomous system) and they can run independently without disturbing each other. The interface running IRMP can send/accept IRMP messages; however, if the interface has not been designated, then it cannot send/accept IRMP messages, and its route cannot be sent from any other interface.

Entering the IRMP route configuration mode

router(config-irmp)#?

Command	Description
auto-summary	Automatic summary. And only summarize direct routes.
compatible oldversion	Advertise external routes as internal routes
default-metric bandwidth delay reliability mtu loading	Set the default parameters (bandwidth, delay, realibility, mtu, load) for IRMP to introduce other routing protocols.
distance irmp distance-for-internal distance-for-external	Define an administrative distance of the local RIMP internal routes and external routes
distribute-list access-list-name {in|out} [interface]	Filter the route information.
distribute-list gateway prefix-list-name in [interface]	
distribute-list prefix prefix-list-name gateway prefix-list-name in [interface]	
distribute-list prefix prefix-list-name {in|out} [interface]	
network network-number [wild-mask]	Designate the network interface running IRMP .
passive-interface interface	Prohibit the interface from sending/receiving IRMP route information.
Redistribute protocol [route-map]	Configure routing redistribution.
timers active-time minutes	Adjust active timers.
variance metric-variance-multiplier	When the load is of balance, configure the load balancing variance.

Similarly, the command NO can be used to prohibit the usage of the above commands.

Prohibiting an interface from receiving/sending IRMP messages

If you do not want IRMP to take effect on an interface, you can configure the command passive-interface to inhibit IRMP from becoming effective on it. After the configuration, IRMP will not receive/send IRMP message on the interface.

Configuring the routing filter

In some situations, it is likely required to ignore some IRMP routing information accepted or to prohibit the neighbor router from getting some IRMP routing information. The IRMP routing protocol can achieve it via referring to the access list.

Configuring routing redistribution

IRMP can share routing information of opposite parties by redistributing the routing information of other routing protocols.

Commands configuring IRMP of an interface:

router(config-if-xxx)# ?

Command	Description
ip message-digest-key irmp autonomous-sytem key_id md5 0/7 string	Configures authentication.
ip hello-interval irmp autonomous-system seconds	Configures the interval between HELLO messages.
ip hold-time irmp autonomous-system seconds	Configures the neighbor hold-time.
no ip hello-interval irmp autonomous-system	Deletes the configured interval between HELLO messages.
no ip hold-time irmp autonomous-system	Cancels the configured neighbor hold-time.
ip split-horizon irmp autonomous-system	Enables split-horizon.
no ip split-horizin irmp autonomous-sytem	Prohibits split-horizon.
ip summary-address irmp autonomous-system network-number mask	Perform address summarization on the interface
no ip summary-address irmp autonomous-system network-number mask	Disable address summarization on the interface.

When the IRMP MD5 authentication mode is configured, it should be authenticated, and the key_id of the two ends should be congruous; 0 in the command indicates plaintext input while 7 indicates cryptograph input.

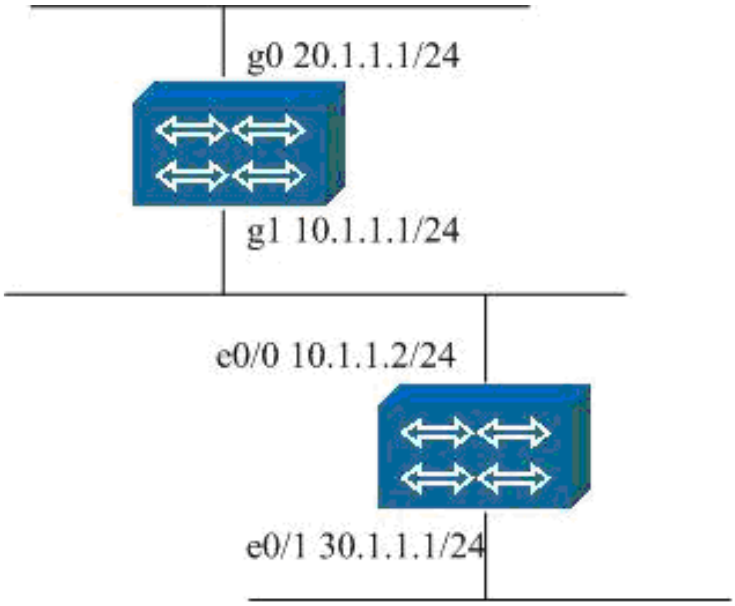
Configuring the interval between HELLO messages and the neighbor hold-time can be described as follows:

The default IRMP sends HELLO messages at 5 second intervals on a broadcasting interface or a point-to-point one, or at 60 second intervals on a NBMA interface. After accepting the HELLO messages, it will add the opposite terminal router to the neighboring table of itself.

If the neighbor already exists in the neighbor table, the neighboring hold-timer will refresh. If the default IRMP in the hold time, has not accepted any HELLO message sent by a neighbor all along, it will think that the neighbor has be invalidated and it will be deleted from the neighbor table. The default hold time will be 3 times the length of the hello time.

Prohibiting horizontal split
In the default situation, IRMP uses the split-horizon on an interface, and it is not recommended that split-horizon be prohibited on a non-NBMA interface.

IRMP Configuration



In the configuration above, the router cisco in the above figure is a Cisco router while Signamax is a Signamax Router.

IRMP Enabling Configuration

Signamax router configuration:

Cisco router configuration:

Command	Description
signamax#configure terminal	
signamax(config)#router irmp 100	Enable IRMP
signamax(config-irmp)#network 10.0.0.0	Designate IRMP running network
signamax(config-irmp)#network 20.0.0.0	Same as above
signamax(config-irmp)#end	

Cisco router configuration:

Command	Description
cisco#configure terminal	
cisco(config)#router eigrp 100	Enable EIGRP
cisco(config-router)#network 10.0.0.0	Designate IRMP running network
cisco(config-router)#network 30.0.0.0	Same as above
cisco(config-router)#no auto-summary	Disable Cisco auto summary
cisco(config-router)#end	

```
Signamax:
show ip irmp neighbor  and  show ip route irmp:
signamax#show ip irmp neighbor
IP-IRMP neighbors for process 100
H       Address         Interface              Hold    Uptime
Seq
                                                       (sec)
Num
0       10.1.1.2        gigaethernet1          12      00:04:30
4
signamax#show ip route irmp
E   30.1.1.0/24 [90/281856] via 10.1.1.2, 00:04:20, gigaethernet1

Cisco:
show ip eigrp neighbors  and  show ip route eigrp:
cisco#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address                 Interface   Hold Uptime   SRTT   RTO  Q
Seq Type
                                        (sec)         (ms)       Cnt
Num
0   10.1.1.1                Et0/0         14 00:05:50    1   200  0
2
cisco#show ip route eigrp
     20.0.0.0/24 is subnetted, 1 subnets
D       20.1.1.0 [90/281856] via 10.1.1.1, 00:05:56, Ethernet0/0
```

IRMP auto summary configuration

Configure auto summary on Signamax.

Command	Description
signamax#configure terminal	
signamax(config)#router irmp 100	Enable IRMP
signamax(config-irmp)#network 10.0.0.0	Designate IRMP running network
signamax(config-irmp)#network 20.0.0.0	Same as above
signamax(config-irmp)#auto-summary	Auto summary
signamax(config-irmp)#end	

Cisco configuration is same as 8.5.3.1.
Cisco studies summary routing 20.0.0.0/8,but not 20.1.1.0/24.

IRMP Administration Distance Configuration

Adjust Signamax IRMP routing administration administration distance.

Command	Description
signamax#configure terminal	
signamax(config)#router irmp 100	Enable IRMP
signamax(config-irmp)#network 10.0.0.0	Designate IRMP running network
signamax(config-irmp)#network 20.0.0.0	Same as above
signamax(config-irmp)#distance 100 150	Configure IRMP inner routing administration distance 100,external routing administration distance 150.
signamax(config-irmp)#end	

Cisco configuration is same.

On Signamax show ip route irmp, IRMP routing administration distance has been adjusted.

```
E       30.1.1.0/24   [100/281856]   via   10.1.1.2,   00:04:20,
gigaethernet1
```

IRMP Routing Filter Configuration

Configure Signamax and filter routing 30.1.1.0/24.

Command	Description
signamax#configure terminal	
signamax(config)#ip access-list standard 10	Configure standard access list
signamax(config-std-nacl)#deny 30.1.1.0 0.0.0.255	Configure rule deny routing
signamax(config-std-nacl)#exit	
signamax(config)#router irmp 100	Enable IRMP
signamax(config-irmp)#network 10.0.0.0	Designate IRMP running network
signamax(config-irmp)#network 20.0.0.0	Same as above
signamax(config-irmp)#ditribute-list 10 in g1	Enable access list on g1, for routing filter
signamax(config-irmp)#end	

IRMP Static Neighbor Configuration

Configure Signamax and Cisco making them static neighbor for each other.

Signamax:

Command	Description
signamax#configure terminal	
signamax(config)#router irmp 100	Enable IRMP
signamax(config-irmp)#network 10.0.0.0	Designate IRMP running network
signamax(config-irmp)#network 20.0.0.0	Same as above
signamax(config-irmp)#neighbor 10.1.1.2 g1	Designate 10.1.1.2 as static neighbor
signamax(config-irmp)#end	

CICSO:

Command	Description
cisco#configure terminal	
cisco(config)#router eigrp 100	Enable EIGRP
cisco(config-router)#network 10.0.0.0	Designate EIGRP running network
cisco(config-router)#network 30.0.0.0	Same as above
cisco(config-router)#no auto-summary	Disable Cisco auto summary

cisco(config-router)#neighbor 10.1.1.1 e0/0	Designate 10.1.1.1 as static neighbor
cisco(config-router)#end	

After above configuration, Signamax and Cisco establish neighbor and study routing. All IRMP/EIGRP packet between Signamax and Cisco adopt unicast mode.

IRMP Passive Interface Configuration

Configure g0 as passive interface.

Command	Description
signamax#configure terminal	
signamax(config)#router irmp 100	Enable IRMP
signamax(config-irmp)#network 10.0.0.0	Designate IRMP running network
signamax(config-irmp)#network 20.0.0.0	Same as above
signamax(config-irmp)#passive-interface g0	Configure g0 as passive interface
signamax(config-irmp)#end	

Cisco configuration is same.
G0 will not send any IRMP or accept IRMP packet.

IRMP Redistribution Configuration

Configure static routing on Signamax. When redistributing static routing in IRMP, Cisco will study these static routing.

Command	Description
signamax#configure terminal	
signamax(config)#ip route 5.1.1.0 255.255.255.0 20.1.1.10	Configure static routing
signamax(config)#ip route 5.1.1.0 255.255.255.0 20.1.1.10	Same as above
signamax(config)#ip route 5.1.3.0 255.255.255.0 20.1.1.10	Same as above
signamax(config)#router irmp 100	Enable IRMP
signamax(config-irmp)#network 10.0.0.0	Designate IRMP running network
signamax(config-irmp)#network 20.0.0.0	Same as above
signamax(config-irmp)#default-metric 1000000 1 255 1 1500	Configure redistributing routing metric.
signamax(config-irmp)#redistribute static	Redistributing static routing.
signamax(config-irmp)#end	

Cisco configuration is same.

Cisco studies these static routing information.

```
D EX    5.1.1.0 [170/281856] via 10.1.1.1, 00:01:14, Ethernet0/0
D EX    5.1.2.0 [170/281856] via 10.1.1.1, 00:01:14, Ethernet0/0
D EX    5.1.3.0 [170/281856] via 10.1.1.1, 00:01:14, Ethernet0/0
```

IRMP Authentication Configuration

Enable IRMP authentication on Signamax and Cisco.

SIGNAMAX:

Command	Description
signamax#configure terminal	
signamax(config)# interface gigaethernet 1	Enter interface mode
signamax(config-if-gigaethernet1)# ip message-digest-key irmp 100 1 md5 0 signamax	Configure authentication
signamax(config-if-gigaethernet1)#exit	
signamax(config)#router irmp 100	Enable IRMP
signamax(config-irmp)#network 10.0.0.0	Designate IRMP running network
signamax(config-irmp)#network 20.0.0.0	Same as above
signamax(config-irmp)#end	

CISCO:

Command	Description
cisco#configure terminal	
cisco(config)#key chain Eigrp100	Configure keychain
cisco(config-keychain)#key 1	Configure key ID
cisco(config-keychain-key)#key-string signamax	Configure password
cisco(config-keychain-key)#exit	
cisco(config-keychain)#exit	
cisco(config)#interface e0/0	Enter interface mode
cisco(config-if)#ip authentication mode eigrp 100 md5	Configure MD5 authentication
cisco(config-if)#ip authentication key-chain eigrp 100 Eigrp100	Designate using key chain for authentication
cisco(config-if)#exit	
cisco(config)#router eigrp 100	Enable EIGRP
cisco(config-router)#network 10.0.0.0	Designate EIGRP running network
cisco(config-router)#network 30.0.0.0	Same as above
cisco(config-router)#no auto-summary	Disable Cisco auto summary
cisco(config-router)#end	

IRMP Address Summary Configuration

Cisco studies three subnet static routing information. And summarize on Signamax. Signamax will summarizes them to one routing information and then sends it to Cisco.

Command	Description
signamax#configure terminal	
signamax(config)#ip route 5.1.1.0 255.255.255.0 20.1.1.10	Configure static routing
signamax(config)#ip route 5.1.1.0 255.255.255.0 20.1.1.10	Same as above
signamax(config)#ip route 5.1.3.0 255.255.255.0 20.1.1.10	Same as above
signamax(config)#interface g1	Enter interface configuration mode
signamax(config-if-gigaethernet1)#ip summary-address irmp 100 5.1.0.0 255.255.0.0	Designate summary routing 5.1.0.0/16
signamax(config-if-gigaethernet1)#exit	
signamax(config)#router irmp 100	Enable IRMP
signamax(config-irmp)#network 10.0.0.0	Designate IRMP running network
signamax(config-irmp)#network 20.0.0.0	Same as above
signamax(config-irmp)#default-metric 1000000 1 255 1 1500	Configure redistribution metric.
signamax(config-irmp)#redistribute static	Redistribute static routing
signamax(config-irmp)#end	

Cisco configuration is same as 8.5.3.1.

After the configuration, Cisco studies one summary routing.

```
D       5.1.0.0 [90/281856] via 10.1.1.1, 00:02:04,
Ethernet0/0
```

Debugging/monitoring IRMP

IRMP monitoring information

Command	Description
show ip irmp interface [interface]	Displays interface information of IRMP .
show ip irmp neighbor [autonomous-system / detail / interface]	Displays neighbor information of IRMP
show ip irmp topology [active / summary / network]	Displays routing information of IRMP

Debugging commands of IRMP

Command	Description
debug ip irmp events	Displays debug information of IRMP events.
debug ip irmp route	Displays debug information of IRMP route.
debug ip irmp timer	Displays IRMP timer.
debug ip irmp packets [hello / terse]	Displays debug information of IRMP messages.
debug ip irmp all	Displays debug information of all the IRMP .

Debug ip irmp packets terse Displays messages including the routing information except HELLO. debug ip irmp packets terse detail Displays detailed information of each route.

Configuring SNSP Route

SNSP (Stub Network Search Protocol) uses Neighbor Device Search Protocol (NDSP),a protocol used to discover other devices on either broadcast or non-broadcast media, to propagate the connected IP prefix of a stub router. SNSP was designed for customers who do not want to usr network bandwidth for routing protocol updates.

Static routing is a good choice,but there is too much overhead to manually maintain th static route.SNSP is not CPU-intensive and is used when IP routes are propagated dynamically on Layer2. SNSP is a perfect solution for hub and spoke topology.

Commands to Configure SNSP

The commands used for configuring SNSP are very simple. Just configure the router snsp command in the hub router and turn off any dynamic routing protocols in the spoke routers. Spoke routers will automatically start advertising their subnets using NDSP. You do not need the router snsp command on spoke routers.

The detailed configuring commands are as follows:

Router(config)# ?

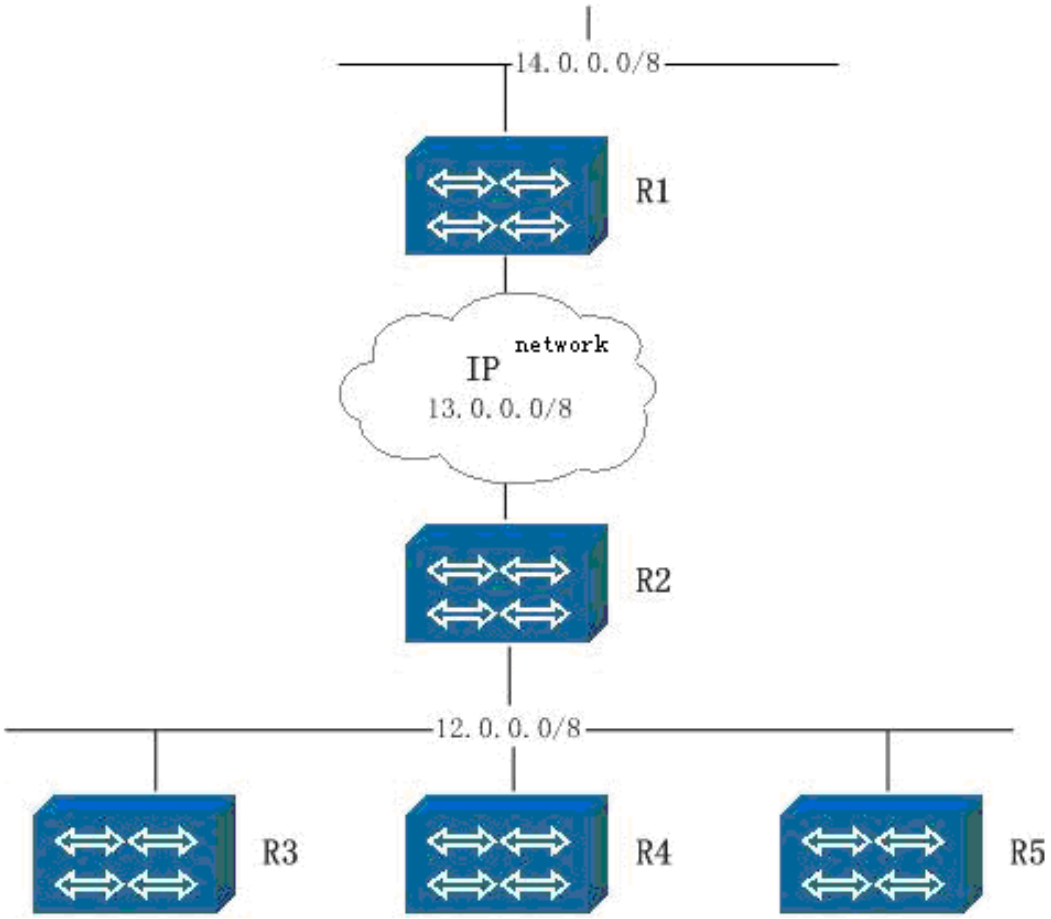
Command	Description
router snsp	Activates SNSP
ndsp run	Runs NDSP

The command NO can be used to prohibit the application of the above command.

In the default situation, the router ignores the received SNSP information.

Use NDSP message to carry the SNSP routing message.

SNSP Configuration Example



The router R2 serves as a hub router. It is configured with SNSP and IRMP routing protocols, and executes NDSP.

The low-end routers, R3, R4 and R5 run NDSP and are configured with the default route without the dynamic route.

IRMP redistributes the SNSP route on the route R2.

The configuration of the Signamax Router R2:

Command	Description
R2#configure terminal	
R2(config)#router snsp	Runs SNSP
R2(config)# ndsp run	Runs NDSP
R2(config)#router irmp 1	
R2(config-irmp)#network 13.0.0.0	
R2(config-irmp)#redistribute snsp	IRMP redistributes SNSP.
R2(config-irmp)#end	

The configuration of the Signamax router R3 (the configuration of R4 or R5 is the same as that of R3)

Command	Description
R3#configure terminal	
R3(config)# ndsp run	Runs NDSP.
R3(config)#ip route 0.0.0.0 0.0.0.0 fastethernet0	Configures the default route.
R3(config)#end	

Load Balance

Signamax routers now supports the routing load balancing, namely, if there exist many routes to a destination, the router will add these routes into the routing table. When the data is transferred, the data load can be transmitted via this interface link in a certain proportion.

Commands

Syntax	Description	Config mode
[no] ip upper-cache	Enable upper routing cache, no is used to disable the cache.	config

Command Supporting Load Balance

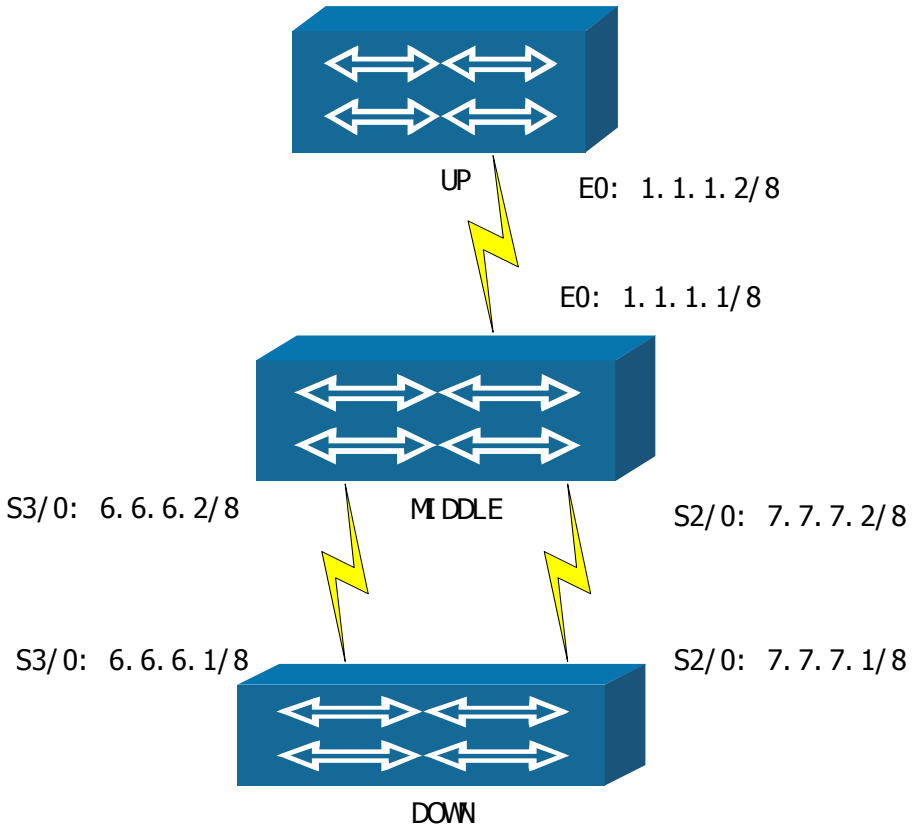
When transmitting data, disable an upper-cache by no ip upper-cache in configuration mode.

```
no ip upper-cache
```

Syntax	Description
upper-cache	Use upper routing cache

(Default status)use upper-cache
(command mode)global configuration mode

Load Balance Configuration Example



The configuration of the Signamax router down:

Syntax	Description
Down#configure terminal	
Down(config)#router ospf 1	
Down(config-ospf)#network 1.0.0.0 0.255.255.255 area 0	
Down(config-ospf)#end	

The configuration of the Signamax router router:

Syntax	Description
Router#configure terminal	
Router(config)#router ospf 1	
Router(config-ospf)#network 1.0.0.0 0.255.255.255 area 0	
Router(config-ospf)#network 6.0.0.0 0.255.255.255 area 0	
Router(config-ospf)#network 7.0.0.0 0.255.255.255 area 0	
Router(config-ospf)#end	

The configuration of the Signamax router up:

Command	Description
Up#configure terminal	
Up(config)#router ospf 1	
Up(config-ospf)#network 6.0.0.0 0.255.255.255 area 0	
Up(config-ospf)#network 7.0.0.0 0.255.255.255 area 0	
Up(config-ospf)#end	

D. Executes the command **show ip route** on the Signamax Router **up:**

```
O    1.0.0.0/8 [110/2] via 6.6.6.2, 11:23:41, serial2
               [110/2] via 7.7.7.2, 11:23:41, serial3
C    6.0.0.0/8 is directly connected, 11:24:27, serial2
C    7.0.0.0/8 is directly connected, 11:24:27, serial3
O    6.6.6.1/32 [110/2] via 6.6.6.2, 11:23:41, serial2
                [110/2] via 7.7.7.2, 11:23:41, serial3
C    6.6.6.2/32 is directly connected, 11:24:27, serial2
O    7.7.7.1/32 [110/2] via 6.6.6.2, 11:23:41, serial2
                [110/2] via 7.7.7.2, 11:23:41, serial3
C    7.7.7.2/32 is directly connected, 11:24:27, serial3
C    11.11.11.11/32 is directly connected, 11:51:54, loopback0
```

Monitoring & Debugging Load Balance

When data is transferred, the extended ping can be used or the debug information of the interface is opened to observe the load balance status.

Command	Description
up#ping Target IP address: 1.1.1.2 Repeat count [5]:2 Datagram size [76]: Timeout in seconds [2]: Extended commands [no]: y Source address or interface: Type of service [0]: Set DF bit in IP header? [no]: Validate reply data? [no]: Data pattern [abcd]: Loose, Strict, Record, Timestamp, Verbose[none]: r Number of hops [9]: Loose, Strict, Record, Timestamp, Verbose[RV]: Sweep range of sizes [no]: Press key (ctrl + shift + 6) interrupt it. Sending 5, 76-byte ICMP Echos to 32.16.3.1 timeout is 2 seconds: Packet has IP options: Total option bytes = 40 . Record route number : 9 Reply to request 0 from 32.16.3.1, size = 76, time = 149 ms. Received packet has options: RR : 1.1.1.1 1.1.1.2 6.6.6.2 6.6.6.1 RR : 1.1.1.1 1.1.1.2 7.7.7.2 7.7.7.1 Success rate is 100% (2/2). Round-trip min/avg/max = 149/154/159 ms.	The interface that packets pass in or out when the packet ping is examined.
Show ip route Net-r	Displays route table. Displays times the router has been used.

Configuring BGP Dynamic Routing Protocol

BGP (Border Gateway Protocol) is distance-vector-based path vector routing protocol. This protocol is used to transfer the route information between autonomous systems. IGP can be used to determine the route in the autonomous system.

BGP uses TCP as the transfer protocol (port number 179). This not only ensures the reliability of all transmission, but also reduces the resource occupied by the protocols. BGP is a factual standard of external routing. This section explains how to configure BGP dynamic routing protocol of Signamax routers for network interconnection.

BGP Configuration Commands

router bgp

Use the command router bgp to enable BGP and enter the BGP protocol configuration mode; or, use the negation of the command to disable BGP.

-

- `router bgp autonomous-system`
- `no router bgp autonomous-system`

Syntax	Description
autonomous-system	Autonomous-system is the local autonomous-system number, and its value range is from 1 to 65535.

(By default) BGP is disabled.

(Command mode)the global configuration mode

(Guide)The command can be used to enable/disable BGP and specify the local autonomous system number.

neighbor remote-as

Use the command neighbor remote-as to specify the autonomous system number of BGP peer/peer group; or, use the negation of the command to delete the autonomous system number of BGP peer/peer group.

- `neighbor {neighbor-address | group-name } remote-as as-number`

- `no neighbor { neighbor-address | group-name } remote-as as-number`

Syntax	Description
neighbor-address	The IP address of the peer.
group-name	The name of the peer group.
as-number	The autonomous-system number of the peer/peer group.

(By default) There exists no BGP peer/peer group.
(Command mode)the BGP protocol configuration mode.

neighbor peer-group(Creating)

Use the command neighbor peer-group(Creating) toe create a peer group; or, use the negation of the command to delete a peer group.

-

- `neighbor group-name peer-group`

- `no neighbor group-name peer-group`

Syntax	Description
group-name	The name of the peer group.

(By default) There exists no peer group.
(Command mode)the BGP protocol configuration mode.

neighbor peer-group(Assigning)

Use the command neighbor peer-group (Assigning) to add a peer to the specified peer group; or, use the negation of the command to delete a peer from the specified peer group.

-

- `neighbor neighbor-address peer-group group-name`

- `no neighbor neighbor-address peer-group group-name`

Syntax	Description
neighbor-address	The IP address of the peer.
group-name	The name of the peer group.

(By default) The command is invalid.
(Command mode)the BGP protocol configuration mode.

neighbor next-hop-self

Use the command neighbor next-hop-self to cancel the action BGP takes for the next hop in the route that need be announced to the peer/peer group; or, use the negation of the command to cancel the existing configuration.

-
- `neighbor {neighbor-address | group-name } next-hop-self`
- `no neighbor {neighbor-address | group-name } next-hop-self`

Syntax	Description
neighbor-address	The IP address of the peer.
group-name	The name of the peer group.

(By default) The command is invalid.
(Command mode)the BGP protocol configuration mode.

neighbor password

Use the command neighbor password to configure MD5 authentication of the TCP connection between two BGP peers; or, use the negation of the command to cancel the configuration.

•

• `neighbor {neighbor-address | group-name } password string`

• `no neighbor {neighbor-address | group-name } password string`

Syntax	Description
neighbor-address	The IP address of the peer.
group-name	The name of the peer group.
String	MD5 password.

(By default) There exists no MD5 authentication.
(Command mode)the BGP protocol configuration mode.

neighbor advertisement-interval

Use the command neighbor advertisement-interval to configure the interval for the peer/peer group to send route information; or, use the negation of the command to restore the default interval for the peer/peer group to send route information.

•

• `neighbor {neighbor-address | group-name } advertisement-interval seconds`

• `no neighbor {neighbor-address | group-name } advertisement-interval seconds`

Syntax	Description
neighbor-address	The IP address of the peer.
group-name	The name of the peer group.
seconds	The minimal interval of sending Update message. Its value range is from 0 to 600 seconds.

(Command mode)the BGP protocol configuration mode.

neighbor route-map

Use the command neighbor route-map to configure the route-map of the peer/peer group; or, use the negation of the command to delete the route-map of the peer/peer group.

-

- `neighbor {neighbor-address | group-name } route-map map-name {in | out }`

- `no neighbor {neighbor-address | group-name } route-map map-name {in | out }`

Syntax	Description
neighbor-address	The IP address of the peer.
group-name	The name of the peer group.
map-name	The name of the route-map
In	Input the announcement.`
Out	Output the announcement.

(By default) The command is invalid.
(Command mode)the BGP protocol configuration mode.

neighbor route-reflector-client

Use the command neighbor route-reflector-client to configure the peer/peer group as CLIent of the route reflector; or, use the negation of the command to cancel the existing configuration.

-

- `neighbor {neighbor-address | group-name } route-reflector-client`

- `no neighbor {neighbor-address | group-name } route-reflector-client`

-

Syntax	Description
neighbor-address	The IP address of the peer.
group-name	The name of the peer group.

(By default) The command is invalid.
(Command mode)the BGP protocol configuration mode.

neighbor send-community

Use the command neighbor send-community to send the community properties to the peer/peer group; or, use the negation of the command to cancel the existing configuration.

-
- `neighbor {neighbor-address | group-name } send-community`
- `no neighbor {neighbor-address | group-name } send-community`

Syntax	Description
neighbor-address	The IP address of the peer.
group-name	The name of the peer group.

(By default) No community property is sent.
(Command mode)the BGP protocol configuration mode.

neighbor timers

Use the command neighbor timers to configure the Holdtime of the specified peer/peer group; or, use the negation of the command to cancel the existing configuration.

•

• `neighbor {neighbor-address | group-name } timers holdtime-interval`

• `no neighbor {neighbor-address | group-name } timers`

Syntax	Description
neighbor-address	The IP address of the peer.
group-name	The name of the peer group.
holdtime-interval	The specified holdtime interval.

(By default) The default keepalive is 60 seconds and default holdtime interval is 180 seconds.
(Command mode)the BGP protocol configuration mode.

neighbor ebgp-multihop

Use the command neighbor ebgp-multihop to allow establishing the connection with the EBGP peer/peer group that are not connected directly with the network; or, use the negation of the command to cancel the existing configuration.

•

• `neighbor {neighbor-address | group-name } ebgp-multihop ttl`

• `no neighbor {neighbor-address | group-name } ebgp-multihop`

Syntax	Description
neighbor-address	The IP address of the peer.

group-name	The name of the peer group.
Ttl	The maximal number of hops. Its value range is from 1 to 255.

(Command mode)the BGP protocol configuration mode.

neighbor update-source

Use the command neighbor update-source to allow internal BGP to use any operational TCP to connect with an interface; or, use the negation of the command to cancel the existing configuration.

-

- `neighbor {neighbor-address | group-name } update-source interface`

- `no neighbor {neighbor-address | group-name } update-source interface`

Syntax	Description
neighbor-address	The IP address of the peer
group-name	The name of the peer group.
interface	Specify the interface for TCP connection.

(By default) The local interface.
(Command mode)the BGP protocol configuration mode.

neighbor distribute-list

Use the command neighbor distribute-list to configure the access list of the peer/peer group; or, use the negation of the command to cancel the configuration.

-

- `neighbor {neighbor-address | group-name } distribute-list access-list-number {in | out}`

- `no neighbor {neighbor-address | group-name } distribute-list access-list-number {in | out}`

Syntax	Description
neighbor-address	The IP address of the peer.
group-name	The name of the peer group.
access-list-name	The name of the access list. Its range is from 1 to 1000.
In	Input the announcement.
Out	Output the announcement.

(By default) The command is invalid.
(Command mode)the BGP protocol configuration mode.

neighbor filter-list

Use the command neighbor filter-list to configure the filtering list of the peer/peer group; or, use the negation of the command to cancel the configuration.

-
- `neighbor {neighbor-address | group-name } filter-list aspath-list-number {in | out}`
- `no neighbor {neighbor-address | group-name } filter-list access-list-number {in | out}`
-

Syntax	Description
neighbor-address	The IP address of the peer.
group-name	The name of the peer group.
aspath-list-name	AS regular expression list number. Its value range is from 1 to 199.
In	Input the announcement.
Out	Output the announcement.

(By default) The command is invalid.
(Command mode)the BGP protocol configuration mode.

neighbor prefix-list

configure peer prefix filter list, and no is used to cancel the configuration.

-
- `neighbor neighbor-address prefix-list prefix-list-name {in | out}`
- `no neighbor neighbor-address prefix-list prefixs-list-name {in | out}`

Syntax	Description
neighbor-address	Peer IP address.
prefixs-list-name	Prefix list name.
in	Use for in routing.
out	Use for out routing

(By default) invalid.
(command mode)BGP protocol configuration mode

neighbor version
Use the command neighbor version to configure the special BGP version for receiving; or, use the negation of the command to use the default version.

- `neighbor {neighbor-address | group-name } version value`
- `no neighbor {neighbor-address | group-name } version value`

Syntax	Description
neighbor-address	The IP address of the peer.
group-name	The name of the peer group.

value	The BGP version number.

(Command mode)the BGP protocol configuration mode.

neighbor shutdown

Use the command neighbor shutdown to close the connection with the specified neighbor; or, use the negation of the command to open the connection with the specified neighbor.

- `neighbor {neighbor-address | peer_group-name } shutdown`
- `no neighbor {neighbor-address | peer_group-name } shutdown`

Syntax	Description
neighbor-address	The IP address of the peer.
Peer_group-name	The name of the peer group

(Command mode)the BGP protocol configuration mode.

neighbor soft-reconfiguration inbound

Use the command neighbor soft-reconfiguration inbound to save the received corrected value; or, use the negation of the command not to save the received corrected value.

- `neighbor {neighbor-address | peer_group-name } soft-reconfiguration inbound`
- `no neighbor {neighbor-address | peer_group-name } soft-reconfiguration inbound`
-

Syntax	Description
neighbor-address	The IP address of the peer.
Peer_group-name	The name of the peer group.

(Command mode)the BGP protocol configuration mode.

neighbor activate

configure neighbor activation in address cluster, and no is used to disable the function.

-
- `neighbor neighbor-address activate`
- `no neighbor neighbor-address activate`

Syntax	Description

neighbor-address	Peer IP address

(Default status)activate in global address cluster by default, other conditions will not.
(command mode)BGP protocol configuration mode

Configure neighbor description, and no is used to cancel the content.

-
- `neighbor neighbor-address description string`
- `no neighbor neighbor-address description`

Syntax	Description
neighbor-address	Peer IP address
string	Description content, max 80 characters.

(Default status)empty by default
(command mode)BGP protocol configuration mode ◦

neighbor maximum-prefix

Configure max routing prefix number from neighbor, and no is used to cancel the configuration.

•

• `neighbor neighbor-address maximum-prefix prefix_num [Threshold_vlaue] [warning-only]`

• `no neighbor neighbor-address maximum-prefix prefix_num`

Syntax	Description
neighbor-address	Peer IP address
prefix_num	Max prefix number
Threshold_vlaue	Threshold value
warning-only	Whether executing warning.

(Default status)no prefix number limitation
(command mode)BGP protocol configuration mode

neighbor remove-private-AS

This command is used for filtering AS number from AS_PATH before advertising it to neighbor, and no is used to cancel the configuration.

•

• `neighbor neighbor-address remove-private-AS`

• `no neighbor neighbor-address remove-private-AS`

•

Syntax	Description
neighbor-address	Peer IP address

(Default status)no filter by default.
(command mode)BGP protocol configuration mode

bgp always-compare-med

Use the command bgp always-compare-med to allow comparing the MED value of route paths from different AS neighbors; or, use the negation of the command to forbid the comparison.

-
- `bgp always-compare-med`
- `no bgp always-compare-med`

(By default) There exists no comparison.
(Command mode)the BGP protocol configuration mode.

bgp cluster-id

Use the command bgp cluster-id to configure the cluster ID of the route reflector; or, use the negation of the command to delete the cluster ID of the route reflector.

-
- `bgp cluster-id cluster-id`
- `no bgp cluster-id cluster-id`

Syntax	Description
cluster-id	The router ID of a single route reflector in the cluster.

(Command mode)the BGP protocol configuration mode.

bgp router-id

Use the command bgp router-id to configure the router-id of the router; or, use the negation of the command to disable the router-id of the router.

-
- `bgp router-id router-id`
- `no bgp router-id router-id`

Syntax	Description
router-id	The router-id of the router.

(Command mode)the BGP protocol configuration mode.

bgp confederation identifier

Use the command bgp confederation identifier to configure the bgp confederation identifier; or, use the negation of the command to remove the bgp confederation identifier.

-
- `bgp confederation identifier as-number`
- `no bgp confederation identifier as-number`

Syntax	Description
as-number	The autonomous system number.

(Command mode)the BGP protocol configuration mode.

bgp confederation peers

Use the command bgp confederation peers to configure the autonomous system belonging to the bgp confederation; or, use the negation of the command to remove the autonomous system from the bgp confederation.

- `bgp confederation peers as-number`
- `no bgp confederation peers as-number`

Syntax	Description
as-number	The autonomous system number.

(Command mode)the BGP protocol configuration mode.

bgp default local-preference

Use the command bgp default local-preference to configure the local preference; or, use the negation of the command to restore the default value of the local preference.

-
- `bgp default local-preference value`
- `no bgp default local-preference value`

Syntax	Description
value	The local preference. Its value range is from 0 to 4294967295.

(By default) The default value of local preference is 100.

(Command mode)the BGP protocol configuration mode.

bgp dampening

Use the command bgp dampening to configure BGP route dampening and other parameters; or, use the negation of the command to cancel the route dampening.

-
- `bgp dampening [half-life reuse suppress max-suppress-time]`
- `no bgp dampening [half-life reuse suppress max-suppress-time]`

Syntax	Description
half-life	The half-life of the BGP route dampening. Its value range is from 1 to 45.
reuse	The route reuse limit. Its value range is from 1 to 20000.
Suppress	The route suppression limit. Its value range is from 1 to 20000.
max-suppress-time	the maximal suppression time. Its value range is from 1 to 255.

(By default) half-life : 15 minutes; reuse :750; suppress: 2000; max-suppress-time: four times of half-life.
(Command mode)the BGP protocol configuration mode.
bgp updatert-timer

-
- `enable routing updating timer, and no is used to disable the timer.`
- `bgp updatert-timer`
- `no bgp updatert-timer`

(Default status)not enable routing update timer.
(command mode)BGP protocol configuration mode.

address-family

activate and enter address cluster for configuration, and no is used to cancel the configuration.

-
- `address-family {vpnv4 | ipv4 vrf vrfname}`
- `no address-family`

Syntax	Description

vpnv4	vpnv4 address cluster
Ipv4	ipv4 address cluster.
Vrf	Vrf address cluster
vrfname	Designate vrf name

(Default status)configure in global address cluster.
(command mode)BGP protocol configuration mode

network

Use the command network to configure the network to which BGP is sent; or, use the negation of the command to cancel the existing configuration.

•

• `network network-number [mask network-mask] [route-map map-name]`

• `no network network-number [mask network-mask] [route-map map-name]`

Syntax	Description
network-number	The network BGP need announce.
mask	The network mask.
network-mask	The network mask BGP need announce.
route-map	The route map.
map-name	The name of the route map.

(By default) BGP sends no route.
(Command mode)the BGP protocol configuration mode.

redistribute

Use the command redistribute to introduce the route information of other protocols; or, use the negation of the command to cancel the introduction of the route information of other protocols.

•

• `redistribute protocol [route-map map-name]`

• `no redistribute protocol [route-map map-name]`

Syntax	Description
protocol	Specify the original route protocol that can be introduced: connected, rip, irmp, ospf, snsp, static.
route-map	route map
map-name	name of the route map.

(By default) BGP does not introduces routes of other protocols.
(Command mode)the BGP protocol configuration mode.

synchronization

Use the command synchronization to configure the synchronization between BGP and IGP; or, use the negation of the command to disable the synchronization between BGP and IGP.

-
- `synchronization`
- `no synchronization`

(By default) BGP is synchronous with IGP.
(Command mode)the BGP protocol configuration mode.

maximum-paths

Use the command maximum-paths to configure BGP to support load balance; or, use the negation of the command to close BGP load balance

-
- `maximum-paths number-paths`
- `no maximum-paths`

Syntax	Description
number-paths	The maximal number of the paths of load balance supported by BGP. Its value range is from 1 to 6.

(By default) BGP does not support load balance.
(Command mode)the BGP protocol configuration mode.

distance bgp

Use the command distance bgp to configure the management distance of external BGP and internal BGP; or, use the negation of the command to

restore the default management distance of external BGP and internal BGP distance bgp external-distance internal-distance

-
- `no distance bgp`

Syntax	Description
external-distance	The management distance of BGP external route. Its value range is from 1 to 255.
internal-distance	The management distance of BGP internal route. Its value range is from 1 to 255.

(By default) The management distance of BGP external route is 20, and the management distance of BGP internal route is 200.

(Command mode)the BGP protocol configuration mode.

default-metric

Use the command default-metric to configure the MED value introduced into other protocols; or, use the negation of the command to cancel the configuration.

-
- `default-metric number`
- `no default-metric number`

Syntax	Description
number	The MED value. Its value range is from 1 to 65535.

(Command mode)the BGP protocol configuration mode.

aggregate-address

Use the command aggregate-address to create an aggregation address in the BGP routing table; or, use the negation of the command to make the command invalid.

-
- `aggregate-address address mask [as-set] [summary-only]`
- `no aggregate-address address mask [as-set] [summary-only]`

Syntax	Description
address	address of the aggregation route
mask	The network mask of the aggregation route.

as-set	Generate a route of AS aggregation segment.
summary-only	Only aggregation routes are announced.

(By default) The command is invalid.
(Command mode)the BGP protocol configuration mode.

match as-path

Use the command match as-path to specify a matched path access list in the route map; or, use the negation of the command to cancel the configuration.

•

• `match as-path path-list-number`

• `no match as-path path-list-number`

Syntax	Description
path-list-number	The path access list number. Its value range is from 1 to 199.

(Command mode)the route map configuration mode.
match ip address

Use the command match ip address to specify the matched IP address range in the route map.

•

• `match ip address access-list-number`

• `no match ip address access-list-number`

Syntax	Description
access-list-number	access list number.

(Command mode)the route map configuration mode.

match ip next-hop

Use the command match ip next-hop to specify the next matched IP address in route map; or, use the negation of the command to cancel the configuration.

•

• `match ip next-hop access-list-name`

• `no match ip next-hop access-list-name`

Syntax	Description
access-list-number	access list number

(Command mode)the route map configuration mode.

set as-path

Use the command set as-path to add an AS number before the original AS path in the route map; or, use the negation of the command to cancel the configuration.

-
- `set as-path [prepend as-path-string]`
- `no set as-path [prepend as-path-string]`

Syntax	Description
prepend	Add an AS number.
as-path-string	The AS number.

(Command mode)the route map configuration mode.

set community

Use the command set community to configure BGP community property in route map; or, use the negation of the command to cancel the configuration.

-
- `set community {additive | local-AS | no-advertise | no-export | none}`
- `no set community {additive | local-AS | no-advertise | no-export | none}`

Syntax	Description
additive	Add the community property to the existing community.
local-AS	Do not send the matched route out of the autonomous system.
No-advertise	Do not advertise the matched route to any peer/peer group.
No-export	Do not advertise the route with the property to any peer/peer group out of the autonomous system except any peer/peer group in the autonomous system.
none	Delete the community property of the route.

(Command mode)the route map configuration mode.

set ip next-hop

Use the command set ip next-hop to specify the next hop for the alteration of the original route in the route map; or, use the negation of the command to cancel the configuration.

-
- `set ip next-hop ip-address`
- `no set ip next-hop ip-address`

Syntax	Description
ipt-address	Set the IP address of the next hop

(Command mode)the route map configuration mode.

set local-preference

Use the command set local-preference to change the local preference of the original route for the route map; or, use the negation of the command to cancel the configuration of the local preference of the original route.
set local-preference value

-

- `no set local-preference value`

Syntax	Description
value	Set the local preference.

(Command mode)the route map configuration mode.

set metric

Use the command set metric to change the property metric of the original route in the route map; or, use the negation of the command to cancel the configuration.

- `set metric metric`

- `no set metric metric`

Syntax	Description
metric	Set the property metric.

(Command mode)the route map configuration mode.

set origin

Use the command set origin to change the property origin of the original route in the route map; or, use the negation of the command to cancel the configuration.

-

- `set origin {egp | igp | incomplete}`

- `no set origin`

Syntax	Description
Egp, igp, incomplete	Set the property origin

(Command mode)the route map configuration mode.

clear ip bgp

Use the command clear ip bgp to reset the BGP connection and make the configured-newly policy valid after the configuration of route policy or BGP has been changed.

-

- `clear ip bgp {* | address | as-number}`

Syntax	Description
*	All peers
address	The IP address of the specified peer.
as-number	Reset the BGP connection matching with the AS number. The value range of AS number is from 1 to 65535.

(Command mode)The privileged user configuration mode.

clear ip bgp dampening

Use the command clear ip bgp dampening to clear information about route flap dampening and remove the restraint of the restrained routes.

-
- `clear ip bgp dampening {address | mask }`

Syntax	Description
address	The network IP address used to clear the dampening information.
mask	The network mask.

(Command mode)The privileged user configuration mode.

clear ip bgp flap-statistic

Clear routing flap statistics information.

-
- `clear ip bgp flap-statistic { network-number | mask }`

Syntax	Description
address	Network IP address about clearing flap information
mask	Network mask

(command mode)privileged user configuration mode

clear ip bgp vpnv4 vrf

Clear vrf BGP information, and reconnect.

-
- `clear ip bgp vpnv4 vrf  vrfname {* | address | as-number}`

Syntax	Description
vrfname	Designate vrf name
*	All peer
address	Special peer ip address
as-number	AS number BGP connection, and the range is 1 ~ 65535.

(command mode)privileged user configuration mode

clear ip bgp peer-group

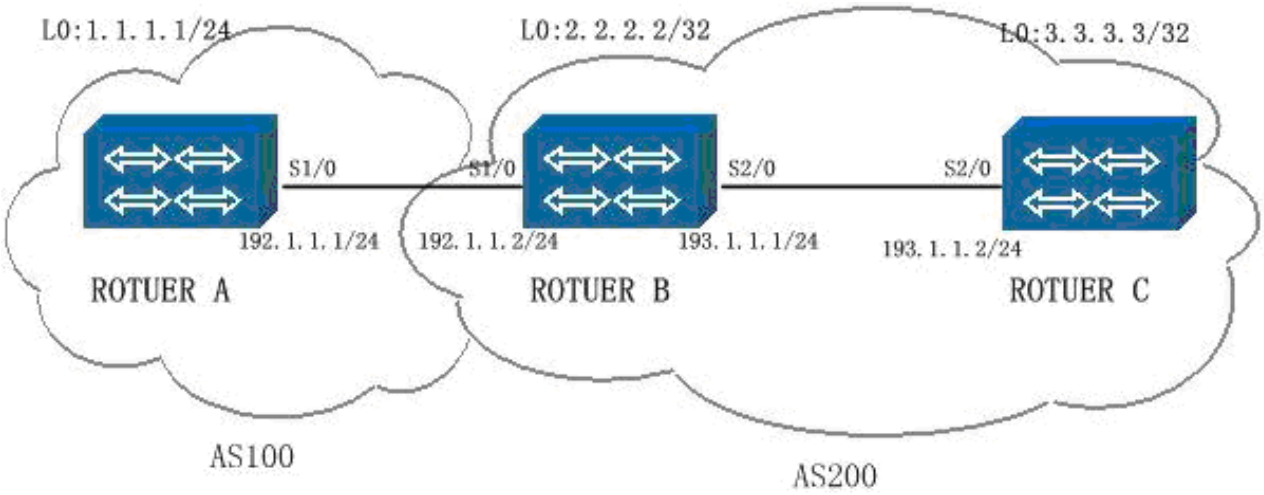
Use the command clear ip bgp peer-group to reset all BGP connections of the specified peer group.

-
- `clear ip bgp peer-group group-name`

Syntax	Description
Group-name	The name of the peer group.

(Command mode)The privileged user configuration mode.

BGP Configuration Examples



The port S1/0(192.1.1.1) of RouterA connects to the port S1/0 (192.1.1.2) of RouterB; the port S2/0(193.1.1.1) of RouterB connects to the port S2/0 (193.1.1.2) of RouterC;

The loopback addresses of three routers are 1.1.1.1(RouterA), 2.2.2.2(RouterB) and 3.3.3.3(RouterC).

RouterA is located in AS 100, while RouterB and RouterC are located in AS 200.

RouterA is configured as follows:

Command	Description
RouterA#configure terminal	Enter the global configuration mode.
RouterA(config)#interface loopback0	Enter the loopback interface.
RouterA(config-if-loopback0)#ip address 1.1.1.1 255.255.255.0	Configure the IP address.
RouterA(config-if-loopback0)#interface s1/0	Enter the interface s1/0.
RouterA(config-if-serial1/0)#encapsulation hdlc	Encapsulate the link-layer protocol HDLC.
RouterA(config-if-serial1/0)#ip address 192.1.1.1 255.255.255.0	Configure the IP address.
RouterA(config-if-serial1/0)#exit	
RouterA(config)#router bgp 100	Enter the BGP configuration mode.
RouterA(config-bgp)#neighbor 192.1.1.2 remote-as 200	Specify the AS number of the BGP peer.
RouterA(config-bgp)#network 1.1.1.0 mask 255.255.255.0	Configure the network to which the BGP is sent.
RouterA(config-bgp)#exit	

RouterB is configured as follows:

Command	Description
RouterB#configure terminal	Enter the global configuration mode.
RouterB(config)#interface loopback0	Enter the loopback interface.
RouterB(config-if-loopback0)#ip address 2.2.2.2 255.255.255.255	Configure the IP address.
RouterB(config-if-loopback0)#interface s1/0	Enter the configuration interface s1/0.
RouterB(config-if-serial1/0)#encapsulation hdlc	Encapsulate the link-layer protocol HDLC.
RouterB(config-if-serial1/0)#ip address 192.1.1.2 255.255.255.0	
RouterB(config-if-serial1/0)#clock rate 9600	Configure clock rate.
RouterB(config-if-serial1/0)#interface s2/0	
RouterB(config-if-serial2/0)#encapsulation hdlc	Encapsulate the link-layer protocol HDLC.
RouterB(config-if-serial2/0)#ip address 193.1.1.1 255.255.255.0	
RouterB(config-if-serial2/0)#clock rate 9600	
RouterB(config-if-serial2/0)#exit	
RouterB(config)#router bgp 200	Enter the BGP configuration mode.

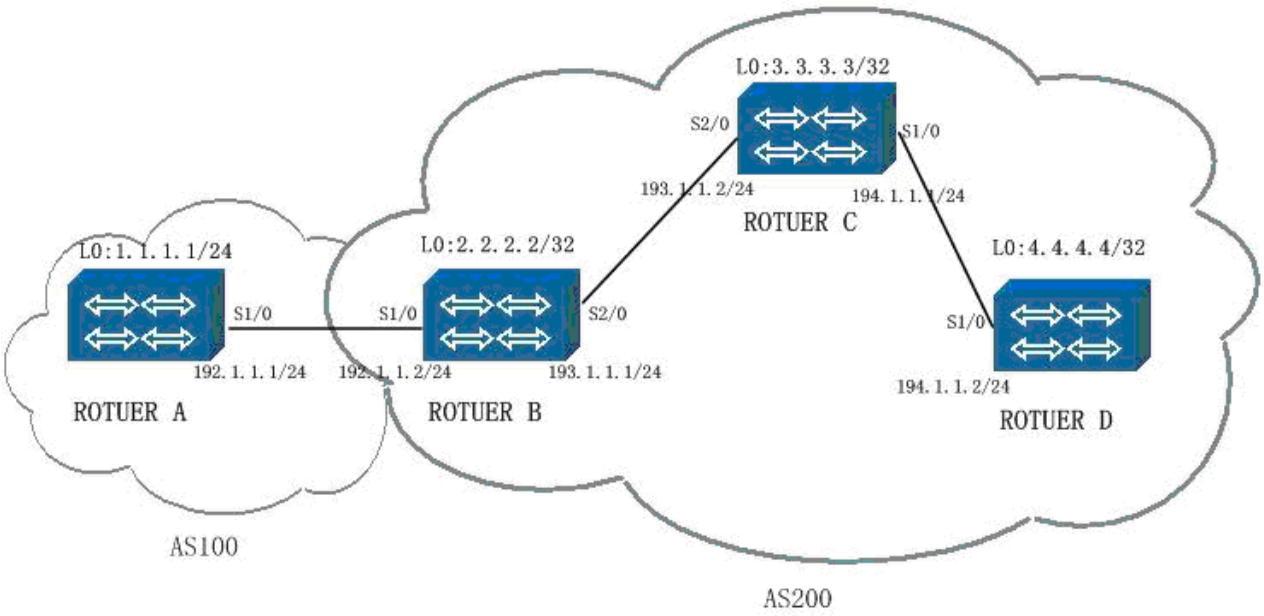
RouterB(config-bgp)#neighbor 192.1.1.1 remote-as 100	Specify the AS number of the BGP peer.
RouterB(config-bgp)#neighbor 193.1.1.2 remote-as 200	The same as the above.
RouterB(config-bgp)#neighbor 193.1.1.2 next-hop-self	Regard its own address as the next hop.
RouterB(config-bgp)#exit	

RouterC is configured as follows:

Command	Description
RouterC#configure terminal	Enter the global configuration mode.
RouterC(config)#interface loopback0	
RouterC(config-if-loopback0)#ip address 3.3.3.3 255.255.255.255	
RouterC(config-if-loopback0)#interface s2/0	
RouterC(config-if-serial2/0)#encapsulation hdlc	Encapsulate the link-layer protocol HDLC.
RouterC(config-if-serial2/0)#ip address 193.1.1.2 255.255.255.0	
RouterC(config-if-serial2/0)#exit	
RouterC(config)#router bgp 200	Enter the BGP configuration mode.
RouterC(config-bgp)#neighbor 193.1.1.1 remote-as 200	Specify the AS number of the BGP peer.
RouterC(config-bgp)#no synchronization	Set the asynchronic between BGP and IGP.
RouterC(config-bgp)#exit	

The above explains the dynamic routing protocol BGP. About the configuration mode of the physical layer and link layer, refer to related sections.

Configuring BGP route reflector



As shown in the figure above, the configuration of RouterA, RouterB and RouterC is the same as that of example 1. RouterD is an additional router, belonging to AS 200, its interface s1/0 connects with the interface s1/0 of RouterC, and their related addresses are 194.1.1.1(RouterC) and 194.1.1.2(RouterD).

In the example above, RouterC acts as a reflector and supports two clients: RouterB and RouterC.

RouterA is located in AS 100, while RouterB, RouterC and RouterD is located in AS 200.

RouterA is configured as follows:

Syntax	Description
RouterA#configure terminal	Enter the global configuration mode.
RouterA(config)#interface loopback0	
RouterA(config-if-loopback0)#ip address 1.1.1.1 255.255.255.0	
RouterA(config-if-loopback0)#interface s1/0	Enter the interface s1/0.
RouterA(config-if-serial1/0)#encapsulation hdlc	Encapsulate the link-layer protocol HDLC.
RouterA(config-if-serial1/0)#ip address 192.1.1.1 255.255.255.0	
RouterA(config-if-serial1/0)#exit	
RouterA(config)#router bgp 100	Enter the BGP configuration mode.
RouterA(config-bgp)#neighbor 192.1.1.2 remote-as 200	Specify the autonomous system number of the BGP peer.
RouterA(config-bgp)#network 1.1.1.0 mask	Configure the network to which

255.255.255.0	the BGP is sent.
RouterA(config-bgp)#exit	

RouterB is configured as follows:

Syntax	Description
RouterB#configure terminal	Enter the global configuration mode.
RouterB(config)#interface loopback0	
RouterB(config-if-loopback0)#ip address 2.2.2.2 255.255.255.255	
RouterB(config-if-loopback0)#interface s1/0	
RouterB(config-if-serial1/0)#encapsulation hdlc	Encapsulate the link-layer protocol HDLC.
RouterB(config-if-serial1/0)#ip address 192.1.1.2 255.255.255.0	
RouterB(config-if-serial1/0)#clock rate 9600	
RouterB(config-if-serial1/0)#interface s2/0	
RouterB(config-if-serial2/0)#encapsulation hdlc	Encapsulate the link-layer protocol HDLC.
RouterB(config-if-serial2/0)#ip address 193.1.1.1 255.255.255.0	
RouterB(config-if-serial2/0)#clock rate 9600	
RouterB(config-if-serial2/0)#exit	
RouterB(config)#router rip	Enter the RIP configuration mode.
RouterB(config-rip)#network 193.1.1.0	
RouterB(config-rip)#version 2	
RouterB(config-rip)#exit	
RouterB(config)#router bgp 200	Enter the BGP configuration mode.
RouterB(config-bgp)#neighbor 192.1.1.1 remote-as 100	Specify the autonomous system number of the BGP peer.
RouterB(config-bgp)#neighbor 193.1.1.2 remote-as 200	The same as above.
RouterB(config-bgp)#neighbor 193.1.1.2 next-hop-self	Regard its own address as the next hop.
RouterB(config-bgp)#exit	

RouterC is configured as follows:

Syntax	Description
RouterC#configure terminal	Enter the global configuration

	mode.
RouterC(config)#interface loopback0	
RouterC(config-if-loopback0)#ip address 3.3.3.3 255.255.255.255	
RouterC(config-if-loopback0)#interface s1/0	
RouterC(config-if-serial1/0)#encapsulation hdlc	Encapsulate the link-layer protocol HDLC.
RouterC(config-if-serial1/0)#ip address 194.1.1.1 255.255.255.0	
RouterC(config-if-serial1/0)#interface s2/0	
RouterC(config-if-serial2/0)#encapsulation hdlc	Encapsulate the link-layer protocol HDLC.
RouterC(config-if-serial2/0)#ip address 193.1.1.2 255.255.255.0	
RouterC(config-if-serial2/0)#exit	
RouterC(config)#router rip	Enter the RIP configuration mode.
RouterC(config-rip)#network 193.1.1.0	
RouterC(config-rip)#network 194.1.1.0	
RouterC(config-rip)#version 2	
RouterC(config-rip)#exit	
RouterC(config)#router bgp 200	Enter the BGP configuration mode.
RouterC(config-bgp)#neighbor 193.1.1.1 remote-as 200	
RouterC(config-bgp)#neighbor 194.1.1.2 remote-as 200	
RouterC(config-bgp)#neighbor 193.1.1.1 route-reflector-client	Configure the peer as CLIent of the route reflector.
RouterC(config-bgp)#neighbor 194.1.1.2 route-reflector-client	Configure the peer as CLIent of the route reflector.
RouterC(config-bgp)#no synchronization	Set the asynchronic between BGP and IGP.
RouterC(config-bgp)#exit	

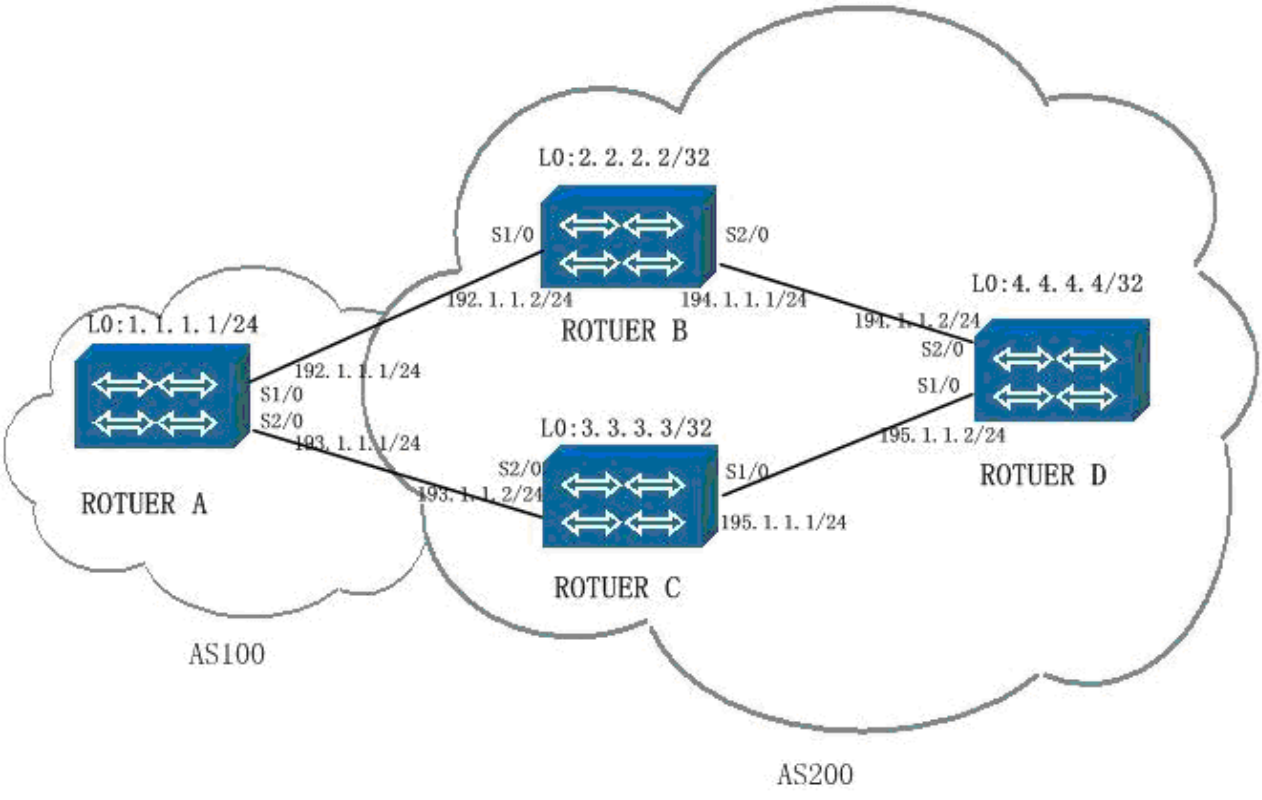
RouterD is configured as follows:

Syntax	Description
RouterD#configure terminal	Enter the global configuration mode.
RouterD(config)#interface s1/0	
RouterD(config-if-serial1/0)#encapsulation hdlc	Encapsulate the link-layer protocol HDLC.
RouterD(config-if-serial1/0)#ip address 194.1.1.2 255.255.255.0	
RouterD(config-if-serial1/0)#clock rate 9600	

RouterD(config-if-serial1/0)#exit	
RouterD(config)#router rip	Enter the RIP configuration mode.
RouterD(config-rip)#network 194.1.1.0	
RouterD(config-rip)#version 2	
RouterD(config-rip)#exit	
RouterD(config)#router bgp 200	Enter the BGP configuration mode.
RouterD(config-bgp)#neighbor 194.1.1.1 remote-as 200	Specify the autonomous system number of the BGP peer.
RouterD(config-bgp)#no synchronization	Set the asynchronic between BGP and IGP.
RouterD(config-bgp)#exit	

The above explains the dynamic routing protocol BGP. About the configuration mode of the physical layer and link layer, refer to related sections.

Example 3: Configuring BGP Routing



RouterA, RouterB, RouterC and RouterD are connected as shown in the figure above. Configure the command route-map on RouterC and set the local-preference of the router so that the route information matching the access list (1.1.1.0/24) can be transmitted over the path with higher local-preference.

RouterA is located in AS 100, while RouterB, RouterC and RouterD are located in AS 200.

RouterA is configured as follows:

Syntax	Description
RouterA#configure terminal	Enter the global configuration mode.
RouterA(config)#interface loopback0	
RouterA(config-if-loopback0)#ip address 1.1.1.1 255.255.255.0	
RouterA(config-if-loopback0)#interface loopback1	
RouterA(config-if-loopback1)#ip address 2.2.2.2 255.255.255.0	
RouterA(config-if-loopback1)#interface s1/0	Enter the interface s1/0.
RouterA(config-if-serial1/0)#encapsulation hdlc	Encapsulate the link-layer protocol HDLC.
RouterA(config-if-serial1/0)#ip address 192.1.1.1 255.255.255.0	
RouterA(config-if-serial1/0)#interface s2/0	
RouterA(config-if-serial2/0)#encapsulation hdlc	
RouterA(config-if-serial2/0)#ip address 193.1.1.1 255.255.255.0	
RouterA(config-if-serial2/0)#exit	
RouterA(config)#router bgp 100	Enter the BGP configuration mode.
RouterA(config-bgp)#network 1.1.1.0 mask 255.255.255.0	Configure the network to which the BGP is sent.
RouterA(config-bgp)#network 2.2.2.0 mask 255.255.255.0	The same as above.
RouterA(config-bgp)#neighbor 192.1.1.2 remote-as 200	Specify the autonomous system number of the BGP peer.
RouterA(config-bgp)#neighbor 193.1.1.2 remote-as 200	The same as above.
RouterA(config-bgp)#exit	

RouterB is configured as follows:

Syntax	Description
RouterB#configure terminal	Enter the global configuration mode.
RouterB(config)#interface serial1/0	
RouterB(config-if-serial1/0)#encapsulation hdlc	Encapsulate the link-layer protocol HDLC.

RouterB(config-if-serial1/0)#ip address 192.1.1.2 255.255.255.0	
RouterB(config-if-serial1/0)#clock rate 9600	
RouterB(config-if-serial1/0)#interface s2/0	
RouterB(config-if-serial2/0)#encapsulation hdlc	Encapsulate the link-layer protocol HDLC.
RouterB(config-if-serial2/0)#ip address 194.1.1.2 255.255.255.0	
RouterB(config-if-serial2/0)#clock rate 9600	
RouterB(config-if-serial2/0)#exit	
RouterB(config)#router bgp 200	Enter the BGP configuration mode.
RouterB(config-bgp)#neighbor 192.1.1.1 remote-as 100	Specify the autonomous system number of the BGP peer.
RouterB(config-bgp)#neighbor 194.1.1.1 remote-as 200	The same as above.
RouterB(config-bgp)#neighbor 195.1.1.2 remote-as 200	The same as above.
RouterB(config-bgp)#neighbor 194.1.1.1 next-hop-self	Regard its own address as the next hop.
RouterB(config-bgp)#exit	

RouterC is configured as follows:

Syntax	Description
RouterC#configure terminal	Enter the global configuration mode.
RouterC(config)#interface serial1/0	
RouterC(config-if-serial1/0)#encapsulation hdlc	Encapsulate the link-layer protocol HDLC.
RouterC(config-if-serial1/0)# ip address 195.1.1.2 255.255.255.0	
RouterC(config-if-serial1/0)#clock rate 9600	
RouterC(config-if-serial1/0)#interface s2/0	
RouterC(config-if-serial2/0)#encapsulation hdlc	Encapsulate the link-layer protocol HDLC.
RouterC(config-if-serial2/0)#ip address 193.1.1.2 255.255.255.0	
RouterC(config-if-serial2/0)#clock rate 9600	
RouterC(config-if-serial2/0)#exit	
RouterC(config)#ip access-list standard 1	Set the access list.
RouterC(config-std-nacl)#permit 1.1.1.0 0.0.0.255	
RouterC(config-std-nacl)#exit	
RouterC(config)# route-map localpref permit 10	Set the route map.
RouterC(config-route-map)# match ip address 1	
RouterC(config-route-map)#set local-preference 200	Set the local preference.
RouterC(config-route-map)#exit	
RouterC(config)# route-map localpref permit 20	Set the route map.
RouterC(config-route-map)#set local-preference 100	Set the local preference.
RouterC(config-route-map)#exit	
RouterC(config)#router bgp 200	Enter the BGP configuration mode.
RouterC(config-bgp)#neighbor 193.1.1.1 remote-as 100	Specify the autonomous system number of the BGP peer.
RouterC(config-bgp)#neighbor 194.1.1.2 remote-as 200	The same as above.
RouterC(config-bgp)#neighbor 195.1.1.1 remote-as 200	The same as above.
RouterC(config-bgp)#neighbor 195.1.1.1 next-hop-self	Regard its own address as the next hop.
RouterC(config-bgp)#neighbor 193.1.1.1 route-map localpref in	Apply localpref to ingress traffic of the neighbor 193.1.1.1.
RouterC(config-bgp)#exit	

RouterD is configured as follows:

Syntax	Description
RouterD#configure terminal	Enter the global configuration mode.
RouterD(config)#interface loopback0	
RouterD(config-if-loopback0)#ip address 4.4.4.4 255.255.255.0	
RouterD(config-if-loopback0)#interface s1/0	
RouterD(config-if-serial1/0)#encapsulation hdlc	Encapsulate the link-layer protocol HDLC.
RouterD(config-if-serial1/0)#ip address 195.1.1.1 255.255.255.0	
RouterD(config-if- serial1/0)#interface s2/0	
RouterD(config-if-serial2/0)#encapsulation hdlc	Encapsulate the link-layer protocol HDLC.
RouterD(config-if-serial2/0)#ip address 194.1.1.1 255.255.255.0	
RouterD(config-if-serial2/0)#exit	
RouterD(config)#router bgp 200	Enter the BGP configuration mode.
RouterD(config-bgp)#neighbor 194.1.1.2 remote-as 200	Specify the autonomous system number of the BGP peer.
RouterD(config-bgp)#neighbor 195.1.1.2 remote-as 200	The same as above.
RouterD(config-bgp)#no synchronization	Set the asynchronic between BGP and IGP.
RouterD(config-bgp)#exit	

The above explains the dynamic routing protocol BGP. About the configuration mode of the physical layer and link layer, refer to related sections.

BGP Monitoring & Debugging

show ip bgp

Use the command show ip bgp to display all BGP information.

•

• `show ip bgp [address] [mask]`

Syntax	Description
Address	Display the route of the specified IP address in the BGP routing table
Mask	network mask

(Command mode)the privileged user configuration mode

show ip bgp flap-statistics

Use the command show ip bgp flap-statistic to display the statistics information about route flap dampening.

•

• `show ip bgp flap-statistics [address ] [mask]`

Syntax	Description
Address	Display the statistics information about route flap dampening of the specified IP address in the BGP routing table
Mask	network mask

(Command mode)the privileged user configuration mode

show ip bgp neighbor

Use the command show ip bgp neighbor to display information about the peer.

• `show ip bgp neighbor [neighbor-address]`

Syntax	Description
neighbor-address	Display information about the specified peer.

(Command mode)the privileged user configuration mode

show ip bgp regexp

Use the command show ip bgp regexp to display the route information matching with the specified AS regular expression.

- `show ip bgp regexp regular-expression`

Syntax	Description
regular-expression	Display the route information matching with the specified AS regular expression.

(Command mode)the privileged user configuration mode

show ip bgp summary

Use the command show ip bgp summary to display information about the BGP summary.

- `show ip bgp summary`

(Command mode)the privileged user configuration mode

show ip bgp community-list

Display BGP community list information.

-

- `show ip bgp community-list list-num`

(command mode)privileged user configuration mode

show ip bgp dampening

Display BGP routing dampening information

-

- `show ip bgp dampening { dampened-paths | parameters | flap-statistics }`

Syntax	Description
dampened-paths	Display dampened path information.
parameters	Display parameter
flap-statistics	Display statistics

(command mode)privileged user configuration mode

show ip bgp filter-list

Display BGP routing filter event.

-

- `show ip bgp filter-list list-num`

(command mode)privileged user configuration mode

show ip bgp prefix-list

Display BGP prefix list information.

-
- `show ip bgp prefix-list list-name`

(command mode)privileged user configuration mode

show ip bgp route-map

Display BGP routing information

-
- `show ip bgp route-map map-name`

(command mode)privileged user configuration mode

show ip bgp in-route

Display BGP accepted routing.

-
- `show ip bgp in-route`

(command mode)privileged user configuration mode

show ip bgp vpn4

Display BGP L3VPN routing.

-
- `show ip bgp vpn4`

Syntax	Description
all	Display all VPN routing
vrf vrf-name	Display designated vrf routing

(command mode)privileged user configuration mode

debug ip bgp

Use the command debug ip bgp to open the BGP message debugging information switch.

-
- `debug ip bgp [address]{all | event | keepalives | open | packets | route | state | task | timer | updates }`

Syntax	Description
Address	Open the message debugging information switch of the specified BGP peer.

All	Open all debugging information switches of BGP messages.
Event	Open BGP event debugging information switch.
Keepalive	Open BGP keepalive debugging information switch.
Open	Open BGP open debugging information switch.
Packets	Open all debugging information switches of BGP messages.
Route	Open BGP route debugging information switch.
State	Open BGP status debugging information switch.
Task	Open BGP task debugging information switch.
Timer	Open BGP timer debugging information switch.
Updates	Open BGP update debugging information switch.

(Command mode)the privileged user configuration mode.

Configuring Route-map

Route-map Configuration Commands

The configuration commands of IP route-map include the following commands:

route-map

Use the command route-map to configure a route-map and enter the route-map configuration mode; or, use the negation of the command to delete a route-map.

-
- `route-map map-name [ { permit | deny} [ seq-number ] ]`
- `no route-map map-name [ [ permit | deny ] [ seq-number ] ]`

Syntax	Description
Map-name	Identify a route-map uniquely.
permit	Set the match mode of the defined route-map sentence as Permit. When satisfying all match sub-sentences of the sentence, the route is permitted to pass the filter of the sentence and execute the set sub-sentence of the sentence; or else, the next sentence of the route-map will be tested.
deny	Set the match mode of the defined route-map sentence as Deny. When satisfying all match sub-sentences of the sentence, the route is prohibited from passing the filter of the sentence and no test of the next sentence is performed.

Seq-number	A sentence used to identify a route-map. When the route-map is applied to match, the sentence seq-number is tested.

(Command mode)the global configuration mode.

The route-map can be applied to route redistribution, policy route and BGP. One route-map is composed of several sentences and each sentence is composed of some match sub-sentences and set sub-sentences.

A match sub-sentence is used to define the match rule of the sentence and a set sub-sentence is used to define the action that will be taken after the sentence is matched successfully. The filtering relationship among the match sub-sentences of the sentence is "And", that is to say that all match sub-sentences of the sentence should be satisfied fully.

The filtering relationship among the route-map sentences is "Or", that is to say that the route-map can be regarded as matched successfully as long as one sub-sentence of the sentence is satisfied. If no sub-sentence of the sentence is satisfied, the route-map is matched unsuccessfully.

If the command parameter comprises nothing but the route-map name and the match mode or sentence number is omitted, a sentence (the sentence number is 10 and the match mode is Permit) is added by default. If the negation of the command is adopted, then all sentences of the route-map will be deleted.

match as-path

Use the command match as-path to specify the matched path list for the route-map; or, use the negation of the command to cancel the configuration.

- `match as-path path-list-number`
- `no match as-path path-list-number`

Syntax	Description
path-list-number	The path-list number. Its value range is from 1 to 199 and multiple numbers can be input .

(Command mode)the route-map configuration mode.

match community

Use the command match community to specify the matched BGP community; or, use the negation of the command to cancel the configuration.

-

- `match community community-list--number`
- `no match community community-list—number`

Syntax	Description
community-list--number	The BGP community number. Its value range is from 1 to 199 and multiple numbers can be input .

(Command mode)the route-map configuration mode.

match extcommunity

Use the command match extcommunity to specify the matched BGP/VPN extended-community; or, use the negation of the command to cancel the configuration.

- `match extcommunity extcommunity-list--number`
- `no match extcommunity extcommunity-list—number`

Syntax	Description
extcommunity-list--number	The BGP/VPN extended-community number. Its value range is from 1 to 199 and multiple numbers can be input .

(Command mode)the route-map configuration mode.

match interface

Use the command match interface to specify the matched interface; or, use the negation of the command to cancel the configuration.

- `match interface interface-names`
- `no match interface interface-names`

Syntax	Description
interface-names	name of the match interface.

(Command mode)the route-map configuration mode.

match ip address

Use the command match ip address the IP address range for route-map match; or, use the negation of the command to cancel the configuration.

- `match ip address access-list`
- `no match ip address access-list`

Syntax	Description
Access-list	The serial-number or name of the matched access-list. Multiple ones can be input successively.

(Command mode)the route-map configuration mode.

match ip next-hop

Use the command match ip next-hop to specify the matched IP address of the next hop for route-map; or, use the negation of the command to cancel the configuration.

-
- `match ip next-hop std-access-list`
- `no match ip next-hop std-access-list`

Syntax	Description
Std-access-list	The standard-access-list or name that will be matched by the next hop. Multiple ones can be input successively.

(Command mode)the route-map configuration mode.

match ip route-source

Use the command match ip route-source to specify the matched route-source address; or, use the negation of the command to cancel the configuration.

-
- `match ip route-source std-access-list`
- `no match ip route-source std-access-list`

Syntax	Description
Std-access-list	The standard-access-list number or name that is matched by the resource-route. Multiple ones can be input successively.

(Command mode)the route-map configuration mode.

match length

Use the command match length to specify the length range of the matched message; or, use the negation of the command to cancel the configuration.

-
- `match length min-pkt-length max-pkt-length`
- `no match length min-pkt-length max-pkt-length`

Syntax	Description
min-pkt-length	The minimal packet length

max-pkt-length	maximal packet length

(Command mode)the route-map configuration mode.

match metric

Use the command match metric to specify the matched metric value; or, use the negation of the command to cancel the configuration.

-
- `match metric metric-value`
- `no match metric metric-value`

Syntax	Description
Metric-value	The matched metric values. Multiple ones can be input.

(Command mode)the route-map configuration mode.

match route-type

Use the command match route-type to specify the matched route type; or, use the negation of the command to cancel the configuration.

-
- `match route-type route-type`
- `no match route-type route-type`

Syntax	Description
route-type	The matched route type: external, internal, level-1, level-2, local or nssa-external

(Command mode)the route-map configuration mode.

match tag

Use the command match tag to specify the matched tag-value of the route information; or, use the negation of the command to cancel the configuration.

-
- `match tag tag-value`
- `no match tag [tag-value]`

Syntax	Description
Tag-value	The matched tag value. Multiple ones can be input.

(Command mode)the route-map configuration mode.

set as-path

Use the command set as-path to specify an AS number; or, use the negation of the command to cancel the configuration.

-
- `set as-path prepend as-path-number`
- `no set as-path prepend as-path-number`

Syntax	Description
as-path-number	The AS number. Multiple ones can be input.

(Command mode)the route-map configuration mode.

set community

Use the command set community to set the BGP community of the source-route in the route-map; or, use the negation of the command to cancel the configuration.

-
- `set communtiy {additive | local-AS | no-advertise | no-export | none}`
- `no set communtiy {additive | local-AS | no-advertise | no-export | none}`

Syntax	Description
additive	Add the community to the existing community.
local-AS	Do not send the matched route out of the autonomous system.
no-advertise	Do not send the matched route to any peer/ any peer group.
no-export	Announce the route with the attribute to the peer/peer group of the autonomous system except the peer/peer group out of the autonomous system.
None	Delete the community of the route.

(Command mode)the route-map configuration mode.

set ip next-hop

Use the command set ip next-hop to change the next hop of the source-route in the route-map; or, use the negation of the command to cancel the configuration.

-
- `set ip next-hop ip-address`
- `no set ip next-hop ip-address`

Syntax	Description
ip-address	Set the IP address of the next hop

(Command mode)the route-map configuration mode.

set ip next-hop peer-address

Designate BGP neighbor address, and no is used to cancel the configuration.

-
- `set ip next-hop peer-address`
- `no set ip next-hop peer-address`

(command mode)routing mapping configuration mode.

set ip next-hop verify-availability

Configure whether the next hop is the neighbor of NDSP, and no is used to cancel the configuration.

-
- `set ip next-hop verify-availability`
- `no set ip next-hop verify-availability`

(command mode)routing mapping configuration mode

set local-preference

Use the command set local-preference to change the local preference of the source-route in the route-map; or, use the negation of the command to cancel the local preference of the source-route.

- `set local-preference value`
- `no set local-preference value`

Syntax	Description
value	The local preference.

(Command mode)the route-map configuration mode.

set metric

Use the command set metric to change the metric of the source-route in the route-map; or, use the negation of the command to cancel the configuration.

- `set metric metric`
- `no set metric metric`

Syntax	Description
metric	Set the metric.

(Command mode)the route-map configuration mode.

set metric-type

Configure routing protocol metric type, and no is used to cancel the configuration.

-
- `set metric-type {external | internal | type-1 | type-2}`
- `no set metric-type`

Syntax	Description
external	Configure IS—IS external metric.
internal	Configure IS-IS internal metric,or BGP using IGP metric as MED.
type-1	Configure OSPF external routing type 1 metric.

type-2	Configure OSPF external routing type 2 metric.

(command mode)routing mapping configuration mode.

set origin

Use the command set origin to change the origin of the source-route in the route-map; or, use the negation of the command to cancel the configuration.

-
- `set origin {egp | igp | incomplete}`
- `no set origin`

Syntax	Description
egp, igp,incomplete	Set the origin.

(Command mode)the route-map configuration mode.

set automatic-tag

Use the command set automatic-tag to set the automatic-tag area; or, use the negation of the command to cancel the configuration.

-
- `set automatic-tag`
- `no set automatic-tag`

(Command mode)the route-map configuration mode.

set comm-list

Use the command set comm-list to adopt the community list to set the community; or, use the negation of the command to cancel the configuration.

-
- `set comm-list  std-comm-list | ext-comm-list`
- `no set comm-list  [ std-comm-list | ext-comm-list ]`

Syntax	Description
std-comm-list	The standard-community-list number (1-99).
ext-comm-list	The extended-community-list number(100-199).

(Command mode)the route-map configuration mode.

set dampening

Use the command set dampening to set BGP route dampening (attenuation) parameter; or, use the negation of the command to cancel the configuration.

- set dampening time
- no set dampening [time]

Syntax	Description
time	The time.

(Command mode)the route-map configuration mode.

set extcommunity rt

Configure routing Target extended community attribute, and no is used to cancel the configuration.

-
- set extcommunity rt ext-community
- no set extcommunity

Syntax	Description
ext-community	VPN community extension.

(command mode)routing mapping configuration mode
set extcommunity soo
Configure routing Target extension community, and no is used to cancel the configuration.

- set extcommunity soo ext-community
- no set extcommunity

Syntax	Description
ext-community	VPN community extension.

(command mode)routing mapping configuration mode
set default

Use the command set default to specify the default interface for transmitting packets; or, use the negation of the command to cancel the configuration.

-
- set default interface interface-names
- no set default interface interface-name

Syntax	Description
Interface-name	The interface name. Multiple interfaces can be supported .

(Command mode)the route-map configuration mode.

set interface

Use the command set interface to set the interface for transmitting packets; or, use the negation of the command to cancel the configuration.

- `set interface interface-names`
- `no set interface interface-name`

Syntax	Description
Interface-name	The interface name. Multiple interfaces can be supported .

(Command mode)the route-map configuration mode.

set ip default next-hop

Configure packet forwarding next hop IP address. And no is used to cancel the configuration.

- `set ip default next-hop ip-address`
- `no set ip default next-hop ip-address`

Syntax	Description
Ip-address	The next hop IP address

`(command mode)routing mapping configuration modeset ip default next-hop verify-availability`
Configure whether next hop is the neighbor of NDSP, and no is used to cancel the configuration.

- `set ip default next-hop verify-availability`
- `no set ip default next-hop verify-availability`

(Command mode)the route-map configuration mode.

set ip default

Use the command set ip default to specify the next hop IP address to which the packet will be transmitted; or, use the negation of the command to cancel the configuration.

- `set ip default next-hop ip-address`
- `no set ip default next-hop ip-address`

Syntax	Description
Ip-address	The next hop IP address (in the form of dotted decimal notation)

(Command mode)the route-map configuration mode.

set ip df

Use the command set ip df to set the slicing-flag of an IP message; or, use the negation of the command to cancel the configuration.

•

• `set ip df bit-value`

• `no set ip df [ bit-value ]`

Syntax	Description
bit-value	The value of the slicing-bit.(0 or 1).

(Command mode)the route-map configuration mode.

set ip precedence

Use the command set ip precedence to specify the priority level of an IP message; or, use the negation of the command to cancel the configuration.

•

• `set ip precedence number | critical | flash-override | immediate | internet | network | priority | routine`

• `no set ip precedence [ number | critical | flash-override | immediate | internet | network | priority | routine ]`

Syntax	Description
number	Priority level(0-7).
routine	0
priority	1
immediate	2
flash	3
flash-override	4
critical	5
internet	6

network	7

(Command mode)the route-map configuration mode.

set ip qos-group

Use the command set ip qos-group to set the QoS group of an IP packet; or, use the negation of the command to cancel the configuration.

•

• `set ip qos-group qos-group-number`

• `no set ip qos-group [ qos-group-number ]`

Syntax	Description
qos-group-number	QOS group-number(0-99).

(Command mode)the route-map configuration mode.

set ip tos

Use the command set ip tos to set the IP TOS; or, use the negation of the command to cancel the configuration.

•

• `set ip tos tos-value | max-reliability | max-viaput | min-delay | min-monetary-cost | normal`

• `no set ip tos [ tos-value | max-reliability | max-viaput | min-delay | min-monetary-cost | normal ]`

Syntax	Description
tos-value	The value of TOS field(0-15).
max-reliability	The maximal reliability.
max-viaput	The maximal viaput.
min-delay	The minimal delay.
min-monetary-cost	The minimal costs

(Command mode)the route-map configuration mode.

set tag

Use the command set tag to configure the tag value of the OSPF route information; or, use the negation of the command to delete the configuration.

•

- `set tag tag-value`
- `no set tag [tag-value]`

Syntax	Description
Tag-value	configured tag-value

(Command mode)the route-map configuration mode.

set weight

Use the command set weight to set the attribute weight; or, use the negation of the command to cancel the configuration.

- `set weight weight-value`
- `no set weight [weight-value]`

Syntax	Description
weight-value	weight value

(Command mode)the route-map configuration mode.

show route-map

Use the command show route-map to display contents of the route-map.

- `show route-map [ routemap-name ]`

Syntax	Description
routemap-name	The name of the route-map whose contents will be displayed.

(Command mode)the privileged user configuration mode.

Configuring Route-Map

Please refer to the examples of configuring policy route and BGP route.

Configuring Policy Route

Policy route is a more flexible mechanism of routing messages than destination routing. It is a procedure that a packet is transmitted by means of route mapping before a router routes a packet.

The route mapping determines which next route the packet will be routed to. When the shortest route path of a packet is uncertain, the policy route can be enabled to solve the problem. And the policy route can perform routing according to source address, protocol and port-number.

Policy-based Route Configuration Commands

To enable policy route, you should determine which route mapping is applied to policy route and establish a route mapping. The route mapping is used to specify the match standard and related actions that can be taken when the match conditions are met.

There exist three aspects of policy route configuration commands: A) enabling policy routing for packet forwarding; B) enabling rapid-switch policy routing; C) enabling local policy routing. And the configuration commands are described in details as follows:

ip policy route-map

To enable the policy route of an interface in the interface configuration mode, execute the command ip policy route-map. The policy route controls all packets arriving at the interface.

If the policy route fails to control them, packets will go on finding a routing table. The negation of the command is used to disclose the policy route of the interface.

-
- `ip policy route-map route-map-name`
- `no ip policy route-map route-map-name`

Syntax	Description
route-map-name	Specify the name of the route mapping applied to the policy route of packet forwarding

(By default) Nothing
(Command mode)the interface configuration mode

The command is enabled to disabled the rapid forwarding of the interface.

ip route-cache policy

The rapid forwarding of the policy route can enhance the rate of forwarding a packet. To enable the function, execute the command ip route-cache policy in the interface configuration mode. After the command is enabled, the forwarding packet received on the local interface will first be controlled by rapid buffer memory the policy route. The negation of the command is used to disable the rapid forwarding of the policy route.

-
- `ip route-cache policy`
- `no ip route-cache policy`

(By default) Nothing
(Command mode)the interface configuration mode.

ip local policy route-map

To enable the local policy route for the packets generated from the router, execute the command ip local policy route-map in the global configuration mode so that which route mapping should be applied by the router.

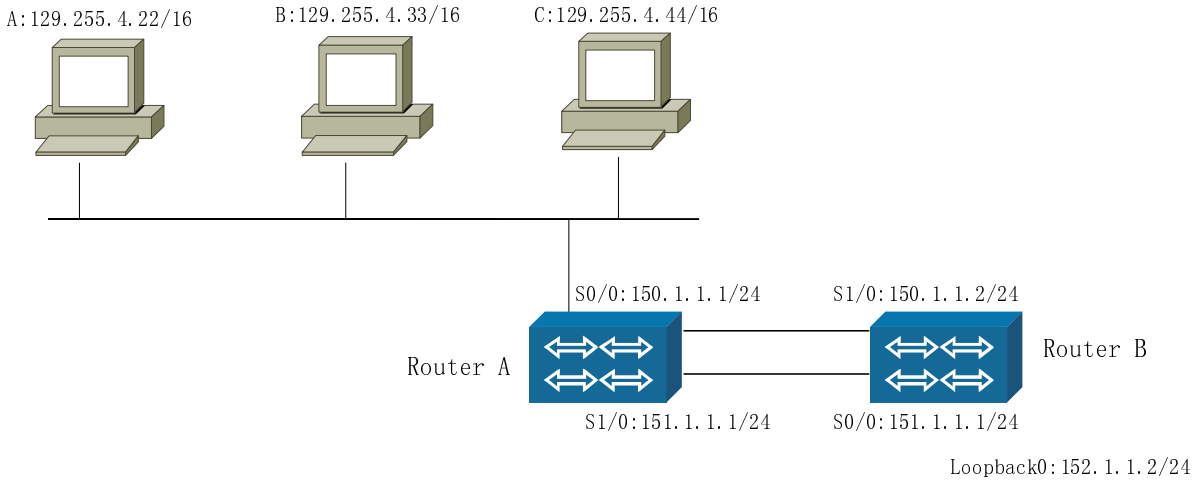
After the command is enabled, the local policy route controls all packets from the router. If the policy route fails to do them, the packets will go on finding a routing table.

- `ip local policy route-map route-map-name`
- `no ip local policy route-map route-map-name`

Syntax	Description
route-map-name	Specify the name of the route mapping applied to the local policy route.

(By default) Nothing.
(Command mode)the global configuration mode

Policy-based Route Configuration



RouterA connects with RouterB via two private lines.

RouterA connects with 3 PCs via the Ethernet.

Configure the loopback interface of RouterB as the testing point.

A static route is configured between RouterA and RouterB.

The goal of the example is to demonstrate the packet policy route based on the source IP address: RouterA sends all data from 129.255.4.44 out of the interface S0/0 and sends all data from 129.255.4.33 out of the interface S1/0, and all other data are routed according to the destination.

RouterA is configured as follows:

Command	Task
routerA(config-if-fastethernet0)#ip address 129.255.4.11 255.255.0.0	Configure the Ethernet address.
routerA(config-if-fastethernet0)#ip policy route-map map1	Apply IP policy route map 1 to interface f0.
routerA(config-if-fastethernet0)#interface serial0/0	
routerA(config-if-serial0/0)# physical-layer sync	Configure the physical-layer as the synchronism mode.
routerA(config-if-serial0/0)# encapsulation ppp	Encapsulate PPP on the interface s0/0.
routerA(config-if-serial0/0)#ip address 150.1.1.1 255.255.255.0	
routerA(config-if- serial0/0)#interface serial1/0	
routerA(config-if-serial1/0)#physical-layer sync	
routerA(config-if-serial1/0)# clock rate 64000	
routerA(config-if-serial1/0)# encapsulation ppp	Encapsulate PPP on the interface s1/0.
routerA(config-if-serial1/0)#ip address 151.1.1.1 255.255.255.0	
routerA(config-if-serial1/0)#exit	
routerA(config)# ip local policy route-map map1	Make the route use the policy map1 to route the packets generated by itself.
routerA(config)# ip route 152.1.1.2 255.255.255.255 serial1/0	Configure the static route to the loopback interface of RouterB.
routerA(config)#ip route 152.1.1.2 255.255.255.255 serial0/0	Configure the static route to the loopback interface of RouterB.
routerA(config)# route-map map1 permit 10	Configure route map 1 and rule execution number 10.
routerA(config-route-map)# match ip address 1	The match standard that adopts the policy route for data packet to enter the Ethernet port of the router accords with standard access list 1.
routerA(config-route-map)#set interface serial0/0	Set the packet path: the packet is sent out of the interface s0/0.
routerA(config-route-map)#exit	
routerA(config)# route-map map1 permit 20	Configure route map 1 and rule execution number 20.
routerA(config-route-map)# match ip address 2	The match standard that adopts the policy route for data packet to enter the Ethernet port of the router accords with standard access list 2.
routerA(config-route-map)#set interface serial1/0	Set the packet path: the packet is sent out of the interface s1/0.
routerA(config-route-map)#exit	

routerA(config)#access-list 1 permit host 129.255.4.44	Set access list 1.
routerA(config)#access-list 2 permit host 129.255.4.33	Set access list 2.

RouterB is configured as follows:

Command	Task
routerB(config-if-loopback0)#ip address 152.1.1.2 255.255.255.255	Configure the loopback interface as the testing point.
routerB(config-if-serial0/0)# physical-layer sync	
routerB(config-if-serial0/0)# encapsulation ppp	Encapsulate PPP on the interface s0/0.
routerB(config-if-serial0/0)# ip address 151.1.1.2 255.255.255.0	
routerB(config-if-serial0/0)#interface serial1/0	
routerB(config-if-serial1/0)#physical-layer sync	
routerB(config-if-serial1/0)# clock rate 64000	
routerB(config-if-serial1/0)# encapsulation ppp	Encapsulate PPP on the interface s1/0.
routerB(config-if-serial1/0)#ip address 150.1.1.2 255.255.255.0	
routerB(config-if-serial1/0)#exit	
routerB(config)#ip route 129.255.0.0 255.255.0.0 serial1/0	Configure the static route to the interface f0 of Route A.
routerB(config)#ip route 129.255.0.0 255.255.0.0 serial0/0	Configure the static route to the interface f0 of Route A.

Monitoring and Debugging of Policy Route

show ip policy

The command is used to display the policy route configuration of an interface.

-
- `show ip policy`

(Command mode)the privileged user mode.

Show ip cache policy

The command is used to display policy route buffer.

-
- `show ip cache policy`
- `show ip cache policy detail`

(Command mode)the privileged user mode.

Show ip local policy

The command is used to display the configuration of the local policy route.

- `show ip local policy`

(Command mode)the privileged user mode.

debug ip policy

The command is used to trace the policy route control of a packet.

-
- `debug ip policy`
- `no debug ip policy`

(Command mode)the privileged user mode.

Configuring M-VRF

M-VRF is a technology supporting VPN. There exist multiple VRFs on each router, and each kind of source on the router (such as interface, IP address, protocol, control module and routing table) has its own VRF attribute.

The mutual access among the resources with different VRF is denied. M-VRF can be used to realize network isolation and address overlap. This can realize the network security to a certain extent.

M-VRF Configuration Commands

To enable M-VRF, it is necessary to generate a VRF (there exists a global VRF in the system):

ip vrf

To generate a vrf, use the command ip vrf. And the negation of the command is used to delete a vrf.

-

- `ip vrf vrf-name`
- `no ip vrf vrf-name`

Syntax	Description
vrf—name	Specify a name for generating a vrf.

(By default) Nothing.
(Command mode)the global configuration mode

rd

The command rd is used to specify a RD (route distinguisher) for a generated vrf. The generated VRF cannot take effect until the RD is specified.

-
- `rd as:nn`
- `rd ip_addr:nn`

Syntax	Description
as:nn	As: a value within 0 and 65535; Nn: a value within 0 and 4294967295.
ip_adr:nn	Ip_addr: the value within 0.0.0.0 and 255.255.255.255 nn: the value within 0 and 65535.

(By default) Nothing.
(Command mode)the vrf configuration.

Once the RD is configured, it should be deleted if it need be modified.

ip vrf forwarding

To related an interface with a valid vrf, use the command ip vrf forwarding. The negation of the command is used to delete the relation between the interface and the vrf.

-
- `ip vrf forwarding vrf-name`
- `no ip vrf forwarding vrf-name`

Syntax	Description
vrf—name	The vrf_name bound with the interface.

(By default) Nothing
(Command mode)the interface configuration mode.

After there exists a relation between an interface and an effective vrf, all configured IP addresses will be deleted.

An interface can establish a relation with only one vrf.

To describe related vrf information, use the command description. And the negation of the command is used to delete the description information about the vrf.

-
- `description line`
- `no description line`

Syntax	Description
line	The description of the interface

ip route

The command ip route is used to expand the static route and make it support vrf. The negation of the command is used to delete the static route.

-
- `ip route vrf vrf_name xxxx xxxx`
- `no ip route vrf vrf_name xxxx xxxx`

Syntax	Description
vrf—name	The vrf name of the static route.

(By default) Nothing
(Command mode)the global configuration mode

arp

The command arp is used to expand a static arp and make it support vrf. The negation of the command is used to delete the static arp.

•

• `arp vrf vrf_name xxxx xxxx`

• `no arp vrf vrf_name xxxx xxxx`

Syntax	Description
Vrf—name	The vrf name of the static arp.

(By default) Nothing.
(Command mode)the global configuration mode

telnet

The command telnet is used to expand telnet and make it support vrf.

•

• `telnet vrf vrf_name xxxx`

Syntax	Description
vrf—name	Telnet the vrf_name of the server.

(By default) Nothing
(Command mode)the privileged user mode

ping

The command ping is used to expand ping and make it support vrf.

•

• `ping vrf vrf_name xxxx`

Syntax	Description
vrf—name	Ping vrf_name of opposite end

	address

(By default) Nothing.
(Command mode)the privileged user mode

quickping
The command quickping is used to expand quickping and make it support vrf.

- `quickping vrf vrf_name xxxx`

Syntax	Description
Vrf—name	Specify a vrf name.

(By default) Nothing
(Command mode)the privileged user mode
clear ip route

The command clear ip route is used to expand clear ip route and make it support vrf.

-

- `clear ip route vrf vrf_name xxxx`

Syntax	Description
vrf—name	Specify a vrf name.

(By default) Nothing
(Command mode)the privileged user mode

traceroute

The command traceroute is used to expand traceroute and make it support vrf.

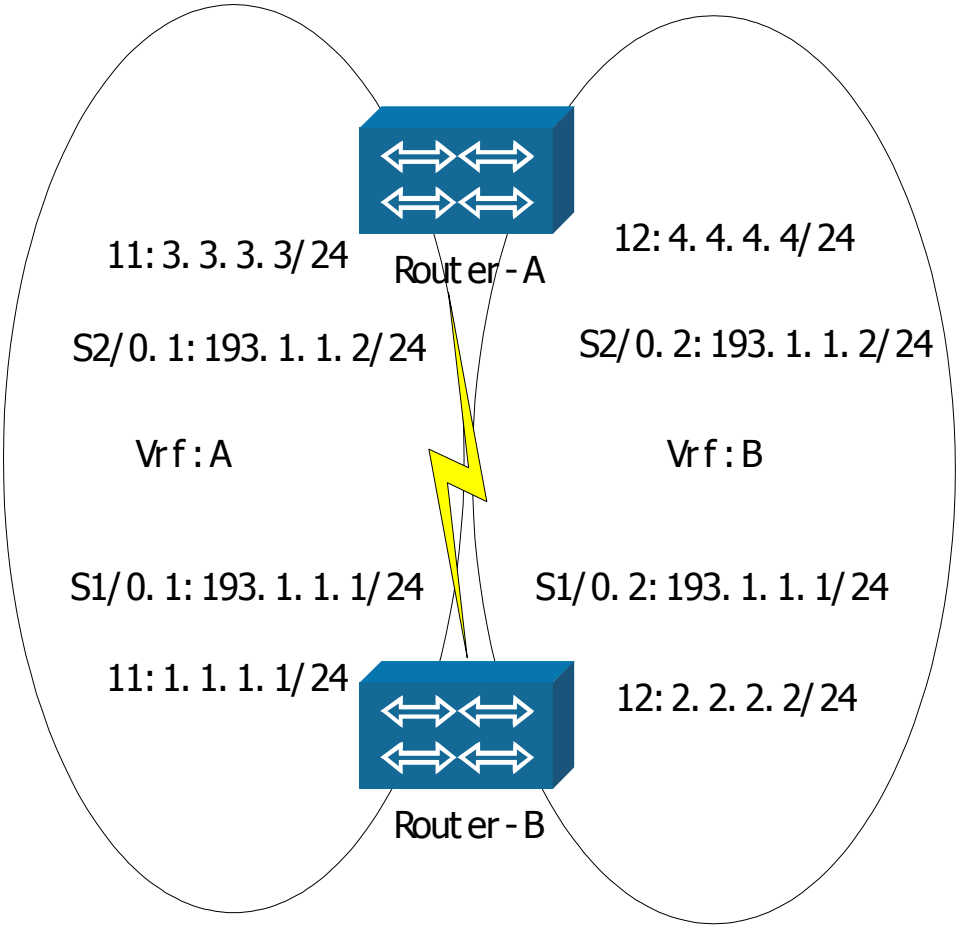
-

- `traceroute vrf vrf_name`

Syntax	Description
vrf—name	Specify a vrf name.

(By default) Nothing
(Command mode)the privileged user mode

M-VRF Configuration



The interface s2/0 of RouterA connects with the interface s1/0 of RouterB. Interfaces s2/0.1, s2/0.2, s1/0.1 and s1/0.2 are configured respectively. For RouterA, s2/0.1、l1 belongs to vrf A, and s2/0.2、l2 belongs to vrf B; For RouterB, s1/0.1、l1 belongs to vrf A, and s1/0.2、l2 belongs to vrf B.

2) Enable the dynamic routing protocol RIP on RouterA and RouterB.

RouterA is configured as follows:

Command	Task
RouterA#configure terminal	Enter the global configuration mode.
RouterA(config)#ip vrf a	Create vrf a.
RouterA(config-vrf)#rd 1:1	Specify a route description character.
RouterA(config-vrf)#exit	
RouterA(config)#ip vrf b	Create vrf b
RouterA(config-vrf)#rd 2:2	Specify a route description

	character.
RouterA(config-vrf)#exit	
RouterA(config)#interface loopback1	Create loopback interface 11.
RouterA(config-if-loopback1)# ip vrf forwarding a	Add the interface to vrf a.
RouterA(config-if-loopback1)#ip address 3.3.3.3 255.255.255.0	Configure an IP address.
RouterA(config-if-loopback1)#interface loopback2	Create loopback interface 12.
RouterA(config-if-loopback2)# ip vrf forwarding b	Add the interface to vrf b.
RouterA(config-if-loopback2)#ip address 4.4.4.4 255.255.255.0	Configure an IP address.
RouterA(config-if-loopback2)# interface serial2/0	Enter the interface s2/0.
RouterA(config-if-serial2/0)#encapsulation frame-relay	Encapsulate the frame-relay.
RouterA(config-if-serial2/0)# clock rate 128000	Configure the clock rate.
RouterA(config-if-serial2/0)#frame-relay intf-type dte	Configure the dte mode.
RouterA(config-if-serial2/0)#interface serial2/0.1	Create sub-interface s2/0.1.
RouterA(config-if-serial2/0.1)#ip vrf forwarding a	Add the sub-interface to vrf a.
RouterA(config-if-serial2/0.1)#frame-relay interface-dlci 100	Assign a DLCI number 100.
RouterA(config-fr-dlci)#frame-relay map ip 193.1.1.1 100 broadcast	Set a mapping between the opposite-end IP address and local-end DLCI number.
RouterA(config-if-serial2/0.1)#ip address 193.1.1.2 255.255.255.0	Configure an IP address.
RouterA(config-if-serial2/0.1)#interface serial2/0.2	Create sub-interface s2/0.1.
RouterA(config-if-serial2/0.2)#ip vrf forwarding b	Add the sub-interface to vrf b.
RouterA(config-if-serial2/0.2)#frame-relay interface-dlci 200	Assign a DLCI number 200.
RouterA(config-fr-dlci)#frame-relay map ip 193.1.1.1 200 broadcast	Set a mapping between the opposite-end IP address and local-end DLCI number.
RouterA(config-if-serial2/0.2)#ip address 193.1.1.2 255.255.255.0	Configure an IP address.
RouterA(config-if-serial2/0.2)#exit	
RouterA(config)#router rip	Enable RIP routing protocol.
RouterA(config-rip)#address-family ipv4 vrf a	Create a address-family vrf a.
RouterA(config-rip-af)#network 3.0.0.0	
RouterA(config-rip-af)#network 193.1.1.0	
RouterA(config-rip-af)#exit	
RouterA(config-rip)#address-family ipv4 vrf b	Create a address-family vrf b.
RouterA(config-rip-af)#network 4.0.0.0	

RouterA(config-rip-af)#network 193.1.1.0	
RouterA(config-rip-af)#end	The configuration ends.

RouterB is configured as follows:

Command	Task
RouterB#configure terminal	
RouterB(config)#ip vrf a	
RouterB(config-vrf)#rd 1:1	
RouterB(config-vrf)#exit	
RouterB(config)#ip vrf b	
RouterB(config-vrf)#rd 2:2	
RouterB(config-vrf)#exit	
RouterB(config)#interface loopback1	
RouterB(config-if-loopback1)# ip vrf forwarding a	
RouterB(config-if-loopback1)#ip address 1.1.1.1 255.255.255.0	
RouterB(config-if-loopback1)#interface loopback2	
RouterB(config-if-loopback2)# ip vrf forwarding b	
RouterB(config-if-loopback2)#ip address 2.2.2.2 255.255.255.0	
RouterB(config-if-loopback2)#exit	
RouterB(config)#frame-relay switching	
RouterB(config)#interface serial1/0	
RouterB(config-if-serial1/0)#encapsulation frame-relay	
RouterB(config-if-serial1/0)#frame-relay intf-type dce	
RouterB(config-if-serial1/0)#interface serial1/0.1	
RouterB(config-if-serial1/0.1)#ip vrf forwarding a	
RouterB(config-if-serial1/0.1)#frame-relay interface-dlci 100	
RouterB(config-fr-dlci)#frame-relay map ip 193.1.1.2 100 broadcast	
RouterB(config-if-serial1/0.1)#ip address 193.1.1.1 255.255.255.0	
RouterB(config-if-serial1/0.1)#interface serial1/0.2	
RouterB(config-if-serial1/0.2)#ip vrf forwarding b	
RouterB(config-if-serial1/0.2)#frame-relay interface-dlci 200	
RouterB(config-fr-dlci)#frame-relay map ip 193.1.1.2 200 broadcast	
RouterB(config-if-serial1/0.2)#ip address 193.1.1.1 255.255.255.0	

RouterB(config-if-serial1/0.2)#exit	
RouterB(config)#router rip	
RouterB(config-rip)#address-family ipv4 vrf a	
RouterB(config-rip-af)#network 1.0.0.0	
RouterB(config-rip-af)#network 193.1.1.0	
RouterB(config-rip-af)#exit	
RouterB(config-rip)#address-family ipv4 vrf b	
RouterB(config-rip-af)#network 2.0.0.0	
RouterB(config-rip-af)#network 193.1.1.0	
RouterB(config-rip-af)#end	

Any vrf cannot be added to Loopback0.
only one vrf can be added to an interface.

Monitoring & Debugging M-VRF

Show ip route

The command Show ip route is used to expand Show ip route and make it support vrf.

- `show ip route vrf vrf_name`

Syntax	Description
vrf—name	Specify a vrf name.

(Command mode)the privileged user mode

Show arp

The command Show arp is used to expand Show arp and make it support vrf.

-

- `show arp vrf vrf_name xxxx`

Syntax	Description
Vrf—name	Specify a vrf name.

(Command mode)the privileged user mode

netstat –r

The command netstat –r is used to expand netstat –r and make it support vrf.

-

- `netstat -r vrf vrf_name`

Syntax	Description
vrf—name	Specify a vrf name.

(Command mode)the privileged user mode

Multicast Routing Configuration

This chapter introduces the core multicast packet forwarding on a router, IGMP application and the selection of multicast routes.

Configure Multicast Common Part

Multicast Common Configuration

Multicast common configuration part is the basis of running multicast, and the common part of all multicast. For example, no matter running any multicast routing protocol, first we should enable ip multicast-routing.

Basic Commands of Multicast Common Configuration

Command	Description	Config. mode
Ip multicast-routing	* enable multicast routing	Config
Ip multicast route-limit num	Multicast routing entry number	Config

ip multicast heartbeat group-ip source-ip min-packets interval	Data packet forwarding rate monitor	Config
ip multicast boundary {access-list num| access-list name}	*multicast management boundary configuration	Config-if-××
ip multicast rate-limit {in | out} {access-list num | access-list name} rate	Multicast forwarding rate control	Config-if-××
ip multicast ttl-threshold num	Multicast interface TTL value configuration	Config-if-××

"*" before command means it has configuration example description.

configuration mode is: config, config-if-××(interface name) config-××(protocol name) .

ip multicast-routing

This command is used to enable multicast routing, and command no is used to disable multicast routing.

```
ip multicast-routing
no ip multicast-routing
```

(Default status)disable multicast routing by default
(command mode) global configuration mode.

ip multicast route-limit

This command is used to limit setting up multicast routing entry number.

```
ip multicast route-limit num
no ip multicast route-limit
```

Syntax	Description
num	Multicast routing entry number

(Default status) multicast routing entry number default value(MP3700/MP7200/MP3680(except MPU102) 4K by default, other series 1K by default.)

(command mode) global configuration mode

ip multicast heartbeat

After configuring this command, if the time is in interval, and (S, G) forwarding packet number is less than min-packets, the warning information will be printed. Command no is used to cancel heartbeat warning.

```
ip multicast heartbeat group-ip source-ip min-packets
interval
no ip multicast heartbeat group-ip source-ip
```

Syntax	Description
group-ip source-ip min-packets interval	Group address Source address Forwarding data packet number minimum value(1-2147483647) Statistics time interval (10-3600 seconds)

(Default status)not enable this warning function
(command mode)global configuration mode

ip multicast boundary

Configure multicast egress management boundary. Command no is used to cancel the configuration.

```
ip multicast boundary {access-list num| access-list name}
no ip multicast boundary
```

Syntax	Description
access-list num | access-list name	Access list number or name

(Default status)no management boundary
(command mode)interface configuration mode

Configure standard access list.

The configuration is as following:

```
ROUTER1#conf t
ROUTER1(config)#
ROUTER1(config)#ip access-list standard 1
ROUTER1(config-std-nacl)#deny 239.255.0.0 0.0.255.255
ROUTER1(config-std-nacl)#exit
ROUTER1(config)#inter f0
ROUTER1(config-if-fastethernet0)#ip multicast boundary 1
ROUTER2 configuration is the same.
```

ip multicast rate-limit

Configure interface input and output multicast data packet rate. Command no is used to cancel the configuration.

```
ip multicast rate-limit {in | out} {access-list num | access-
list name} rate
no ip multicast rate-limit {in | out} {access-list num |
access-list name}
```

Syntax	Description
in	Limit input data packet rate.

out access-list num | access-list name rate	Limit output data packet rate. Access list number or name, only for extension access list. Rate value(60-4294967 bytes/second)

(Default status) not enable multicast rate limit by default
(command mode)interface configuration mode

ip multicast ttl-threshold

Configure multicast interface TTL value. The packet only can be passed when TTL is bigger than this
value. The default value is 0. Command no is used to cancel ttl configuration.

```
ip multicast ttl-threshold num
no ip multicast ttl-threshold
```

Syntax	Description
Num	TTL value

(Default status)not enable multicast TTL threshold
(command mode)interface configuration mode

Configure IGMP

Overview

IGMP (Internet Group Management Protocol) is a part of IP that is used by muticast routers to manage the local group memberships, and by IP hosts to report their host group memberships to any immediately-neighboring multicast routers.

There are three types of IGMP messages: Membership Query, Membership Report and Leave Group Report.

Membership Query:
There are two sub-type of Membership Query messages: General Query (which sent periodically by router to learn which groups have members on an attached network) and Group-Specific Query (which used by router to learn if a particular group has any members on an attached network).
These two messages are differentiated by the Group Address: General Query is sent with group address field set to zero and to an IP destination address of all-systems group (224.0.0.1), and Group-Specific Query is sent with group address field set to the group being queried ant to an IP destination address of this group.

Membership Report:
Receiving a Membership Query, the host sets a delay timer for the queried group(if a General Query is received) or delay timers for each group (if a Group-Specific Query is received, and excluding the all-systems group) of which it is a member on the interface from which it received the query. When a group's timer expires, the host multicasts a Version 2 Membership Report packet to the group.

When a router receives a Report, it adds the group being reported to the list of multicast group memberships on the network the Report arrived, and sets the timer for the membership to the [Group Membership Interval]. Repeated Reports refresh the timer. If no Reports are received for a particular group before this timer has expired, the router assumes that the group has no local members and that it need not forward remotely-originated multicasts for that group onto the attached network.

Leave Group Report:
When a host leaves a multicast group, it send a Leave Group message to the all-routers multicast group (224.0.0.2).

IGMP is an asymmetric protocol from the points of view of a host and a router. The host responds the IGMP query message from the multicast router with a Membership Report; The router sends General Query packets periodically to learn which groups have members on its attached network and sends a Group-Specific Query message to learn whether a specific group has members.

Configuring IGMP

ip igmp query-interval

This command is used to configure the interval for the router to send IGMP query messages. The no form of this command is used to reset the value of the interval to default.

```
ip igmp query-interval seconds
no ip igmp query-interval
```

Syntax	Description
Seconds	The interval to send IGMP query messages. It can be a number from 1 to 65535

(Default) 60 seconds.

(Command mode)The interface configuration mode.

ip igmp access-group

This command is used to control which groups can be joined by hosts on the router's attached network. The no form of this command is used to disable the control.

```
ip igmp access-group {access-list num | access-list name}
no ip igmp access-group
```

Syntax	Description
access-list num | access-list name	Standard access list number or name

(Default status)no group access list, accepting all group membership reports.
(command mode)The interface configuration mode

Note: Only standard access list can be used.

ip igmp static-group

This command is used to configure the router to act as having a statically connected member of this group, so the router will forward all the muticast packets for this group to the attached network. The no form of this command is to remove the statical member of this group.

```
ip igmp static-group {all | multicast-ipaddress}
no ip igmp static-group {all | multicast-ipaddress}
```

Syntax	Description
all multicast-ipaddress	Configure static group Configure as static group

(Default status)no static member of any group
(command mode)The interface configuration mode

ip igmp version

This command is used to configure which IGMP version the router uses on the interface. Our router supports v2 and v3, and default to v3. The no form is used to restore the default version of v3.

```
ip igmp version version-num
no ip igmp version
```

Syntax	Description
version-num	IGMP version number (2～3)

(Default status)IGMP version 3

(command mode) The interface configuration mode

ip igmp explicit-tracking

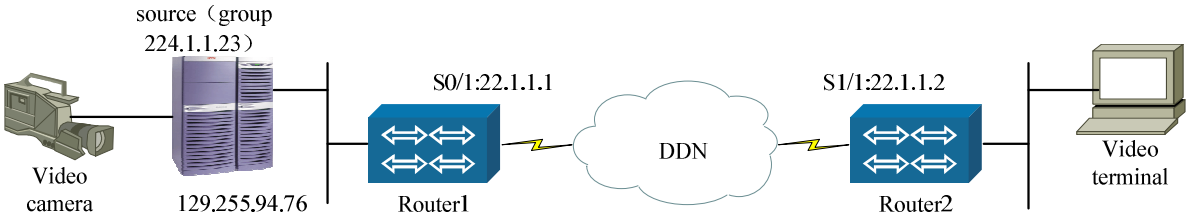
This command is used to enable the router to track the IGMP membership state of all reporting hosts. If the last host leave a group, the router deletes the group from the membership list immediately without sending any Group-Specific Query. This feature allows the router to achieve minimal leave latencies when host leave a multicast group. The no form of this command is used to disable this feature.

```
ip igmp explicit-tracking
no ip igmp explicit-tracking
```

(Default status) Tracking of hosts is disabled
(command mode) The interface configuration mode

IGMP Configuration Example

The example is illustrated with the following figure:



Interface s0/1 (22.1.1.1) of router1 connects with interface s1/1(22.1.1.2) of router2 through PPP network. The video server(129.255.94.76) connecting to Router1 serves as the source for multicast group 224.1.1.23, the video terminal connecting to Router2 serves as the member of this group.

The configurations of router1 and router2 are showed below:

Command	Description
router1#configure terminal	
router1(config)#ip multicast-routing	Enable multicast routing forwarding.
router1(config)#interface s0/1	
router1(config-if-serial0/1)#physical-layer sync	
router1(config-if-serial0/1)#clock rate 2000000	
router1(config-if-serial0/1)#encapsulation ppp	
router1(config-if-serial0/1)#ip address 22.1.1.1 255.255.255.0	
router1(config-if-serial0/1)#ip pim sparse-mode	This command is used to configure the multicast routing protocol. It should be used on all the interfaces that are used for multicast forwarding.
router1(config-if-serial0/1)#ip igmp query-interval 30	Set the IGMP query interval to be 30 seconds.
router1(config-if-serial0/1)# interface f0	
router1(config-if-fastethernet0)#ip address 129.255.22.253 255.255.0.0	
router1(config-if-fastethernet0)#ip pim sparse-mode	This command is used to configure the multicast routing protocol. It should be used on all the interfaces that are used for multicast forwarding.
router1(config-if-fastethernet0)#exit	
router1(config)#ip pim rp-candidate s0/1	Configure this specific interface as PIM RP candidate.
router1(config)#ip pim bsr-candidate s0/1	Configure this specific interface as PIM BSR candidate.
router2#conf t	
router2(config)#ip multicast-routing	Enable the multicast routing forwarding.
router2(config)#interface s1/1	
router2(config-if-serial1/1)#physical-layer sync	
router2(config-if-serial1/1)#encapsulation ppp	
router2(config-if-serial1/1)#ip address 22.1.1.2 255.255.255.0	
router2(config-if-serial1/1)#ip pim sparse-mode	This command is used to configure the multicast routing protocol. It should be used on all the interfaces that are used for multicast forwarding.
router2(config-if-serial1/1)#interface f0	
router2(config-if-fastethernet0)#ip address 130.255.1.1 255.255.0.0	
router2(config-if-fastethernet0)#ip pim sparse-	This command is used to configure the multicast routing protocol. It should be

mode	used on all the interfaces that are used for multicast forwarding.
router2(config-if-fastethernet0)#exit	

IGMP Monitoring & Debugging

show ip igmp groups
This command is used to display the multicast groups that were learned through Internet Group Management Protocol (IGMP),.

```
show ip igmp groups
```

(Command mode)The privileged user mode.

show ip igmp interface
This command is used to display the IGMP-related information about an interface.

```
show ip igmp interface
```

(Command mode)The privileged user mode.

show ip igmp stat
This command is used to display the statistic information of IGMP messages.

```
show ip igmp stat
```

(Command mode)The privileged user mode.

debug ip igmp
This command is used to display IGMP packets received and sent, and IGMP-group
related events,.

```
debug ip igmp
```

(Command mode)The privileged user mode.

Configure PIM-SM

Overview

PIM-SM (Protocol Independent Multicast, Sparse Mode) applies to the following situations:

Group members are relatively dispersive and their range is relatively broad

The network bandwidth resource is relatively limited

PIM-SM is not dependent on any particular unicast routing protocol, and it demands that all PIM-SM routers can not forward multicast datagrams unless receiving explicit requests. The information of RPs (Rendezvous Point) is announced to all PIM routers by the BSR (BootStrap Router) in the same domain, and the PIM routers calculate the set of group-range-to-RP mapping by it. Via explicit join/prune messages and membership/leave group reports, it is reduced that the network bandwidth occupied by multicast datagrams and PIM-SM control messages.

The PIM-SM constructs a sharing RPT (RP Tree) whose root is the RP, so that multicast datagrams can be transmitted along the RPT. When a multicast receiver expresses its interest in receiving traffic destined for a multicast group, the router, which act on behalf of directly connected host with respect to the PIM-SM protocol, sends a PIM join message to the RP for that multicast group. While the multicast data sender's local router elected as the Designated Router (DR) for that subnet sends register message to the RP, so as to make the sender known by that RP; and the DR (Designated Router) of the receiver sends join message to the RP, so that multicast datagrams can flow along the reverse path of the join message to the receiver.

Using the RPT to forward multicast datagrams can not only reduce much protocol statuses that need be maintained by the router and the processing cost of the router, and but also enhance the flexibility of protocols. The multicast datagrams forwarding can be switched from RPT to SPT (Shortest Path Tree), so as to reduce the transmitting delay.

Commands to Configure PIM-SM

ip pim bsr-candidate

This command is used to configure an interface to be a candidate BSR. The no form of this command is used to cancel the interface to be a candidate BSR.

```
ip pim bsr-candidate interface [hash-mask-length priority]
no ip pim bsr-candidate
```

Syntax	Description
interface	The interface configured as Candidate BSR.
hash-mask-length	The length of the mask in HASH algorithm, its value range is between 0 and 32. The larger the length is, the littler the C-BSR discreteness is.
priority	The priority of the candidate BSR, its value range is between 0 and 255. The candidate BSR with larger priority is elected as the final BSR; if having an equal priority, the router with a larger IP address is elected as the final BSR.

(Default status) The hash-mask-length value is 30 and priority default value is 0

(Command mode) The global configuration mode

In a PIM-SM domain, there is only one elected BSR (Bootstrap Router), which answers for gathering and distributing the information of RPs. Each C-BSR (Candidate BootStrap Router) originates BSMs (BootStrap Messages). Every BSM contains a BSR Priority field. Routers within the domain flood the BSMs which destination IP address is 224.0.0.13 throughout the domain. A C-BSR that hears about a higher-priority (/or a larger IP address if priority is equal) C-BSR than itself then suppresses its sending of further BSMs for some period of time. The single remaining C-BSR becomes the elected BSR, and its BSMs inform all the other routers in the domain that it is the elected BSR.

ip pim query-interval

This command is used to configure the interval for PIM sending Hello messages on an interface. The no form of this command is used to reset the interval to default value.

```
ip pim query-interval seconds
```

```
no ip pim query-interval
```

Syntax	Description
seconds	The interval for PIM sending Hello messages, its value range is between 1 and 65535.

(Default status)The interval is 30 seconds
(Command mode) The interface configuration mode

ip pim dr-priority

This command is used to configure the priority to PIM on an interface. The no form of this command is used to reset the priority to default value.

```
ip pim dr-priority priority
```

```
no ip pim dr-priority
```

Syntax	Description
priority	The priority of the PIM, its value range is between 0 and 4294967294.

(Default status) The priority is 1
(Command mode) The interface configuration mode

ip pim gen-id

The command ip pim gen-id enable is used to configure for PIM sending Hello messages, including generation ID option. The command ip pim gen-id disable is used to configure for PIM sending Hello messages, not including generation ID option.

```
ip pim gen-id { enable | disable }
```

Syntax	Description
enable	PIM sending hello messages including generation ID option.
disable	PIM sending hello messages not including generation ID option.

(Default status)It is for compatibility that PIM sending hello messages not including generation ID option. And PIM sends hello messages including generation ID option by default

(Command mode) The interface configuration mode

```
ip pim rp-candidate
```

This command is used to configure an interface to be a candidate RP. The no form of this command is used to cancel the interface to be a candidate RP.

```
ip pim rp-candidate interface [group-list access-list-number]
```

```
no ip pim rp-candidate interface
```

Syntax	Description
interface	The interface configured as Candidate RP.
access-list-number	The standard IP access list number, its value range is between 1 and 1000. And the range is also the service range of the announced RP.

(Default status) If this command is not followed by the parameter group-list, then it indicates that this RP is the candidate RP for all groups
(Command mode) The global configuration mode

In a PIM-SM domain, a RPT (RP Tree) is constructed by the reverse path of the join messages. Each C-RP (Candidate RP) within a domain sends periodic C-RP-Adv (Candidate-RP Advertisement) messages to the elected BSR. A C-RP-Adv message includes the priority of the advertising C-RP, as well as a list of group ranges for which the candidacy is advertised. In this way, the BSR learns about possible RPs that are currently up and reachable. And then, the elected BSR floods the BSMs (BootStrap Messages) which includes the information of RPs through the domain.

It is suggested that the C-RP should be configured as close as possible to the multicast source whose group it want to function as an RP.

ip pim sparse-mode

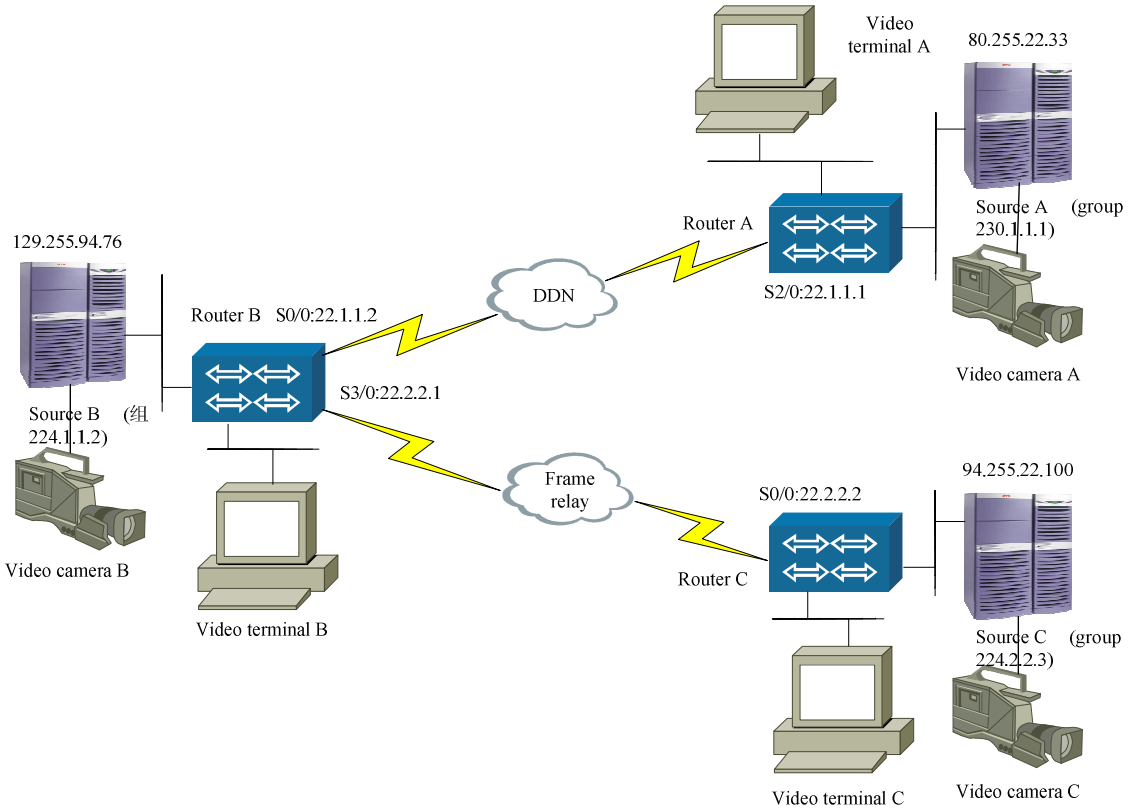
This command is used to configure PIM running on the interface as sparse mode. The no form of this command is used to disable PIM running on the interface as sparse mode.

```
ip pim sparse-mode
no ip pim sparse-mode
```

(Default status) PIM-SM protocol is not running on an interface
(Command mode) The interface configuration mode

PIM-SM Configuration Example

The example is illustrated as the following figure:



The interface s2/0 (22.1.1.1) of Router A adopts PPP protocol to connect with the interface s0/0(22.1.1.2) of the opposite-end Router. The interface s3/0 (22.2.2.1) of the Router B adopts the frame-delay to connect with the interface s0/0(22.2.2.2) of the opposite-end Router C. The three routers connect respectively with different multicast group sources, which serve as the receiving-ends.

The router A configuration is as follows:

Command	Task
routerA#configure terminal	
routerA(config)#ip multicast—routing	Enable the multicast routing forwarding.
routerA(config)#interface s2/0	
routerA(config-if-serial2/0)#physical-layer sync	
routerA(config-if-serial2/0)#clock rate 1800000	
routerA(config-if-serial2/0)#encapsulation ppp	
routerA(config-if-serial2/0)#ip address 22.1.1.1 255.255.255.0	
routerA(config-if-serial2/0)#ip pim sparse-mode	This command is used to configure the multicast routing protocol. It should be used on all the interfaces that are used for multicast forwarding.

routerA(config-if-serial2/0)#interface f0	
routerA(config-if-fastethernet0)#ip address 80.255.22.253 255.255.0.0	
routerA(config-if-fastethernet0)#ip pim sparse-mode	This command is used to configure the multicast routing protocol. It should be used on all the interfaces that are used for multicast forwarding.
routerA(config-if-fastethernet0)#exit	
routerA(config)#ip access-list standard 1	Configure the standard access list.
routerA(config-std-nacl)#permit host 230.1.1.1	Configure the usage range of the access list.
routerA(config-std-nacl)#exit	
routerA(config)#ip pim rp-candidate fastethernet0 group-list 1	Configure the RP proxy of the specified group.
routerA(config)#ip pim bsr-candidate s2/0	Configure the multicast BSR proxy.
routerA(config)#router ospf 1	
routerA(config-ospf)#network 22.1.1.0 0.0.0.255 area 5	
routerA(config-ospf)#network 80.255.0 0.0.255.255 area 5	

The router B configuration is as follows:

Command	Task
routerB(config)# configure terminal	
routerB(config)#ip multicast－routing	Enable the multicast routing forwarding.
routerB(config)#frame-relay switching	
routerB(config)#interface s0/0	
routerB(config-if-serial0/0)#physical-layer sync sync	
routerB(config-if-serial0/0)#encapsulation ppp	
routerB(config-if-serial0/0)#ip address 22.1.1.2 255.255.255.0	
routerB(config-if-serial0/0)#ip pim sparse-mode	This command is used configure the multicast routing protocol. It should be used on all the interfaces that are used for multicast forwarding.
routerB(config-if-serial0/0)#interface f0	
routerB(config-if-fastethernet0)#ip address 129.255.22.253 255.255.0.0	
routerB(config-if-fastethernet0)#ip pim sparse-mode	This command is used to configure the multicast routing protocol. It should be used on all the interfaces that are used for forwarding.
routerB(config-if-fastethernet0)#interface serial3/0	
routerB(config-if-serial3/0)#clock rate 2000000	
routerB(config-if-serial3/0)#ip address 22.2.2.1 255.255.255.0	
routerB(config-if-serial3/0)#ip pim sparse-mode	
routerB(config-if-serial3/0)#encapsulation frame-relay	
routerB(config-if-serial3/0)#frame-relay intf-type dce	
routerB(config-if-serial3/0)#frame-relay interface-dlci 100	
routerB(config-if-serial3/0)#frame-relay map ip 22.2.2.2 100 broadcast	
routerB(config-if-serial3/0)#exit	
routerB(config)#ip access-list standard 1	Configure the standard access list.
routerB(config-std-nacl)#permit host 224.1.1.2	Configure the usage range of the access list.
routerB(config-std-nacl)#exit	
routerB(config)#ip pim rp-candidate fastethernet0 group-list 1	Configure the RP proxy of a specific group.
routerB(config)#router ospf 1	
routerB(config-ospf)#network 22.0.0.0 0.255.255.255 area 5	Enable the OSFP on interfaces s0/0 and s3/0..

routerB(config-ospf)#network 129.255.0.0 0.0.255.255.255 area 5	Enable the OSFP on the interface f0.

The Router C is configured as follows:

Command	Task
routerC(config)# configure terminal	
routerC(config)#ip multicast-routing	Enable the multicast routing forwarding.
routerC(config)#int s0/0	
routerC(config-if-serial0/0)#ip address 22.2.2.2 255.255.255.0	
routerC(config-if-serial0/0)#ip pim sparse-mode	This command is used to configure the multicast routing protocol. It should be used on all the interfaces that are used for multicast forwarding.
routerC(config-if-serial0/0)#encapsulation frame-relay	
routerC(config-if-serial0/0)#frame-relay intf-type dte	
routerC(config-if-serial0/0)#frame-relay interface-dlci 100	
routerC(config-if-serial0/0)#frame-relay map ip 22.2.2.1 100 broadcast	
routerC(config-if-serial0/0)#interface f0	
routerC(config-if-fastethernet0)#ip address 94.255.22.33 255.255.0.0	
routerC(config-if-fastethernet0)#ip pim sparse-mode	This command is used to configure the multicast routing protocol. It should be used on all the interfaces that are used for multicast forwarding.
routerC(config-if-fastethernet0)#exit	
routerC(config)#ip access-list standard 1	
routerC(config-std-nacl)#permit host 224.2.2.3	Configure the usage range of the access list.
routerC(config-std-nacl)#exit	
routerC(config)#ip pim rp-candidate f0 group-list 1	Configure the RP proxy of a specific group.
routerC(config)#router ospf 1	
routerC(config-ospf)#network 22.2.2.0 0.0.0.255 area 5	
routerC(config-ospf)#network 94.255.0.0 0.0.255.255 area 5	

Please implement the configuration strictly according to the Configuration Manual.

What is discussed here is the basic configuration specification for multicast communication. Multicast also supports other link layer protocols and dynamic routing protocols. Their configurations aren't described here.

Monitoring & Debugging PIM-SM

show ip mcache
This command is used to display the mrt kernel cache information.

```
show ip mcache
```

(Command mode) The privileged user mode

show ip mroute
This command is used to display the PIM tree information base.

```
show ip mroute
```

(Command mode) The privileged user mode

show ip pim bsr
This command is used to display the information about the PIM bootstrap router.

```
show ip pim bsr
```

(Command mode) The privileged user mode

show ip pim interface
This command is used to display the information about the PIM interface.

```
show ip pim interface
```

(Command mode) The privileged user mode

show ip pim neighbor
This command is used to display the information about PIM neighbors.

```
show ip pim neighbor
```

(Command mode) The privileged user mode

show ip pim rp
This command is used to display information about the PIM RP (Rendezvous Point).

```
show ip pim rp
```

(Command mode) The privileged user mode

show ip pim rp-hash A.B.C.D
This command is used to display the information of RP to be chosen based on group selected.

```
show ip pim rp-hash A.B.C.D
```

(command mode) The privileged user mode

debug ip pim all
This command is used to display all the PIM debugs.

```
debug ip pim all
```

(Command mode) The privileged user mode

debug ip pim mrt
This command is used to display the PIM multicast route related information.

```
debug ip pim mrt
```

(Command mode) The privileged user mode

debug ip pim packet all
This command is used to display all the PIM packet alternating information.

```
debug ip pim packet all
```

(Command mode) The privileged user mode

debug ip pim packet bootstrap
This command is used to display the PIM bootstrap packet alternating information.

```
debug ip pim packet bootstrap
```

(Command mode) The privileged user mode

debug ip pim packet cand_rp
This command is used to display the PIM candidate RP packet alternating information.

```
debug ip pim packet cand_rp
```

(Command mode) The privileged user mode

debug ip pim packet hello
This command is used to display the PIM hello packet alternating information.

```
debug ip pim packet hello
```

(Command mode) The privileged user mode

debug ip pim packet join-prune
This command is used to display the PIM join-prune packet alternating information.

```
debug ip pim packet join-prune
```

(Command mode) The privileged user mode

debug ip pim packet register
This command is used to display the PIM register packet alternating information

```
debug ip pim packet register
```

(Command mode) The privileged user mode

debug ip pim packet assert

This command is used to display the PIM assert packet alternating information.

```
debug ip pim packet assert
```

(Command mode) The privileged user mode

Configure PIM-DM

Overview

PIM-DM (Protocol Independent Multicast - Dense mode) is a multicast routing protocol. Protocol Independent means that it uses the underlying unicast information base to make decisions regarding RPF interfaces before flooding multicast datagrams to all multicast routers. Dense mode means that it uses the well known flood-and-prune mechanism for multicast routing process.

PIM-DM assumes that when a source starts sending, all downstream systems want to receive multicast datagrams. Initially, multicast datagrams are flooded to all areas of the network. PIM-DM uses RPF to prevent looping of multicast datagrams while flooding. Routers that do not want these multicast datagrams can prune to the upstream.

When upstream router receives this prune message, it sets a prune pending timer, and before this timer expires, routers downstream and attached to the same network who still want to receive these multicast datagrams can send join message to override the former prune message from the neighborly router.

If the upstream router receives the join message, it will keep on forwarding the multicast datagrams to this network, and if the network do not have any group members and no join message, PIM-DM will prune off the forwarding branch by instantiating prune state. Prune state has a finite lifetime. When that lifetime expires, data will again be forwarded down the previously pruned branch.

Prune state is associated with an (S,G) pair. When a new member for a group G appears in a pruned area, a router can "graft" toward the source S for the group, thereby turning the pruned branch back into a forwarding branch.

PIM-DM has following features:

Protocol independent by using unicast informaiton base for RPF checking

periodicly flooding and pruning

Configuring PIM-DM

Command	Description	Command mode
ip pim dense-mode	* Enables PIM dense mode on the interface.	config-if-××
ip pim query-interval seconds	PIM-DM query interval	config-if-××
ip pim state-refresh origination-interval seconds	PIM-DM state-refresh origination-interval	config-if-××
ip pim neighbor-filter {access-list num | access-list name}	PIM-DM neighbor filter	config-if-××
ip pim state-refresh disable	Disable PIM-DM state refresh	config
ip pim sparse-dense-mode	Enables PIM to operate in sparse or dense mode, depending on the group.	config-if-××

1, Asterisk (' * ') before a command means configuration example for this command is given in the configuration example section.
2, Command mode is the mode under which the command can be executed, such as config, config-if-××(interface name) config-××(protocol name)

ip pim dense-mode
This command is used to configure PIM on an interface to be in dense mode, the no form of this command is used to disable the PIM-DM running on an interface.

```
ip pim dense-mode
no ip pim dense-mode
```

(Default status) PIM-DM protocol is not running on an interface.
(command mode) The interface configuration mode

ip pim query-interval
This command is used to configure the interval to PIM send Hello messages on an interface. The no form of this command is used to reset the interval to default value.

```
ip pim query-interval seconds
no ip pim query-interval
```

Syntax	Description
seconds	The interval to send PIM Hello messages. It can be a number from 1 to 65535

(Default status)30 seconds
(command mode) The interface configuration mode

ip pim state-refresh origination-interval
This command is used to configure the interval for PIM-DM state refresh contro messages on PIM router. The no form of this command is used to reset the interval to default value.

```
ip pim state-refresh origination-interval seconds
no ip pim state-refresh origination-interval
```

Syntax	Description
seconds	The number of seconds between PIM-DM state refresh control messages, and the available range is from 1 to 100 seconds.

(Default status)60 seconds
(command mode) The interface configuration mode

ip pim neighbor-filter

This command is used to configure pim to filter its neighbors on the attached networks, only messages from neighbors permitted by the access list can be accepted. The no form of this command is used to disable the neighbor fitlering control.

```
ip pim neighbor-filter {access-list num | access-list name}
no ip pim neighbor-filter
```

Syntax	Description
access-list num | access-list name	Standard access list number or name

(Default status)no neighbor filter control and all the messages from all the neighbors is accepted.
(command mode) The interface configuration mode
Note: This command uses only standard access list.

ip pim state-refresh disable

```
ip pim state-refresh disable
no ip pim state-refresh disable
```

This command is used to disable the processing and forwarding of PIM-DM state refresh control messages on a PIM router. The no form of this command is used to enable state refresh message processing and forwarding.

(Default status) State refresh mechanism is enabled on the router
(command mode)The global configuration mode

ip pim sparse-dense-mode

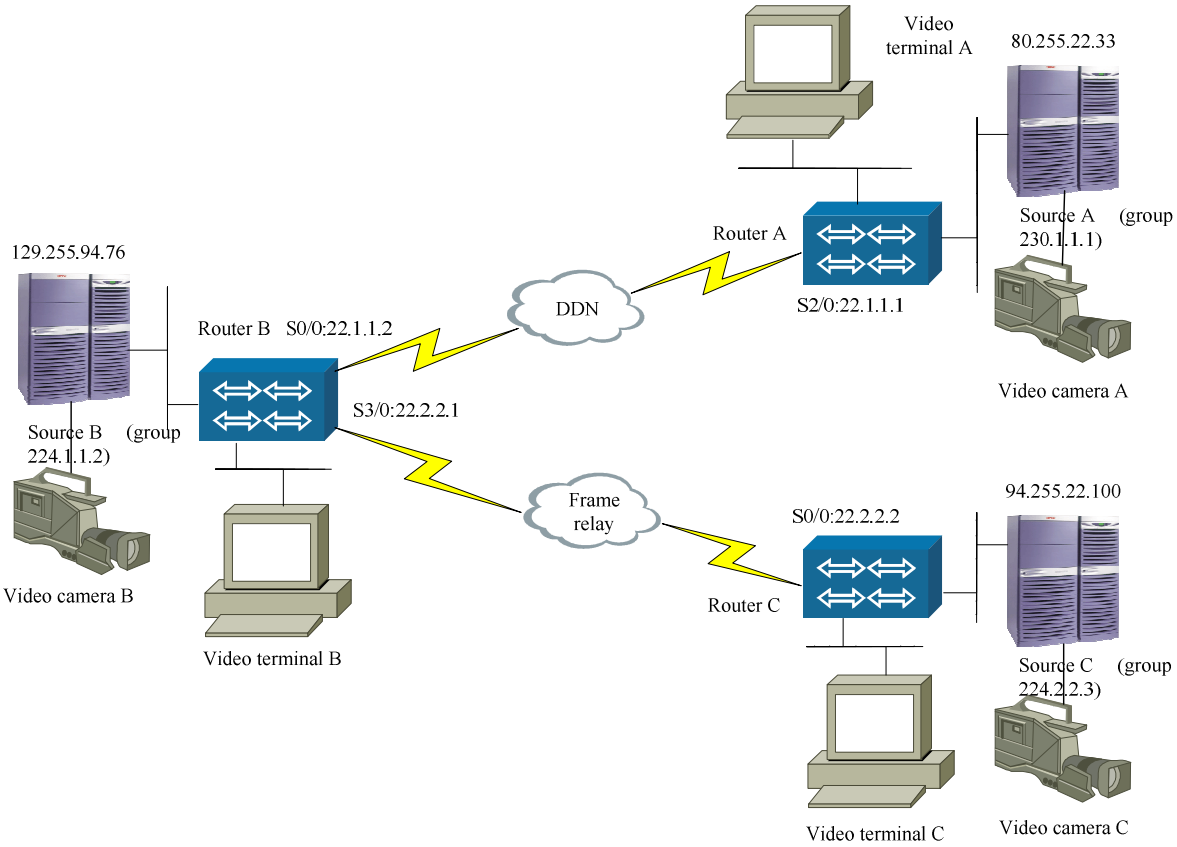
Enable PIM-SM and PIM-DM auto adaptive mode. Running under this mode the interface is default to PIM-DM, and switch to PIM-SM by receiving bootstrap packet. The no form of this command is used to diable interface running this mode.

```
ip pim sparse-dense-mode
no ip pim sparse-dense-mode
```

(Default status) This mode is not running on an interface
(command mode) The interface configuration mode
Note: If one interface use this mode, all interfaces should also use this mode.
If the router is configured to be a BSR candidate, all interfaces will switch to PIM-SM mode, and then if its BSR candidate role is cancled, all interfaces will switch back to PIM-DM again when the RP expires.

PIM-DM Configuration Example

The example is illustrated with the following figure:



Interface s0/2 (22.1.1.1) of routerA connects with interface s0/0(22.1.1.2) of routerB through the PPP network. Interface s3/0 (22.1.1.1) of routerB connects with interface s0/0(22.1.1.2) of routerC through the FR (Frame relay) network. Three video servers connecting to each routers respectively serve as the source and also serve as members of this group.

Configurations of RouterA:

Command	Description
RouterA#configure terminal	
RouterA(config)#ip multicast-routing	Enable multicast routing forwarding
RouterA(config)#interface s2/0	
RouterA(config-if-serial2/0)#physical-layer sync	
RouterA(config-if-serial2/0)#clock rate 2000000	
RouterA(config-if-serial2/0)#encapsulation ppp	
RouterA(config-if-serial2/0)#ip address 22.1.1.1 255.255.255.0	
RouterA(config-if-serial2/0)#ip pim dense-mode	This command is used to configure the multicast routing protocol. It should be used on all the interfaces that are used for multicast forwarding.
RouterA(config-if-serial2/0)#interface f0	
RouterA(config-if-fastethernet0)#ip address 80.255.22.253 255.255.0.0	
RouterA(config-if-fastethernet0)#ip pim dense-mode	This command is used to configure the multicast routing protocol. It should be used on all the interfaces that are used for multicast forwarding.
RouterA(config-if-fastethernet0)#exit	
RouterA(config)#router ospf 1	
RouterA(config-ospf)#network 22.1.1.0 0.0.0.255 area 5	
RouterA(config-ospf)#network 80.255.0 0.0.255.255 area 5	

Configuration of RouterB:

Command	Description
RouterB(config)# configure terminal	
RouterB(config)#ip multicast-routing	Enable multicast routing forwarding
RouterB(config)#frame-relay switching	
RouterB(config)#interface s0/0	
RouterB(config-if-serial0/0)#physical-layer sync sync	
RouterB(config-if-serial0/0)#encapsulation ppp	
RouterB(config-if-serial0/0)#ip address 22.1.1.2 255.255.255.0	
RouterB(config-if-serial0/0)#ip pim dense-mode	This command is used to configure the multicast routing protocol. It should be used on all the interfaces that are

	used for multicast forwarding.
RouterB(config-if-serial0/0)#interface f0	
RouterB(config-if-fastethernet0)#ip address 129.255.22.253 255.255.0.0	
RouterB(config-if-fastethernet0)#ip pim dense-mode	This command is used to configure the multicast routing protocol. It should be used on all the interfaces that are used for multicast forwarding.
RouterB(config-if-fastethernet0)#interface serial3/0	
RouterB(config-if-serial3/0)#clock rate 2000000	
RouterB(config-if-serial3/0)#ip address 22.2.2.1 255.255.255.0	
RouterB(config-if-serial3/0)#ip pim dense-mode	
RouterB(config-if-serial3/0)#encapsulation frame-relay	
RouterB(config-if-serial3/0)#frame-relay intf-type dce	
RouterB(config-if-serial3/0)#frame-relay interface-dlci 100	
RouterB(config-if-serial3/0)#frame-relay map ip 22.2.2.2 100 broadcast	
RouterB(config-if-serial3/0)#exit	
RouterB(config)#router ospf 1	
RouterB(config-ospf)#network 22.0.0.0 0.255.255.255 area 5	Cover the network of s0/0 and s3/0 to OSPF area 5
RouterB(config-ospf)#network 129.255.0.0 0.0.255.255.255 area 5	Cover the network of f0 to OSPF area 5

RouterC configuration:

Command	Description
RouterC(config)# configure terminal	
RouterC(config)#ip multicast-routing	Enable multicast routing forwarding
RouterC(config)#int s0/0	
RouterC(config-if-serial0/0)#ip address 22.2.2.2 255.255.255.0	
RouterC(config-if-serial0/0)#ip pim dense-mode	This command is used to configure the multicast routing protocol. It should be used on all the interfaces that are used for multicast forwarding.
RouterC(config-if-serial0/0)#encapsulation frame-relay	
RouterC(config-if-serial0/0)#frame-relay intf-type dte	
RouterC(config-if-serial0/0)#frame-relay interface-dlci 100	
RouterC(config-if-serial0/0)#frame-relay map ip 22.2.2.1 100 broadcast	
RouterC(config-if-serial0/0)#interface f0	
RouterC(config-if-fastethernet0)#ip address 94.255.22.33 255.255.0.0	
RouterC(config-if-fastethernet0)#ip pim dense-mode	This command is used to configure the multicast routing protocol. It should be used on all the interfaces that are used for multicast forwarding.
RouterC(config-if-fastethernet0)#exit	
RouterC(config)#router ospf 1	
RouterC(config-ospf)#network 22.2.2.0 0.0.0.255 area 5	
RouterC(config-ospf)#network 94.255.0.0 0.0.255.255 area 5	

PIM-DM Monitoring & Debugging

show ip pim interface

This command is used to display the PIM-related information of an interface.
`show ip pim interface`
(command mode) The privileged user mode.

show ip pim neighbor
This command is used to list the PIM neighbors discovered by the router and display their information.
`show ip pim neighbor`
(command mode) The privileged user mode.

debug ip pim all
This command is used to display all the PIM debugs
`debug ip pim all`
(command mode) The privileged user mode.

debug ip pim mrt
This command is used to display PIM multicast route related information.
`debug ip pim mrt`
(command mode) The privileged user mode.

debug ip pim packet all
This command is used to display all the PIM messages received and sent .
`debug ip pim packet all`
(command mode) The privileged user mode.

debug ip pim packet hello
This command is used to display PIM hello messages received and sent.
`debug ip pim packet hello`
(command mode) The privileged user mode.

debug ip pim packet join-prune
This command is used to display PIM join and prunes messages received and sent.
`debug ip pim packet join-prune`
(command mode) The privileged user mode.

debug ip pim packet graft
This command is used to display PIM graft messages received and sent.
`debug ip pim packet graft`
(command mode) The privileged user mode.

debug ip pim packet assert
This command is used to display PIM assert messages received and sent.
`debug ip pim packet assert`
(command mode) The privileged user mode.

debug ip pim packet state-refresh
This command is used to display PIM state refresh messages received and sent.
debug ip pim packet state-refresh
(command mode) The privileged user mode.

Configuring DVMRP

Overview

Distance Vector Multicast Routing Protocol (DVMRP), the first multicast routing protocol applied popularly, uses a distance vector distributed routing algorithm same as RIP protocol and adds the support for multicast. DVMRP routers are discovered dynamically by sending Neighbor Probe Messages on local multicast capable network interfaces and tunnel pseudo interfaces, and then, route exchange of unicast paths is used for upstream routers to determine if any downstream routers depend on them for forwarding from particular source networks.

DVMRP can be summarized as a "broadcast & prune" multicast routing protocol. it uses the a technique called Reverse Path Multicasting to dynamically generate IP Multicast delivery trees. When a datagram arrives on an interface, the reverse path to the source of the datagram is determined by examining a DVMRP routing table of known source networks. If the datagram arrives on an interface that would be used to transmit datagrams back to the source, then it is forwarded to the appropriate list of downstream interfaces. Otherwise, it is not on the optimal delivery tree and should be discarded. In this way duplicate packets can be filtered when loops exist in thenetwork topology. The source specific delivery trees are automatically pruned back as group membership changes or routers determine that no group members are present. This keeps the delivery trees to the minimum branches necessary to reach all of the group members. In order to remove old prune state information for (source network, group) pairs that are no longer active, it is necessary to limit the life of a prune and periodically resume the broadcasting procedure. When the prune lifetime expires, the interface is joined back onto the multicast delivery tree. New sections of the tree can also be added dynamically as new members join the multicast group by grafting the new sections onto the delivery trees.
DVMRP has the following features:

Based on distance vector distributed routing algorithm;

Route updating periodically(per 60 seconds)

The Infinity metric is defined to be 32. (16 for RIP)

Use Poison Reverse to determine downstream dependencies

Route exchange uses Classless Inferdomain Routing, updating route by report contianing source network/mask pairs.

Configuring Commands

ip dvmrp enable
This command is used to enable DVMRP protocol on an interface. The no form of this command is to disable the DVMRP on the interface.

```
ip dvmrp enable
```

```
no ip dvmrp
```

(Default status) DVMRP is not running on an interface
(command mode) The interface configuration mode

ip dvmrp in-metric
This command is used to configure the incoming metric of a DVMRP interface. The no form of this command is used to reset the value of incoming metric to default.

```
ip dvmrp in-metric num
```

```
no ip dvmrp in-metric
```

Syntax	Description
num	Incoming metric value (1～31)

(Default status)1
(command mode) The interface configuration mode

ip dvmrp out-metric
This command is used to configure the outcoming metric of a DVMRP interface. The no form of this command is used to reset the value to default.

```
ip dvmrp out-metric num
```

```
no ip dvmrp out-metric
```

Syntax	Description
num	Outcoming metric value(0～31)

(Default status)0
(command mode) The interface configuration mode

ip dvmrp prune-time

This command is used to configure the life time of DVMRP pruning state. The no form of this command is used to reset the life time to default value.

```
ip dvmrp prune-time seconds
```

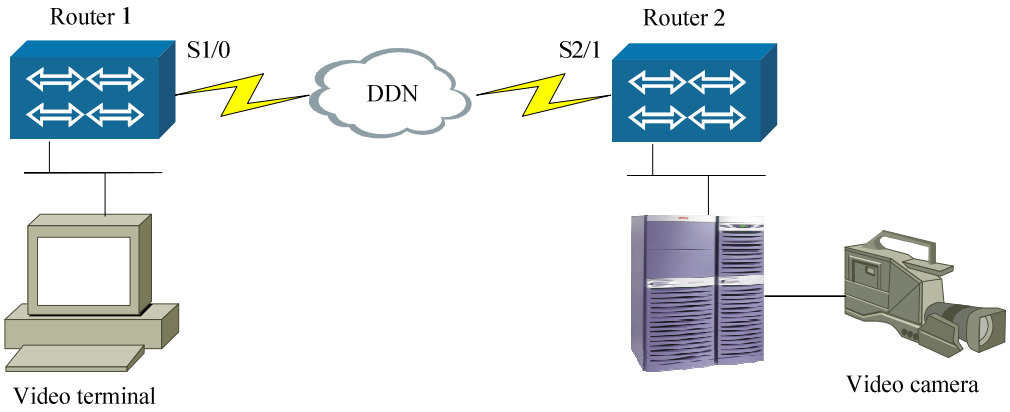
```
no ip dvmrp prune-time
```

Syntax	Description
seconds	Life time of Prune state(1～7200 seconds)

(Default status)7200 seconds
(command mode) The interface configuration mode

DVMRP Configuration

The example is displayed with the following figure:



As shown in the figure above, interface s1/0 of router1 connects to interface s1/2 of router2 through PPP network. The Ethernet interfaces of the two routers respectively connect with two PCs on of which serves as the multicast source and the other of which serves as the multicast group member.

Configurations of Router1:

Syntax	Description
router1#configure terminal	
router1 (config)#ip multicast—routing	Enable multicast routing forwarding.
router1 (config)# interface fastethernet0	
router1 (config-if-fastethernet0)# ip address 131.255.127.3 255.255.0.0	
router1 (config-if-fastethernet0)# ip dvmrp enable	This command is used to configure the multicast routing protocol. It should be used on all the interfaces that are used for multicast forwarding.
router1 (config-if-fastethernet0)# interface serial1/0	
router1 (config-if-serial1/0)# physical-layer sync	
router1 (config-if-serial1/0)#encapsulation ppp	
router1 (config-if-serial1/0)# ip address 8.0.0.1 255.0.0.0	
router1 (config-if-serial1/0)# ip dvmrp	This command is used to configure the multicast routing protocol. It should be used on all the interfaces that are used for multicast forwarding.
router1 (config-if-serial1/0)# exit	

Configurations of Router2:

Syntax	Description
Router2#configure terminal	
Router2(config)#ip multicast—routing	Enable multicast routing forwarding.
Router2(config)# interface fastethernet0	
Router2(config-if-fastethernet0)# ip address 151.255.127.6 255.255.0.0	
Router2(config-if-fastethernet0)# ip dvmrp enable	This command is used to configure the multicast routing protocol. It should be used on all the interfaces that are used for multicast forwarding.
Router2(config-if-fastethernet0)# interface serial2/1	
Router2(config-if-serial2/1)# physical-layer sync	
Router2(config-if-serial2/1)#clock rate 2000000	
Router2(config-if-serial2/1)#encapsulation ppp	
Router2(config-if-serial2/1)# ip address 8.0.0.26 255.0.0.0	
Router2(config-if-serial2/1)# ip dvmrp enable	This command is used to configure the multicast routing protocol. It should be used on all the interfaces that are used for multicast forwarding.
Router2(config-if-serial2/1)# exit	

DVMRP Monitoring & Debugging

show ip dvmrp interface
This command is used to display the DVMRP-related information of an interface.
`show ip dvmrp interface`
(Command mode)The privileged user mode.

show ip dvmrp neighbor
This command is used to list the DVMRP neighbors discovered by the router and display their information.
`show ip dvmrp neighbor`
(Command mode)The privileged user mode.

show ip dvmrp route
This command is used to list the DVMRP routes learned.
`show ip dvmrp route`
(Command mode)The privileged user mode.

debug ip dvmrp all
This command is used to display all the DVMRP debugs.
`debug ip dvmrp all`
(Command mode)The privileged user mode.

debug ip dvmrp peer
This command is used to display DVMRP probe messages received and sent.
`debug ip dvmrp peer`
(Command mode)The privileged user mode.

debug ip dvmrp prune
This command is used to display DVMRP prune messages received and sent.
`debug ip dvmrp prune`
(Command mode)The privileged user mode.

debug ip dvmrp route
This command is used to display DVMRP route report messages received and sent.
`debug ip dvmrp route`
(Command mode)The privileged user mode.

debug ip dvmrp mrt
This command is used to display multicast route related information.
`debug ip dvmrp mrt`
(command mode) The privileged user mode

Configuring VRRP

VRRP(Virtual Router Redundancy Protocol) can provide a gateway backup. The main contents of this section are listed as follows:

Related VRRP configuration commands

An example of VRRP configuration

Monitoring and debugging VRRP

VRRP Configuration Commands

Vrrp enable/disable

The command is used to enable vrrp and specify a virtual IP address. The negation of the command is used to disable vrrp.

```
vrrp vrid ip ip-address
no vrrp vrid
```

Syntax	Description
vrid	Specify a vird number whose value range is from 1 to 255.
ip-address	Specify a virtual IP address.

(By default) Vrrp is disabled.
(Command mode)the interface configuration mode

A virtual IP address and a primary address of the interface should be in the same network segment.

Vrrp authentication

The command is used to enable/disable vrrp simple text authentication.

```
vrrp vrid authentication text string
no vrrp vrid authentication
```

Syntax	Description
vrid	Specify a vird number whose value range is from 1 to 255.
string	The authentication password. The maximal length is 8 (by character).

(By default) The authentication is enabled.
(Command mode)the interface configuration mode

The command cannot be configured until VRRP is enabled.

Vrrp preempt

The command is used to enable/disable vrrp preempt.

```
vrrp vrid preempt
no vrrp vrid preempt
```

Syntax	Description
vrid	Specify a vird number whose value range is from 1 to 255.

(By default) the vrrp preempt is disabled.
(Command mode)the interface configuration mode

The command cannot be configured until VRRP is enabled.

Vrrp priority

The command is used to configure vrrp priority.

```
vrrp vrid priority priority
no vrrp vrid priority
```

Syntax	Description
vrid	Specify a vird number whose value range is from 1 to 255.
priority	Specify a vird priority whose value range is from 1 to 254.

(By default) priority:100。
(Command mode)the interface configuration mode

The command cannot be configured until VRRP is enabled.

Vrrp timer

The command is used to configure the period of sending VRRP packets.

```
vrrp vrid timer_advertise advertise-time
no vrrp vrid timers
```

Syntax	Description
vrid	Specify a vird number whose value range is from 1 to 255.
advertise-time	Specify the period (by second) of sending vrrp packets and its value range is from 1 to 255.

(By default) advertise-time:1。
(Command mode)the interface configuration mode

The command cannot be configured until VRRP is enabled.

Vrrp interface monitoring

The command is used to configure the interface vrrp monitors.

```
vrrp vrid track interface [decrement]
no vrrp vrid track interface
```

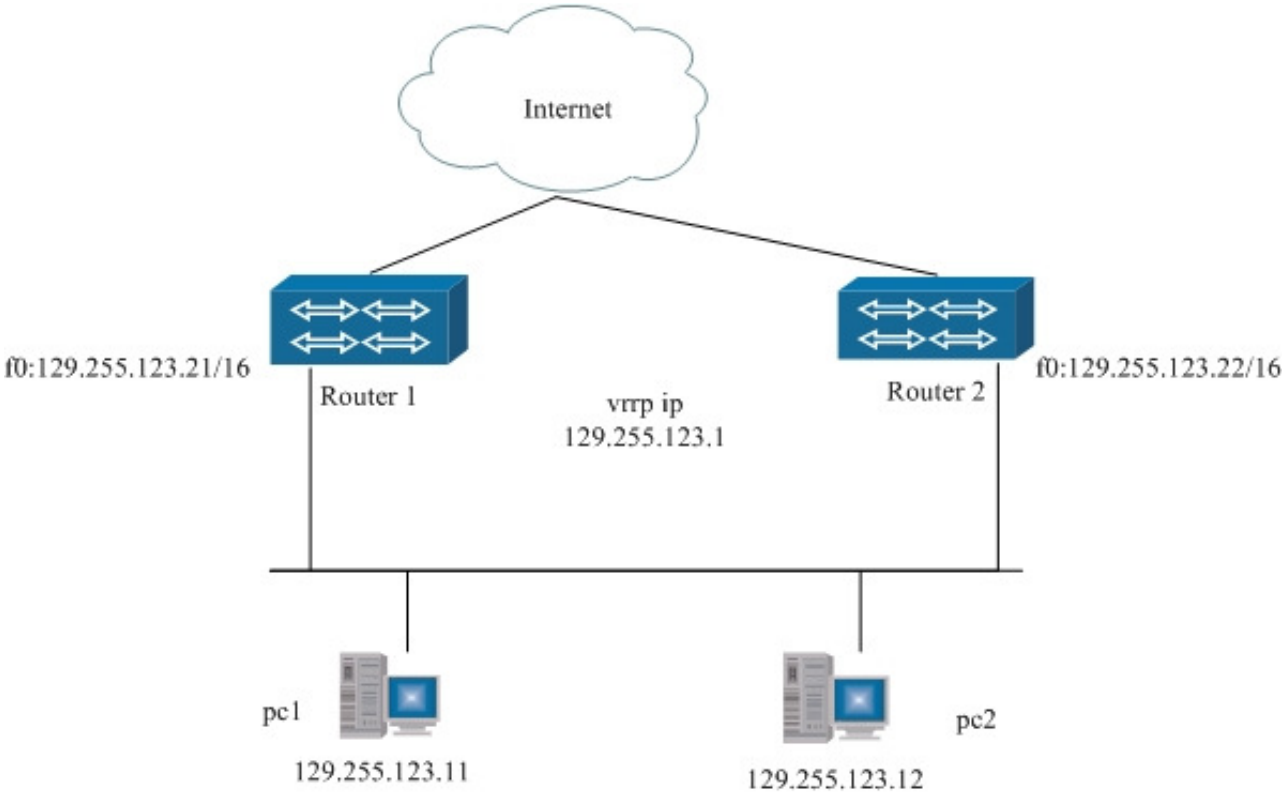
Syntax	Description
vrid	Specify a vird number whose value range is from 1 to 255.
interface	Specify an interface for monitoring.
decrement	Specify the priority decrement.

(By default) An interface is not be monitored.
(Command mode)the interface configuration mode

The command cannot be configured until VRRP is enabled.

if no decrement is specified, the default value of priority decrement is 10.

VRRP Configuration Example



As shown in figure above, pc1 and pc2 connect with Internet respectively via router1 and router2, and their default gateway is 129.255.123.1.

The basic configuration of VRRP is described as follows:

Router1 is configured as follows:

Command	Task
router1#configure terminal	Enter the global configuration mode.
router1(config)#interface fastethernet0	Enter an Ethernet interface.
router1(config-if-fastethernet0)#ip address 129.255.123.21 255.255.0.0	Configure an IP address.
router1(config-if-fastethernet0)#vrrp 1 ip-address 129.255.123.1	Configure VRRP group-number and virtual IP address.
router1(config-if-fastethernet0)#vrrp 1 priority 105	Set the VRRP priority.

Router2 is configured as follows:

Command	Task
router2#configure terminal	Enter the global configuration mode.
route2(config)#interface fastethernet0	Enter an Ethernet interface.
router2(config-if-fastethernet0)#ip address 129.255.123.22 255.255.0.0	Configure an IP address.
router2(config-if-fastethernet0)# vrrp 1 ip-address 129.255.123.1	Configure VRRP group-number and virtual IP address.

Monitoring & Debugging VRRP

show vrrp

The command is used to display all local VRRPs.

```
show vrrp
```

(Command mode)the privileged user mode

debug vrrp event

The command is used to display/close the event information about VRRP running.

```
debug vrrp event
no debug vrrp event
```

(Command mode)the privileged user mode

debug vrrp packet
The command is used to enable/disable the switch of VRRP packet debugging information.

```
debug vrrp packet
no debug vrrp packet
```

(Command mode)the privileged user mode

debug vrrp timer
The command is used to enable/disable the switch of VRRP timer debugging information.

```
debug vrrp timer
```

`no debug vrrp timer`
(Command mode)the privileged user mode

DDR & Interface Backup

This chapter explains how to configure a Signamax Router to perform the remote dialer access via PSTN and ISDN (Integrated Services Digital Network).

The main topics addressed in this chapter are:

Dialer backup

The configuration of DDR dialer

Dialer prototype

Dialer Backup

Built-in Frequency-band MODEM Configuration

A built-in frequency-band modem in a Signamax router supports several dialer modes, such as synchronism, asynchronic, dialer line, and leased line etc. This section explains how to configure the built-in frequency-band modem in a Signamax router to perform the remote dialer function.

Commands

Configuring modem parameters

```
router(config-if-XXX)#modem ?
```

Command	Description
async-mode	Configures it in the asynchronous mode, including buffer asynchronic, direct asynchronic and error-correct asynchronic. (If you add a "?" behind the command modem async-mode, you can see the prompt of the next step. Of course, you can get help of all the configuration via using "?")
clock-mode	In the synchronous mode, internal clock, external clock and slave clock can be configured. In the asynchronous mode, it is unnecessary to configure the clock.
clock-rate	In the synchronous mode, modem circuitry rate is configured. (In the asynchronous mode, the command speed is used to configure interface rate)
outer	The command is used to configure an outer modem, while it isn't used to configure a built-in modem.
party	The command is used to configure modem as originator or answer.
disable	Disable modem.
enable	Enable modem.
line	Configure modem as the leased line mode
v25bis enable	Forbidden AT command, active v.25bits command

The above commands can be used similarly when MP336/56MODEM is connected externally

Configuring the telephone number of a called user

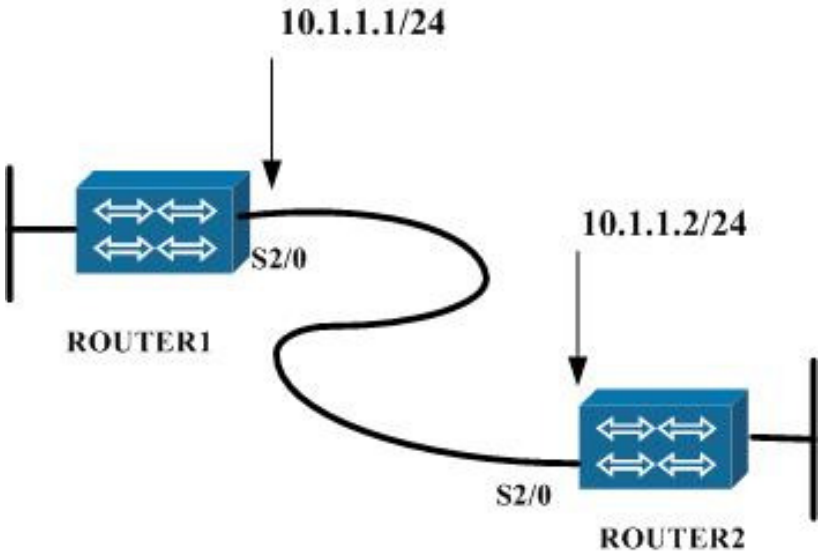
```
Router (config-if-XXX) #dialer string  phone number
```

Command	Description
dialer string <number>	Configures the telephone number of the called side. The number can only be composed of Arabic numerals (When the exterior line of the built-in modem is a dialer line, the number needs to be configured; when the exterior line of the modem is a leased line, the number does not need to be configured.)

Many called numbers can be configured. After this, when the router dials a number, it will adopt the polling dialer (Namely, the first number is dialed; if it is busy, then the second number is dialed in turn)

Usage of Configuring Commands

A leased line mode



Leased line mode

The built-in frequency-band MODEM is configured on the interface interface serial2/0 of router1 and router2. And the leased line mode is configured.

router1 is a caller that uses the internal clock, while router2 is the answer that uses the slave clock. The line speed is 9600.

Router1 configuration is as follows:

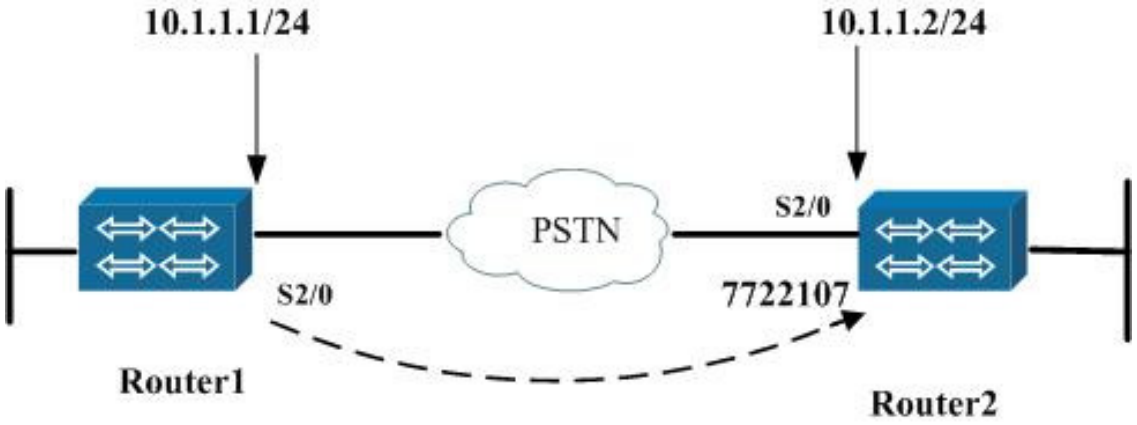
Command	Details
router1# configure terminal	
router1(config)#interface serial2/0	Enters the interface configuration mode with built-in frequency-band MODEM.
router1(config-if-serial2/0)#ip address 10.1.1.1 255.255.255.0	Configures the IP address.
router1(config-if-serial2/0)# encapsulation PPP	Encapsulates PPP protocol.
router1(config-if-serial2/0)#modem clock-mode internal	Configures the MODEM clock as the internal, synchronous mode : internal clock (internal); external clock (external); slave clock (slave).
router1(config-if-serial2/0)#modem clock-rate 9600	Configures the line speed as 9600.
router1(config-if-serial2/0)#modem line leased	Configures MODEM as the leased line mode.
router1(config-if-serial2/0)#modem party originate	Configures MODEM as a caller.
router1(config-if-serial2/0)#modem enable	Enables the MODEM configuration to become effective
router1(config-if-serial2/0)#exit	

Router2 configuration is as follows:

Command	Task
router2# configure terminal	
router2(config)#interface serial2/0	Enters the interface configuration mode with built-in frequency-band MODEM.
router2(config-if-serial2/0)#ip address 10.1.1.2 255.255.255.0	
router2(config-if-serial2/0)# encapsulation PPP	Encapsulates PPP protocol.
router2(config-if-serial2/0)#modem clock-mode slave	Configures it as the slave clock mode
router2(config-if-serial2/0)#modem clock-rate 9600	
router2(config-if-serial2/0)#modem line leased	
router2(config-if-serial2/0)#modem party answer	Configures MODEM as an answer.
Router2(config-if-serial2/0)#modem enable	
Router2(config-if-serial2/0)#exit	

The dialer mode:

The above are the configuration of the built-in modem with a leased line mode and its simple explanation. Then, we will simply explain the configuration of the dialer mode as follows:



Dialer mode

The built-in frequency-band MODEM is configured on the interface serial2/0 of router1 and router2. And the dialer mode is configured.

Router1 is a caller and router2 is an answer.

The configuration (synchronous mode)

Router1 configuration is as follows:

Command	Task
router1#configure terminal	
router1(config)#interface serial2/0	Enters the interface configuration mode with built-in frequency-band MODEM.
router1(config-if-serial2/0)#ip address 10.1.1.1 255.255.255.0	Configures IP address.
router1(config-if-serial2/0)# encapsulation PPP	Encapsulates PPP protocol.
router1(config-if-serial2/0)#physical-layer sync	Configures it as the synchronous mode.
router1(config-if-serial2/0)#modem clock-mode internal	Configures it as the internal clock mode.
router1(config-if-serial2/0)#modem clock-rate 33600	Configures MODEM speed.
router1(config-if-serial2/0)#modem party originate	Configures MODEM as a caller.
router1(config-if-serial2/0)# dialer string 7722107 dialer string 7721679	Configures the telephone number of the opposite terminal.
router1(config-if-serial2/0)# modem enable	Enables the MODEM.
router1(config-if-serial2/0)#exit	

router2

Command	Task
router2#configure terminal	
router2(config)#interface serial2/0	Enters the interface.
router2(config-if-serial2/0)#ip address 10.1.1.2 255.255.255.0	Configures the IP address.
router2config-if-serial2/0)#physical-layer sync	Configures it as the synchronous mode.
router2(config-if-serial2/0)#encapsulation PPP	Encapsulates PPP protocol.
router2(config-if-serial2/0)#modem party answer	Configures it as an answer.
router2config-if-serial2/0)#modem clock-rate 33600	Configures MODEM ratio.
router2(config-if-serial2/0)#modem enable	Enables the MODEM.
router2(config-if-serial2/0)#exit	

The configuration of the asynchronous mode is as follows:

Router1 configuration	Router2 configuration
interface serial3	interface serial3
physical-layer async	physical-layer async
speed 115200	speed 115200
databits 8	databits 8
stopbits 1	stopbits 1
parity none	parity none
flow-control none	flow-control none
encapsulation ppp	encapsulation ppp
ip address 10.0.0.1 255.0.0.0	ip address 10.0.0.2 255.0.0.0
dialer string 8005	
modem party originate	modem party answer
modem enable	modem enable
Exit	Exit

When using the leased line mode, MODEM keeps on calling (or answering) until it is connected.

If it is an outer modem, modem outer needs to be configured.

Dialer Script

There are many types of modems for sale in today's market. Although they all support the AT instructions set, there are some differences with regards to their implementation.

To provide more flexibility, a dialer language, called dialer scripts, can be established. The script language has the following features:

The script is composed of some ordered set of some defined keywords, sent strings and expected strings.

Strings can be separated by a blank.

A script command doesn't match upper/lower case. It begins with at or AT and represents that what will be sent is an AT command.

The AT instructions set of different companies may be different, so they should be configured by referring to their accessory specifications.

Editing script

```
router (config)#chat-script  script-name script
script name script content
```

For example, configuring the following script:

```
router (config)#chat-script  Signamax  at&f&k3%c3  atm1
```

In this example, the script name is Signamax and the script contents are at&f&k3%c3 and atm1.

Using the command no to delete the script:

```
router (config)# no chat-script  script-name
```

Configure the Modem script that is executed when a connection needs to be established:

```
router(config-if- XXX)# script  connection  script-name
```

Script-name is configured in the global configuration mode: chat-script script-name, which is the script-name in the script. Its purpose is to connect the AT command with related interface.

When the router needs the modem to call out, it will send the script designated by script-name to the modem first, and then it will initialize configuration of the modem.

When all of the modem scripts have been executed successfully, the initialization finishes. After this, the router sends the dialer string to the modem to call the opposing party.

Similarly, when the modem is configured as modem party answer, and when the opposite terminal sends call and the local-end receives a bell-shaking signal, the router will also sends the modem initialization script to configure the modem. When all configuration succeeds, the modem will negotiate with the opposite modem, and the router will enter the status Answering incoming call to wait for the connection of modem. When the modem has succeeded in connecting, it will enter the phase of the link layer negotiation.

```
Use no script connection to cancel the feature.
router(config-if-serial2/0)#no script  connection
```

If no script is configured for the modem, then the modem will start the default script set by the system. Because the AT scripts supported by various companies have some differences, it is recommended that users configure the script for a modem via referring to the modem usage manual of its company so that the modems of different companies and types can work in better harmony with the router.

You can use the debug commands (for example, debug modem s2) to examine the default script.

Scripts in common use MP336 series

AT commands in common use	The explanation
&QnDn (the default is D2) Functions of all kinds of compressions triggered respectively when DTR hops from ON to OFF. Notice that D0 can be only useful to the Q1 mode, while D1, D2 and D3 are useful to all the compression modes.	&D0 : simple hangup of the modem; &D1 : changing from the data mode to the command mode; &D2 : the modem hangs up and closes the auto-answer; &D3 : the modem reset
&Qn (The default is &Q5)	&Q0: Using the direct asynchronous mode &Q1: Using the synchronous connection mode (the command mode being of asynchronic) &Q5: Using the error asynchronous mode &Q0: Using the common asynchronous mode (with the function of rate buffer) Result code:n=0-6,OK； other value,ERROR。
&QnCn (controled by DCD) (The default is &C1)	&C0: DCD being ON all the time; &C1: DCD indicating the status of the carrier wave; Result code: n=0,1, OK; other values, ERROR.
&Kn (the flow control modes between DCE and DTE) (The default is &K3)	&K0: no flow control mode &K3: the RTS/CTS flow control mode (the default) &K4: the XON/XOFF flow control mode &K5: transparent XON/XOFF flow control mode &K6: the XON/XOFF and RTS/CTS simultaneous control

	mode The result code: n=0,3 to 6, OK; other values, ERROR
&Ln Functions of the leased (special) line	&L0: the command mode; &L2: the auto leased line mode &L3: the auto dialer line mode &L5: the dialer backup working mode
%Cn (Limit to the error control mode) (The default is &C3)	&C0: No compression &C1: Enable the MNP5 compression mode &C2: Enable the V.42bis compression mode &C3: Enable the V.42bsi compression and the MNP5 compression mode Result code: n=0 to 3, OK; other values, ERROR Notice: & and % are different.
%En Controlling and monitoring line quality (The default is &E0)	&E0: without monitoring line quality, using auto retraining &E1: monitoring line quality, performing auto retraining &E2: monitoring line quality, automatically promoting/depressing speed according to the quality status • Automatically promote/depress speed that is chosen in the V.32bis/V.32 modulation speed. When speed is lower than 4800bps, it can't be promoted/depressed, instead, it can auto retrain only. (This is used in dialer line only) The result code: n=0 to 2, OK; other values, ERROR
&F	The modem loads the factory default configuration.

When the command AT is configured, it should be done according to the instructions of related company.

When different modulation protocols are chosen, the appropriate one should be done according to the different line status. For example, both V.34 protocol and V.22bis support the speed 2400. But in fact, the same speed using different modulation protocols will have different effect because of the line status.

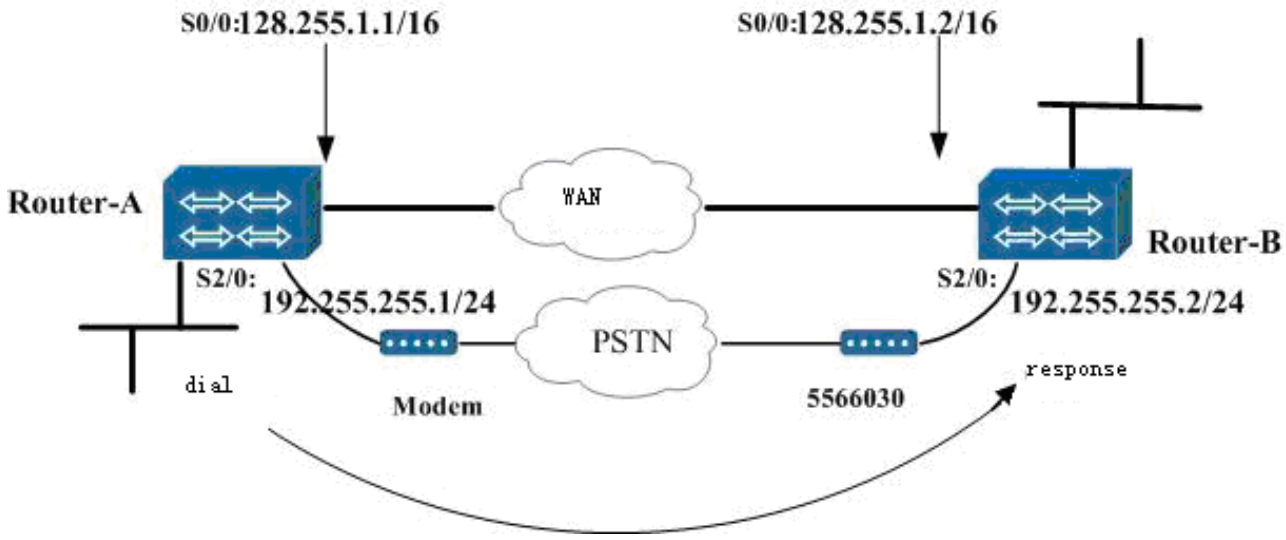
Configuration of Dial Backup

Command	Task
router(config-if- XXX)#backup delay	Configures the time should elapsed before the secondary line status changes after a primary line status has changed
router(config-if-XXX)#backup interface	Configures an interface as a secondary or dail backup

For example:

```
router(config-if- XXX)# backup interface s3/0
Set the interaface s3/0 as the backup line
router(config-if- XXX)# backup delay 5 5
Set a 5-second delay on activating the secondary line and set
a 5-second delay on deactivating the
secondary line
```

Dialer Backup Example



The serial2/0 of the router router-A connects to an outer modem, chooses the asynchronous mode, encapsulates PPP protocol is used as a backup line of serial0/0 and a caller uses the manual configuration of modem script;

The configuration of router-A:

Command	Task
router-A(config)#int s0/0	
router-A(config-if-serial0/0)# encapsulation ppp	
router-A(config-if-serial0/0)# physical-layer sync	
router-A(config-if-serial0/0)# backup interface serial2/0	Configures the S2 as a backup interface.
router-A(config-if-serial0/0)# backup delay 5 5	Set a 5-second delay on activating the secondary line after the primary line goes down and set a 5-second delay on deactivating the secondary line after the primary line comes up
router-A(config-if-serial0/0)#ip add 128.255.1.1 255.255.0.0	
router-A(config-if-serial0/0)#exit	
router-A(config)# chat-script modem-configure at&f%c3&k3&c1	Establishes a MODEM script: The script name: modem-configure The script contents: at&f%c3&k3&c1
router-A(config)#int s2/0	
router-A(config-if-serial2/0)# physical-layer async	
router-A(config-if-serial2/0)# encapsulation ppp	
router-A(config-if-serial2/0)#speed 38400	
router-A(config-if-serial2/0)# modem outer	Configures the outer MODEM.
router-A(config-if-serial2/0)# dialer string 5566030	Configures the called number as 5566030.
router-A(config-if-serial2/0)#modem party originate	Configures MODEM as the caller.
router-A(config-if-serial2/0)#script connection modem-configure	Specify the modem script that should be executed
router-A(config-if-serial2/0)#ip address 192.255.255.1 255.255.255.0	Configures the IP address.
router-A(config-if-serial2/0)#exit	Configuration has been finished.

Analyzing the above script: &f is to used to load the factory default configuration; %c3&k3&c is used to modify related parameters of the script. Of course, if you want to configure parameters by yourself, you need not use the script of &f.

The serial2/0 of the router router-B connects to an outer modem, chooses the asynchronous mode, encapsulates PPP protocol, is used as a backup line of serial0/0 and an answer uses the default script of the modem;

The detailed configuration is as follows:

router-B(config)#int s0/0	
router-B(config-if-serial0/0)# ip add 128.255.1.2 255.255.0.0	
router-B(config-if-serial0/0)# encapsulation ppp	
router-B(config-if-serial0/0)# physical-layer sync	
router-B(config-if-serial0/0)#exit	
router-B(config)# chat-script modem-configure at&f%c3&k3&c1	Configures the dialer script.
router-B(config)#int s2/0	
router-B(config-if-serial2/0)# physical-layer async	
router-B(config-if-serial2/0)# enc ppp	
router-B(config-if-serial2/0)# flow-control software	
router-B(config-if-serial2/0)# ip address 192.255.255.2 255.255.255.0	
router-B(config-if-serial2/0)# modem outer	Starts the outer MODEM.
router-B(config-if-serial2/0)# modem party answer	Configures MODEM as the answer.
router-B(config-if-serial2/0)#speed 38400	
router-B(config-if-serial2/0)#exit`	

Configure Backup Load

You can configure the backup load to activate or deactivate the secondary line based on the traffic load on the primary and sencondary line.When the load on the primary line is greater than the value, the secondary line is enabled.When the load on the primary line plus the load on the secondary line is less than the value, the secondary line is disabled.

Load diapup uses the traffic load to activate/disconnect backup line. When the traffic of the primary line reach some threshold (the percentage of maximal traffice, the same as the below.), the backup line is activated; when the total traffic of the primary and backup line is less than some threshold, the backup line is disconnected.

Commands

```
Backup load
Set a traffic load threthold for dial backup service
Backup load {enable-threshold|never} {disable-load|never}
no backup load
```

Syntax	Description
enable-threshold	Percentage of the primary line's available bandwidth that the traffic load should exceed to enable dail backup
never	Sets the secondary line never to be activated due to traffic load
disable-load	Percentaget of the primary line's available bandwidth that the traffic load should be less than to disable dial backup
never	Sets the secondary line never to be deactivated due to traffic load

You shoud configure backup interface first before configure load dialup.

The traffic statistics of the line is the traffic statistics every 5 minutes.

Usage of Configuring Commands

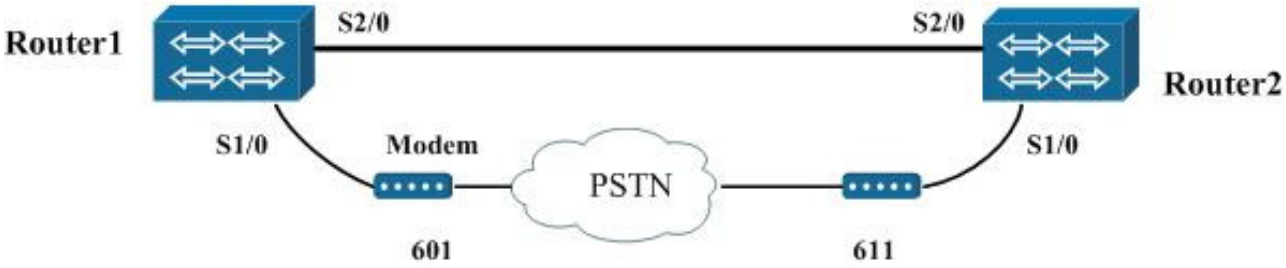


Figure 12-4

Two lines are employed between Router1 and router2: one is the primary line, connecting with the interface s2/0, and the other is the backup line, connecting with. The phone number related router1 is 601 and that related to router2 is 611.

The purpose of the example above is that when the traffic load reaches the value assigned to the line, the secondary line is activated although the primary line is still enabled.

1.

About the detailed DDR configuration, refer to Section 5.2 DDR Dialup Configuration.

Router1 is configured as follows:

command	Task
Router1# configure terminal	
Router1(config)# dialer-list 1 protocol ip permit	
Router1(config)# interface serial1/0	
Router1(config-if-serial1/0)# ip address 22.1.1.1 255.0.0.0	
Router1(config-if-serial1/0)# backup interface serail2/0	Assign interface s 2 to be the backup interface
Router1(config-if-serial1/0)# backup load 90 10	sets the traffic load threshold to 90 percent of the primary line serial 0. When The load is exceeded, the secondary line is activated, and will not be deactivated until the combined load is less than 10 percent of the primary bandwidth.
Router1(config-if-serial1/0)# interface serial2	
Router1(config-if-serial2/0)# physical-layer async	
Router1(config-if-serial2/0)# dialer in-band	Specify DDR (Dial-On-Demand Routing) to be supported
Router1(config-if-serial2/0)# dialer-group 1	
Router1(config-if-serial2/0)# dialer string 611	
Router1(config-if-serial2/0)# modem outer	
Router1(config-if-serial2/0)# ip addr 21.1.1.1 255.0.0.0	
Router1(config-if-serial2/0)# interface loopback0	
Router1(config-if-loopback0)# ip addr 20.1.1.1 255.0.0.0	
Router1(config-if-loopback0)# exit	
Router1(config)# ip route 20.1.1.2 255.255.255.255 21.1.1.2	
Router1(config)#ip route 20.1.1.2	

255.255.255.255 22.1.1.2	

Router2 configuration

Command	Task
Router1# configure terminal	
Router1(config)# dialer-list 1 protocol ip permit	
Router1(config)# interface serial1/0	Configure main interface
Router1(config-if-serial1/0)# ip address 22.1.1.2 255.0.0.0	
Router1(config-if-serial1/0)# interface serial2/0	Configure backup interface
Router1(config-if-serial2/0)# physical-layer async	
Router1(config-if-serial2/0)# modem outer	
Router1(config-if-serial2/0)# ip addr 21.1.1.2 255.0.0.0	
Router1(config-if-serial2/0)# interface loopback0	
Router1(config-if-loopback0)# ip addr 20.1.1.2 255.0.0.0	
Router1(config-if-loopback0)# exit	
Router1(config)# ip route 20.1.1.1 255.255.255.255 21.1.1.1	
Router1(config)# ip route 20.1.1.1 255.255.255.255 22.1.1.1	

Debug commands

show interface

Display the 5-minute traffic load of an interface

Debug backup

Display the debugging information in the course of load dialup.

Debugging of Modem

To examine its dialer status and the relative information, use the debug modem command:

```
router#debug modem interface
```

This command Displays debugging information of a given interface. The following is the debugging information with default parameters:

```
pppdown1#debug modem s3
pppdown1(config)#1d2h: [tMdmDelay]serial3: Config modem for
dialing out
1d2h: [tMdmDelay]serial3: AT configurating command:
AAT&FE0Q0W1S95=44S36=5S25=0X0
AAT&D2&Q5
AATM1L1
1d2h: [tSccRx3]serial3: Success to send the 0th group
configuring command
1d2h: [tSccRx3]serial3: Success to send the 1th group
configuring command
1d2h: [tSccRx3]serial3: success to configure modem
1d2h: [tSccRx3]serial3: Start dialing automatically
1d2h: [tNetTask]serial3: Dialing timeout is set as 45s(DL-
mode)
1d2h: [tNetTask]serial3: Dialing 8005...
Closing the modem debugging switch
router#no debug modem  interface
```

If modem does not dial up, it should be examined whether cables are connected correctly, and make sure that the modem has been turned on and configured as the receiving AT commands mode and reliably connected to the correct interface.

When users try to turn on the dialer connection but the modem doesn't respond to the access request, users should examine whether the remote modem is configured as the auto-answer or the AT command mode. They should make sure that the remote modem has connected with the router or other equipments. If necessary, the dialer sound on the telephone line can be examined.

If the modem cannot receive answers or send calls correctly, users can also examine whether the modem script is configured correctly via the command debug modem interface.

When the modem connects with Cisco products, users should notice whether the modem DTR lamp is normal. If it is abnormal, users should clear the line via the command clear line ***.

DDR Dialer Configurations

Preparing to Configure DDR (Dial-On-Demand Routing)

For a network needing to use DDR, users can perform configuration according to the following series of operations:

Decide which routers use DDR, select what kind of transmission medium will be used, which interfaces of the outer use DDR, which kind of DDR topology structure an interface adopts, whether an interfaces sends call, or accepts call, or both.

Decide the interface type (asynchronous serial port or ISDN interface).

Configure the interface encapsulation, the default is PPP.

Configure the routing protocol (RIP, OSPF or static routing etc) employed on the DDR port.

Commands

Defining the Interesting Traffic

The global configuring command is: dialer-list (also called dialer list). In order to control the condition for a DDR call to take place, users can use the command dialer-list to configure the packet condition.

Only those packets that meet the packets prescribed by dialer-list can initiate DDR to dial up. The simple format of the command can prescribe a set of protocols that are both permitted to trigger a call/prohibited from triggering a call. The complex format of the command can cite an access control list so as to define interesting data in detail.

```
router(config)#dialer-list dialer-group-number protocol ip
{ permit | deny | list access-list-number }
```

Dialer-group-number is the sequence number <1_10> of dialer-list, related with the dialer-group group-number of DDR interface configuration.

Access-list-number is the sequence number of the access list access-list related with dialer-list Ip is a protocol name, and the protocol supported is ip protocol.

Permit indicates packets related with the protocol are permitted. Deny indicates packets related with the protocol are denied.

When configuring the access list, you should do it orderly. In addition, the multicasting packet of the routers from some companies can trigger the dialer. For example, for the multicasting packet of OSPF 224.0.0.5, it is best to deny it; or else, the telephone company will give you the telephone bill. Or you can use debug dialer packer to examine whether there is the multicasting packet, whether it is necessary to configure an access list for the triggered dialer

```
router(config-if-serial1)#dialer ?
```

The configuration is as follows:

Command	Description
callback-secure	Turns on the callback security switch; hang up the call without correct configuration of reverse callback.
enable-timeout	Set the length of time an interface stays down after a call has conmpleted or failed and before it is available to dial again
fast-idle	Configures fast idle time, for which the line will stay before it is disconnected and the competing call is placed, if there exists competition on the line.
hold-queue	Configures the number of outgoing packets to be queued.
idle-timeout	Specify the idle time before the line is disconnected
in-band	Specify DDR (Dial-On-Demand Routing) to be supported.
load-threshold	.Interface load beyond which the dialer will initiate another call to the destionation
map	Associates the IP address of the opposite terminal with the phonenumber or the called user name so as to call one or more sites.
pool	Associates the dialer interface with the dialer pool (taking effect in the dialer interface).
pool-member	Configure the physical interface.to be a member of a dialing pool.
priority	Configures the priority of physical interface in the dialer pool.
remote-name	Configures the name of the remote system.
rotary-group	Adds an interface into the dialer rotary group.
rotor	Designates the method used by DDR to call the outward line.
string	Configures the telephone number to be dialed up.
wait-for-callback-time	Configures the time waiting for the callback.
wait-for-carrier-time	Configures the longest time for DDR to wait for call establishment.

Distributing the dialer list dialer-list to a port

After defining a dialer-list, you need to associate it with the interface answering for originating/accepting call. Related command is as follows:

```
router(config-if-serial1)# dialer-group group-number
```

dialer-group:
The command configures an interface to belong to a given dialer-group, which points to a dialer-list.

group-number:
This is the number of the dialer access group to which the interface belongs. The dialer access group is defined by the command "dialer-list", which defines the trigger data stream originating DDR. The acceptable values are the integer within 1 to 10.

Defining the parameters of the destination

After defining the structure of the interesting traffic, you should provide the interface answering for originating call/answer with all necessary parameters that arriving at the destination needs. Here, "dialer map" or "dialer string" indicates the routing information, such as the telephone number to dial, etc.

The command dialer map:

```
router(config-if-serial1)#dialer map ip A.B.C.D name hostname
dialer-string
ip representing protocol A.B.C.D representing the name of the
remote system
dial-string representing the dialed telephone number to
arrive at the remote-end destination
```

The command dialer string:

```
pppdown1(config-if-XXX)#dialer string <STRING>
<STRING>Dialer string - The telephone number of the opposite
terminal
```

When it is only used to send call, the command dialer map and the telephone number string dialer-string are necessary; the keyword name is optional.

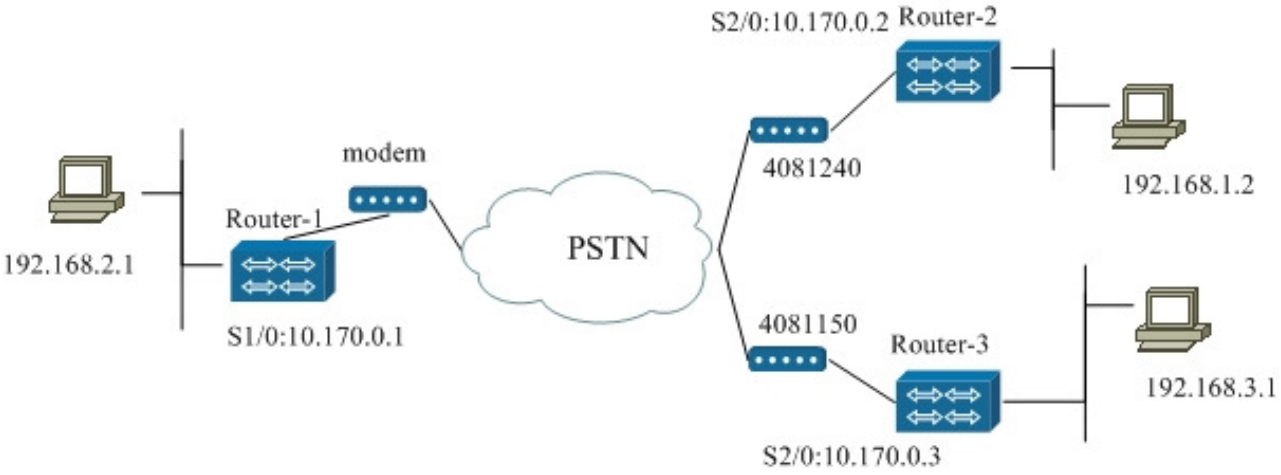
If the keyword name is employed, PPP authentication should be configured. The name should be the same as the hostname sent from the remote end.

If the dynamic routing is configured, the option broadcast should be added behind name hostname.

The command dialer map and dialer string can't be used .

The command dialer map and the keyword name are needed in the dialer callback.

Command Usage



Router-1, Router-2 and Router-3 connects with each other via the outer MODEM and PSTN dialer.

Router1 configuration s1/0 and the DDR configuration are as follows:

User name and dialer-list:

Command	Task
route1#configure terminal	
route1(config)#dialer-list 1 protocol ip list 1001	Permits the dialer access group1 to spur DDR dialer.
route1(config)#user route2 password 0 Signamax route1(config)#user route3 password 0 Signamax	Configures user name and password. You can configure several user names, which has no affect on the configuration of name in dialer map. As long as the user name corresponds with the name in dialer map, it is ok.
route1(config)#ip access-list extended 1001	Establishes an access list 1001.
route1(config-ext-nacl)#deny ip any 224.0.0.0 0.255.255.255 route1(config-ext-nacl)#permit ip any any	The access rule is configured for that some multicasting packets that can trigger DDR dialer.

Configuring dialer triggering route :

```
route1(config)#ip route 192.168.3.0 255.255.255.0 10.170.0.3
route1(config)#ip route 192.168.1.0 255.255.255.0 10.170.0.2
```

The two routes are used to trigger different telephone numbers that different directions of data stream trigger.

Command	Task
route1(config)#interface serial1/0	Enters the interface s1.
route1(config-if-serial1/0)#physical-layer async	Configures it as the asynchronous mode
route1(config-if-serial1/0)#speed 115200	Speed is 115200.
route1(config-if-serial1/0)#databits 8	8 data bits
route1(config-if-serial1/0)#stopbits 1	1 stop bit
route1(config-if-serial1/0)#parity none	The parity bit is NULL.
route1(config-if-serial1/0)#flow-control none	Configures the flow control as NULL.
route1(config-if-serial1/0)#encapsulation ppp	Encapsulates PPP protocol.
route1(config-if-serial1/0)#ip address 10.170.0.1 255.0.0.0	Configures the IP address.
route1(config-if-serial1/0)#modem outer	Enables the outer MODEM to be effective.
route1(config-if-serial1/0)#dialer in-band	Specify DDR (Dial-On-Demand Routing) to be supported
route1(config-if-serial1/0)#dialer idle-timeout 100	DDR hangs up link when no data stream passes via the link within 100 seconds after a call is created.
route1(config-if-serial1/0)#dialer fast-idle 30	After the call has been idle for 30 seconds, the call gives place to another one that is waiting.
route1(config-if-serial1/0)#dialer map ip 10.170.0.2 name route2 4081240	Sends the call with telephone number 4031240 to router2 with the address 10.170.0.2.
route1(config-if-serial1/0)#dialer map ip 10.170.0.3 name route3 4081150	Sends the call with telephone number 4081150 to router3 with the address 10.170.0.3.
route1(config-if-serial1/0)#dialer-group 1	The interface s1 belongs to the dialer access group 1 (Dial up only when the data stream according with the dialer-group1 is triggered.)
route1(config-if-serial1/0)#ppp authentication chap	Configures chap authentication, Configure the command as the chap originator.
route1(config-if-serial1/0)#ppp chap hostname route1	Configures the authenticated name related with the name in the opposite terminal dialer map.
route1(config-if-serial1/0)#exit	

During the course, after the route1 dials on the outer modem of the route2 and constructs an access to the route2, if there is no data sent via the s1/0 within 100 seconds (namely exceeding the value of idle-timeout), the router1 will trigger modem1 to automatically disconnect the connection with the modem2 of the route2. Within the idle time, if the route1 receives the data stream to trigger calling the route3, the timer fast-idle will start. Within the 30 seconds the timer fast-idle times, if there is no data sent to the route2 via the s1/0, the route1 will disconnect the connection with the route2 and call the route3.

For the answer, it should be configured as the authentication originator. At the moment of callback, two same names cannot be configured in dialer map on the side of callbacker. Besides the above, of course, the same user name with that on a Cisco router cannot also be configured at the time of authentication.

Router-1, Router-2 and Router-3 connects with each other via the outer MODEM and PSTN dialer. The configuration of router1 s1/0 and the DDR configuration are as follows:

User name and dialer-list:

Command	Task
route1#configure terminal	
route1(config)#dialer-list 1 protocol ip list 1001	Permits the dialer access group1 to spur DDR dialer.
route1(config)#user route2 password 0 Signamax route1(config)#user route3 password 0 Signamax	Configures user name and password. You can configure several user names, which has no affect on the configuration of name in dialer map. As long as the user name corresponds with the name in dialer map, it is ok.

route1(config)#ip access-list extended 1001	Establishes an access list 1001.
route1(config-ext-nacl)#deny ip any 224.0.0.0 0.255.255.255 route1(config-ext-nacl)#permit ip any any	The access rule is configured for that some multicasting packets that can trigger DDR dialer.

The configuration of the interface:

Command	Task
route1(config)#interface serial1/0	Enters the interface s1/0.
route1(config-if-serial1/0)#physical-layer async	Configures it as the asynchronous mode
route1(config-if-serial1/0)#speed 115200	Speed is 115200.
route1(config-if-serial1/0)#databits 8	8 data bits
route1(config-if-serial1/0)#stopbits 1	1 stop bit
route1(config-if-serial1/0)#parity none	The parity bit is NULL.
route1(config-if-serial1/0)#flow-control none	Configures the flow control as NULL.
route1(config-if-serial1/0)#encapsulation ppp	Encapsulates PPP protocol.
route1(config-if-serial1/0)#ip address 10.170.0.1 255.0.0.0	Configures the IP address.
route1(config-if-serial1/0)#modem outer	Enables the outer MODEM to be effective.
route1(config-if-serial1/0)#dialer in-band	Specify DDR (Dial-On-Demand Routing) to be supported
route1(config-if-serial1/0)# dialer idle-timeout 100	DDR hangs up link when no data stream passes via the link within 100 seconds after a call is created.
route1(config-if-serial1/0)# dialer fast-idle 30	After the call has been idle for 30 seconds, the call gives place to another one that is waiting.
route1(config-if-serial1/0)# dialer map ip 10.170.0.2 name route2 4081240	Sends the call with telephone number 4031240 to router2 with the address 10.170.0.2.
route1(config-if-serial1/0)# dialer map ip 10.170.0.3 name route3 4081150	Sends the call with telephone number 4081150 to router3 with the address 10.170.0.3.
route1(config-if-serial1/0)#dialer-group 1	The interface s1 belongs to the dialer access group 1 (Dial up only when the data stream according with the dialer-group1 is triggered.)
route1(config-if-serial1/0)#ppp authentication chap	Configures chap authentication, Configure the command as the chap originator.
route1(config-if-serial1/0)#ppp chap hostname route1	Configures the authenticated name related with the name in the opposite terminal dialer map.
route1(config-if-serial1/0)#exit	

Configuring dialer triggering route :

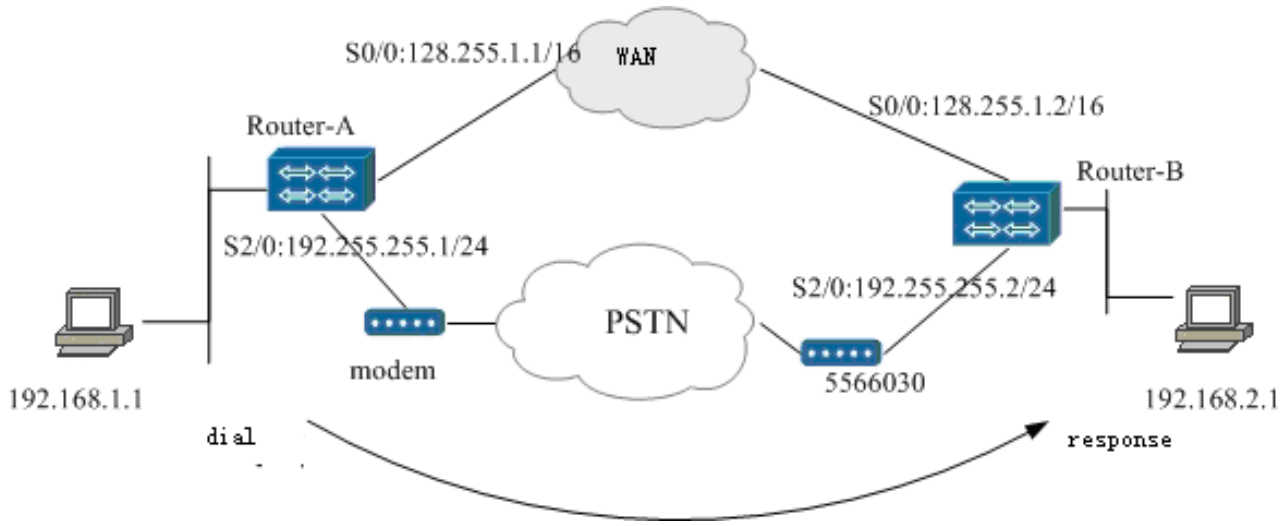
```
route1(config)#ip route 192.168.3.0 255.255.255.0 10.170.0.3
route1(config)#ip route 192.168.1.0 255.255.255.0 10.170.0.2
```

The above two routes are used to trigger the different telephone numbers different directions of data stream trigger.

During the course, after the route1 dials on the outer modem of the route2 and constructs an access to the route2, if there is no data sent via the s1 within 100 seconds (namely exceeding the value of idle-timeout), the router1 will trigger modem1 to automatically disconnect the connection with the modem2 of the route2. Within the idle time, if the route1 receives the data stream to trigger calling the route3, the timer fast-idle will start. Within the 30 seconds the timer fast-idle times, if there is no data sent to the route2 via the s1, the route1 will disconnect the connection with the route2 and call the route3.

For the answer, it should be configured as the authentication originator. At the moment of callback, two same names cannot be configured in dialer map on the side of callbacker. Besides the above, of course, the same user name with that on a Cisco router cannot also be configured at the time of authentication.

The example of DDR (Dial-On-Demand Routing) dialer configuration:



The serial2/0 of the router router-A connects to an outer modem, chooses the asynchronous mode, encapsulates the PPP protocol (using chap authentication), is used as a backup interface and a caller and start the script of the modem: at&f&k3%c3&c1. The serial port 0 is used as the master interface, encapsulates the HDLC protocol. The dialer adopts the dialer map mode.

The serial2/0 of the router router-B connects to an outer modem, chooses the asynchronous mode, encapsulates PPP protocol, is used as a backup line to the serial 0 and a answer uses the script of the modem: at&f&k3%c3&c1. And the static routing is adopted between routers.
The detailed configuration is as follows:

Router-A and Router-B connect with each other via their own s0/0, while their own s2/0 connects the outer modem, which serves as a backup line to the interface s0/0.

The configuration of a caller:

Command	Task
router-A#con t	
router-A(config)# user answer pass 0 Signamax	Configures the opposite terminal as a local user and configure its password, which should be the same as the user password configured by the opposite terminal (namely the chap authentication password sent by the opposite terminal).
router-A(config)# dialer-list 1 protocol ip permit	Configures the packets triggering dialer.
router-A(config)# chat-script m-con at&f&k3%c3&c1	Establishes the MODEM dialer script. The script name: m-con; The script contents: at&f&k3%c3&c1
router-A(config)# int f0	
router-A(config-if-fastethernet0)# ip address 195.168.1.3 255.255.255.0	
router-A(config-if-fastethernet0)#exit	
router-A(config)#int s0/0	
router-A(config-if-serial0/0)#phy sync	
router-A(config-if-serial0/0)# encapsulation hdlc	
router-A(config-if-serial0/0)# ip address 128.255.1.1 255.255.0.0	
router-A(config-if-serial0/0)# backup interface serial2/0	Uses the serial S2/0 as the backup line to the interface s0/0.
router-A(config-if-serial0/0)# backup delay 5 20	Set a 5-second delay on activating the secondary line after the primary line goes down and set a 20-second delay on deactivating the secondary line after the primary line comes up
router-A(config-if-serial0/0)#exit	
router-A(config)#int s2/0	
router-A(config-if-serial2/0)# physical-layer async	
router-A(config-if-serial2/0)# encapsulation ppp	

router-A(config-if-serial2/0)# ppp authentication chap	
router-A(config-if-serial2/0)# ppp chap hostname caller	
router-A(config-if-serial2/0)# ip address 192.255.255.1 255.255.255.0	
router-A(config-if-serial2/0)# modem outer	Configures the outer modem.
router-A(config-if-serial2/0)# dialer in-band	Specify DDR (Dial-On-Demand Routing) to be supported
router-A(config-if-serial2/0)# dialer map ip 192.255.255.2 name answer 5148120	Configures a dialer association. IP address of the opposite terminal is 192.255.255.2, the authentication user name is answer and the telephone number to dial is 5148120. If the dynamic routing is employed, don't forget to add a word broadcast behind the telephone number.
router-A(config-if-serial2/0)# script connection m-con	Configures the MODEM script.
router-A(config-if-serial2/0)# dialer-group 1	Defined the interesting traffic that triggers DDR.
router-A(config-if-serial2/0)#exit	
router-A(config)# ip route 193.168.0.0 255.255.0.0 serial0/0 router-A(config)# ip route 193.168.0.0 255.255.0.0 serial2/0 200	Adds the static route.

Command	Task
router-B# configure terminal	
router-B(config)#user caller password 0 Signamax	Configures the opposite terminal as a local user and configure its password, which should be the same as the user password configured by the opposite terminal (namely the chap authentication password sent by the opposite terminal).
router-B(config)#dialer-list 1 protocol ip permit	Configures the packets triggering dialer.
router-B(config)# chat-script m-con at&f&k3%c3&c1	Establishes MODEM dialer script; The script name: m-con The script contents:

	at&f&k3%c3&c1
router-B(config) # int f0	
router-B(config-if-fastethernet0)# ip address 193.168.2.3 255.255.255.0	
router-B(config-if-fastethernet0)#exit	
router-B(config)#int s0/0	
router-B(config-if-serial0/0)#phy sync	
router-B(config-if-serial0/0)#encapsulation hdlc	
router-B(config-if-serial0/0)#clock rate 64000	
router-B(config-if-serial0/0)#ip address 128.255.1.2 255.255.0.0	
router-B(config-if-serial0/0)#exit	
router-B(config)#int s2/0	
router-B(config-if-serial2/0)# physical-layer async	
router-B(config-if-serial2/0)# encapsulation ppp	
router-B(config-if-serial2/0)# ppp authentication chap	Configures chap authentication.
router-B(config-if-serial2/0)# ppp chap hostname answer	Configures the name of chap authentication.
router-B(config-if-serial2/0)# dialer map ip 192.255.255.1 name caller(5148343)	Of course, if this side serves only as an answer, it will be not necessary to configure the telephone number to dial.
router-B(config-if-serial2/0)# ip address 192.255.255.1 255.255.255.0	
router-B(config-if-serial2/0)#modem outer	Configures the outer modem.
router-B(config-if-serial2/0)# dialer in-band	Specify DDR (Dial-On-Demand Routing) to be supported
router-B(config-if-serial2/0)#script connection m-con	Configures MODEM script.
router-B(config-if-serial2/0)#dialer-group 1	Defines the interesting traffic that triggers DDR.
router-B(config-if-serial2/0)#exit	
router-B(config)#ip route 195.168.0.0 255.255.0.0 serial0/0 router-B(config)#ip route 195.168.0.0 255.255.0.0 serial2/0	Adds the static route

If the modem does not dial up, users should examine whether cables are connected correctly, should make sure that the modem has been turned on, it has been configured as the mode the modem can accept the AT commands and that it has connected reliably with the correct interface.

When users try to open the dialer connection but the modem has no response to the access request, users should examine whether the remote modem is configured as auto-answer or the AT command mode. They should make sure that the remote modem has been connected to the router or to other equipment. When necessary, they can also examine whether there is a dialer sound on the telephone line.

If a modem cannot accept an answer or send call correctly, users can also examine whether the modem script is configured correctly via the command debug modem interface.

When the dialer backup interface does not dial up, then dcd is down, but its flag Flags is often in the status of up (spoofing). However, at the moment, the interface is not up really. Only when the primary line goes down and there is data to trigger, then the dialer backup interface can dial. When it is connected correctly, the flags will be in the status of up.

Dialer Callback

PPP reverse callback provides a kind of client/server relation between the two ends connected in terms of the point-to-point mode. The function of PPP reverse callback permits the router to ask the opposite terminal router connected by dialer to call back. The feature can be used to control access and save the charge of the remote call between routers.

Operation and procedure of reverse callback:

The reverse callback client originates a call. In the LCP negotiation phase of PPP, a client can use the reverse callback option to request the reverse callback.

The reverse callback server determines the reverse callback request and examines the configuration of itself to validate whether the reverse callback is employed.

The reverse callback client and server process the authentication via CHAP or PAP. A user name is used to distinguish the dialer string used by the callback.

After the success of the first authentication, the router used as the reverse callback server will distinguish the dialer string used by the reverse callback. The reverse callback server compares user names with the host names in the dialer-mapping list.

If “dialer callback-secure” is not started, the reverse callback server will maintain the initial call when the reverse callback isn’t configured for the authenticated user name; or else, the reverse callback server will hang up the initial call.

The reverse callback server uses a dialer string to originate a reverse callback. If it fails, it will not try to call again. During the course of returning a call back, the reverse callback does not process LCP negotiation of PPP.

Process to call.

Keep on connecting.
If the caller requests to process reverse callback but the server is not be configured to accept a reverse callback, then the answer router will maintain the initial call originated by the caller.

The commands of reverse callback in the global configuration mode:

Command	Description
Username username password password	Creates a local authentication database based on user names.
map-class dialer string	Creates a callback mapping class.

The configuring commands in the interface mode:

Command	Description
Dialer callback-secure	Starts a secure callback (dialing up an abnormal call).
PPP callback request	Callback request(applied to a client)
PPP callback accept	Callback acceptation
Dialer callback-server	Starts the callback server.
Dialer enable-timeout	Configures the waiting time of a callback
Dialer fast-idle	Configures the fast idle time when there exists competition.
Dialer idle-timeout	Configures the idle time of before hangup
Dialer wait-for-carrier-time	Changes the value of the fast call rerouting timer into twice the value of start pause timer.

The configuration example of dialer callback:

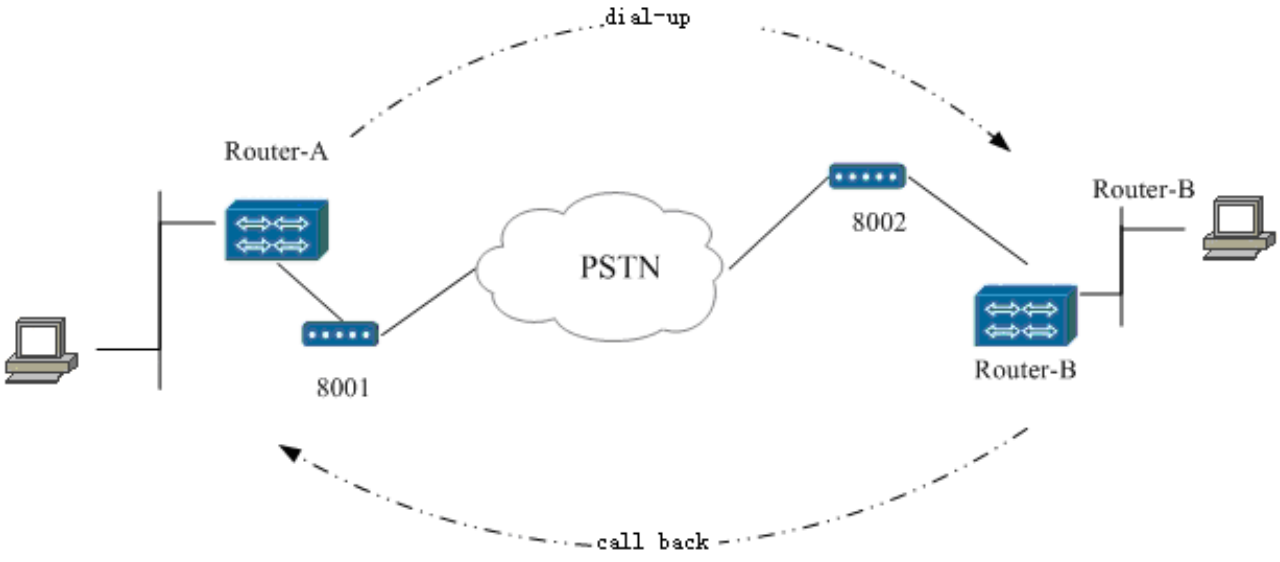


Figure 12-7

The routers Router-A and Router-B connect with each other via PSTN network. The Router-A is a dialer requester the Router-B is a callbacker. The telephone number of the Router-A is 8001 and the number of the Router-B is 8002.

The router Router-B is used as the dialer server in this example.

The configuration is as following:

Router1—A
router1—A (config)#user Signamax password 0 Signamax
router1—A (config)#dialer-list 1 protocol ip permit
router1—A (config)#int s2
router1—A (config-if-serial2)#ip address 100.0.0.1 255.0.0.0
router1—A (config-if-serial2)#enc ppp
router1—A (config-if-serial2)#phy async
router1—A (config-if-serial2)#dialer in-band
router1—A (config-if-serial2)#dialer-group 1
router1—A (config-if-serial2)#dialer map ip 100.0.0.2 name Signamax broadcast 8002
router1—A (config-if-serial2)#ppp callback request
router1—A (config-if-serial2)#ppp authentication chap
router1—A (config-if-serial2)#ppp chap hostname goat
Router2—B
router2—B (config)#user goat password 0 Signamax
router2—B (config)#dialer-list 1 protocol ip permit
router2—B (config)#map-class dialer goat
router2—B (config-map-class)#dialer callback-server
router2—B (config)#int s2
router2—B (config-if-serial2)#ip address 100.0.0.2 255.0.0.0
router2—B (config-if-serial2)#enc ppp
router2—B (config-if-serial2)#phy async
router2—B (config-if-serial2)#dialer in-band
router2—B (config-if-serial2)#dialer-group 1
router2—B (config-if-serial2)#dialer map ip 100.0.0.1 name goat class goat broadcast 8001
router2—B (config-if-serial2)#dialer callback-secure
router2—B (config-if-serial2)#ppp callback accept
router2—B (config-if-serial2)#ppp authentication chap
router2—B (config-if-serial2)#ppp chap hostname Signamax

The callbacker should be configured as the chap originator.

Two same names can't be configured in the dialer map of the callbacker because a callback decides its callback object according to name and the same names will lead that the numbers needed to call back can't be identified.

The function of broadcast in dialer map is to let the dynamic routing pass.

Configuring ISDN

ISDN access interface is a physical connection between users and ISDN service providers. Two different kinds of access interfaces are defined by ISDN suggestions of ITU-T, which are respectively called Basic Rate Interface (BRI) and Primary Rate Interface (PRI).

Because the establishment of ISDN needs a dialer environment, the Signamax router adopts DDR (Dial-on-Demand Routing) technology. So, only when packets arrive, the remote-end router of will be dialed. This technology can save charges for its users.

When the router is configured with the ISDN module, the command show run can be used to see the interface bri0 interface. In order that DDR of ISDN is achieved, the basic configuration of some routers is necessary. The following example, will explain how to use ISDN on a Signamax router.

Commands

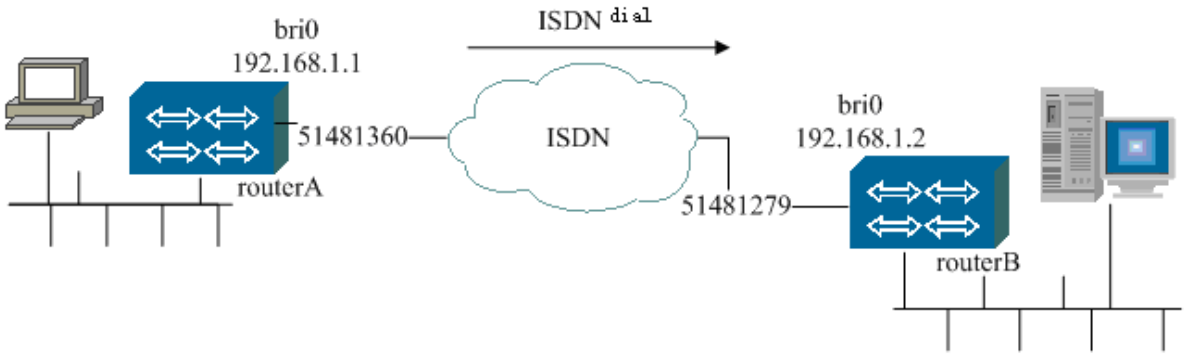
Command	Description	Configuration mode
isdn call interface <string>	Dial up a number from the interface, to check whether isdn line is normal.	enable
isdn disconnect interface channel	Hang up isdn call of interface, to test whether isdn line is normal.	enable
isdn switch-type < | basic-1tr6 | basic-5ess | basic-dms100 | basic-net3 | basic-ni | basic-qsig | basic-ts013 | ntt | vn3	Configure isdn switching type (configure according to connected isdn switch, no default value), to configure isdn default value, switch type has the following: Germany 1TR6 switching type Lucent 5ESS DMS-100 NET3 ISDN QSIG TS013 NTT	config config-if-XX

>	VN3 and VN4	
isdn tei-negotiation < first-call |powerup>	Get TEI number to configure isdn interface default value: The first ISDN TEI TEI when power on	config config-if-XX
isdn activate< every-time | powerup>	Activate isdn physical layer D channel activation when it is down Activate channel D when power on	config-if-XX
isdn answer1 <string>	Answer 1	config-if-XX
isdn answer2 <string>	Answer 2	config-if-XX
isdn caller <string>	Accepted call ID number	config-if-XX
isdn calling-number <string>	Local initiated calling number	config-if-XX
isdn imcoming progress <accept/validate>	Accept or check PROGRESS message	config-if-XX
isdn reject data <56/64>	Refuse to accepted call type	config-if-XX
isdn send-alerting	Whether to send alert message	config-if-XX
isdn switch-type <switch type>	Interface switching type	config-if-XX
isdn tei-negotiation <first-call/powerup>	TEI negotiation refers to before explanation.	config-if-XX
isdn twait-diable	Cancel the waiting when getting TEI	config-if-XX
pri-group [timeslots range]	Use pri-group controller to configure the command. configure ISDN rate interface (PRI) on channlized CE1, and use no form to delete ISDN PRI configuration.	controller e1 XX

Configure switch-type before using isdn function.

ISDN BRI Configuring DDR

The following figure illustrates the structure of a network where one router connects to another one via ISDN. The following example illustrates how to combine commands to establish ISDN and DDR. In the example, the commands "dialer map" and chap authentication are used.



The following is the configuration of the router-A, which adopts the dialer map and ppp chap authentication.

The configuration of router-A:

Command	Task
Router-A(config)#hostname router-A	When the user name of ppp chap hostname is not configured, the chap authentication will send the hostname configured here to the opposing party.
router-A(config)#user router-2 password 0 Signamax	Configures the opposite terminal as a local user; configure the password (it is the same with the user password of the caller). The user is registered when the machine starts.
router-A(config)#dialer-list 1 protocol ip permit	Defines the interesting traffic.
router-A(config)#interface fastethernet0 router-A(config-if-fastethernet0)#ip address 128.255.252.2 255.255.255.0 router-A(config)#exit	Configures the interface f0.
router-A(config)#interface bri0	Enters the bri0 configuration mode.
router-A(config-if-bri0)# encapsulation ppp router-A(config-if-bri0)# ppp authentication chap	Encapsulates PPP protocol and configure CHAP authentication.
router-A(config-if-bri0)#ppp chap hostname router-A	Configures the user name used for chap authentication.
router-A(config-if-bri0)# ip address 192.168.1.1 255.255.255.252	
router-A(config-if-bri0)#dialer idle-timeout 60	Idle timeout
router-A(config-if-bri0)#dialer enable-timeout 5	The interval of next calls
router-A(config-if-bri0)#dialer map ip 192.168.1.2 name router-2 51481279	Defines the parameters of the destination.
router-A(config-if-bri0)#dialer-group 1	The port belongs to the dialer-group1.
router-A(config-if-bri0)#exit	
router-A(config)# ip route 130.255.252.0 255.255.255.0 192.168.1.2	Configures the trigger dialer routing (it is also a static routing).

The configuration of router-2:

Command	Task
router(config)#hostname router-B	
router-B(config)#user router-A password 0 Signamax	
router-B(config)#dialer-list 1 protocol ip permit	Configures a dialer-group.
router-B(config)#interface fastethernet0	
router-B(config-if-fastethernet0)# ip address 130.255.252.10 255.255.255.0	
router-B(config)#exit	
router-B(config)#interface bri0	
router-B(config-if-bri0)#encapsulation ppp	
router-B(config-if-bri0)#ppp authentication chap	Configures CHAP authentication.
router-B(config-if-bri0)#ppp chap hostname router-B	Configures the name of CHAP authentication.
router-B(config-if-bri0)# ip address 192.168.1.2 255.255.255.252	
router-B(config-if-bri0)#dialer idle-timeout 60	Configures idle time.
router-B(config-if-bri0)#dialer enable-timeout 5	
router-B(config-if-bri0)# dialer map ip 192.168.1.2 name router-A	Configures the mapping of dialer.
router-B(config-if-bri0)#dialer-group 1	Configures the trigger dialer-group1.
router-B(config-if-bri0)#exit	
router-B(config)#ip route 128.255.252.0 255.255.255.0 192.168.1.1	

The static routing commands of the router-A defines the IP routing of the 130.255.252.0 network connecting to the LAN interface inter f0 of the router router-2.

Interesting packet can be defined as any IP packet, and they can originate the calls to router-B.

Router-B is defined to accept calls via the command dialer map. There is the static routing to LAN of the router router-A on it.

ISDN PRI Configuration

Command	Description
router(config)#controller e1 0/0	Define controller position (0), to enter E1 configuration mode
router(config-controller)#pri-group timeslot 1-31	Configure the timeslots to set up PRI interface, 1-port CE1 configures one pri-group and channel-group.
router(config-controller)#exit	Exit to E1 configuration mode
router(config)#interface serial0/0:15	Enter PRI configuration interface
router(config-if-serial0/0:15)#isdn switch-type primary-net5	Configure ISDN PRI interface switching type
router(config-if-serial0/0:15)#ip address 1.1.1.1 255.255.255.0	Configure interface IP address
router(config-if-serial0/0:15)#encapsulation ppp	Configure interface encapsulation
router(config-if-serial0/0:15)#ppp multilink	Configure interface PPP multilink negotiation

Debugging & Monitoring

Monitoring an interface:

Display information of the ISDN BRI interface. The used command is as follows:

```
router#sh int bri0
```

False *up* status

Displaying information of the ISDN BRI interface

```
bri (unit number 0):
     Flags:  (0x8071)  UP(spoofing)  POINT-TO-POINT  MULTICAST
ARP RUNNING
Type: PPP

     Internet address: 192.168.1.1
     Netmask 0xffffff00 Subnetmask 0xfffffffc
     Destination Internet address: 0.0.0.0
     Metric is 0
     Maximum Transfer Unit size is 1500
     0 packets received; 0 packets sent
     0 multicast packets received
     0 multicast packets sent
```

```
     0 input errors; 0 output errors
     0 collisions; 0 dropped
      rxFrames: 0, rxChars 0
      txFrames: 0, txChars 0
      rxNoOctet 0, rxAbtErrs 0, rxCrcErrs 0
      rxOverrun 0, rxLenErrs 0, txUnderrun 0
        DCD=down  DSR=down  DTR=up  RTS=up  CTS=down  Txc=up
```

Here, although it can be seen that the DCD signal and DSR signal of the physical layer are DOWN, the interface is still UP. The reason is that the technique called false UP (namely spoofing) is adopted in DDR.

This word indicates that the line need not be UP but a dialer port still forces it to be false UP. The interface can dial on demand to route its packets. All dialer interfaces have this feature.

Display information about some channel status of ISDN, the second layer and the third layer. The command is as follows:

```
router#sh isdn status
```

Displays information about ISDN status

```
ISDN BRI0 interface
    Layer 1 Status:
        F7
    Layer 2 Status:
        TEI = 67          Ces = 01       SAPI = 00      Status =
ST_MULTIFR
        I-Frame: 0/0      RR:  5/5       RNR:  0/0      REJ: 0/0
        SABME:   1/0      DM:  0/0       DISC: 0/0      UA:  0/1
        FRMR:    0/0      TEI: 59/1
     B1 channel:
         Tx Frames = 0 Tx Bytes = 0, Tx Errors = 0
         Rx Frames = 0 Rx Bytes = 0
     B2 channel:
         Tx Frames = 0 Tx Bytes = 0, Tx Errors = 0
         Rx Frames = 0 Rx Bytes = 0
```

In this common situation, as long as the ISDN module of the router connects with the ISDN switch correctly, the command show isdn status can be used to see that the second layer is of ST_MULTIFR status, which indicates that the D channel is active.

The following are some other commands to examine ISDN status:
Examining the active ISDN data channel

```
router#show isdn active
```

Examining the situation of the ISDN calls that have been used

```
router#show isdn history
```

The ISDN Debugging Commands

The following debugging commands are very useful to detect ISDN errors. The two main ISDN commands are "debug isdn q921" and "debug isdn q931".

To display the access procedure that happens on the data link layer of the access server ISDN interface D channel use:

```
router#debug isdn q921
```

To display the establishment and backup of call on the network connection layer (the third layer) between the local router (client) and the ISDN network use:

```
router#debug isdn q931
```

To display contents of ISDN i430 protocol

```
router#debug isdn i430
```

To display contents of information of ISDN packets

```
router#debug isdn trace
```

The following table displays different debugging commands and their relation to OSI model.

The OSI layer	ISDN	DDR dialer
The third layer	Debug isdn q931	Debug dialer events Debug dialer packets
The second layer	Debug isdn q921 Debug isdn i430 Debug isdn trace Debug isdn events	Debug ppp negotiation

When ISDN cannot achieve the connection with the opposite terminal, please check the following details:

Whether ISDN of the router is in ST_MULTIFR status.

Whether the B channel to be used by ISDN of the router is being used by other ISDN equipment.

Whether the called side is being used.

Besides these, the above debugging commands are used to examine whether the configuration is correct.

Dialup Prototype (Profile)

The dialer prototype separates logical interfaces from the ones answering for sending and accepting calls. In the dialer prototype, a physical interface and a logical interface are bound together according to each call, so that the different parameters of the physical interface can be chosen dynamically.

The prototype separates the logical part of DDR, such as network layers, encapsulation, and parameters relative to dialer, from the physical interfaces answering for sending and accepting calls.

Outline of the dialer protocol:

The dialer interface is a logical entity that uses the dialer prototype aimed at the destination.

The physical interface of the dialer prototype can be subject to many different dialer pools.

The included elements of a dialer interface:

Dialer interface

Dialer map-class

Dialer pool

Physical interface

Dialer Interface

A dialer interface is a logical entity that uses the dialer prototype aimed at the destination. The whole configuration directly to the destination will enter the configuration of the dialer interface and several dialer mappings can be designated for a single dialer interface. One dialer mapping can be associated with parameters aimed at different calls and these parameters are defined by respective mapping sets.

The following parameters are used to configure a dialer interface:

The IP address of the destination network

Encapsulating protocol

The remote dialer name (applied to PPP CHAP)

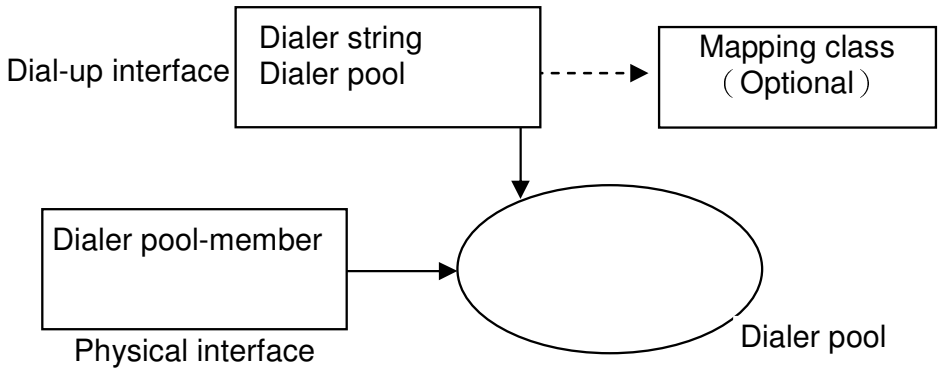
Dialer string or dialer mapping

Dialer pool number

Dialer group number

Dialer list number

The diagram below establishes a relation between parameters of the dialer prototype. The necessary configuring commands are listed below the diagram as well:



The configuring commands of the dialer prototype:

Command	Description
Ip address address mask	Configures the IP address.
dialer remote-name name	Designates the remote router name that will be used in CHAP authentication.
dialer string string class map-class-name	Defines the telephone number of the destination router and support the optional mapping class.
dialer load-threshold load	Interface load beyond which the dialer will initiate another call to the destionation
dialer hold-queue number-of-packets	Configures the number of outgoing packets to be queued
dialer pool number number	Associates the dialer interface with the dialer pool.
dialer-group guoup-number	Creates a dialer control list and define the trigger packets triggering DDR call.
ppp multilink	Designates that the dialer interface can employ the PPP multilink binding. The command used on the physical interface can be applied to the inward call; the command used in the dialer prototype can be applied to

	the outward call. If it can be applied either to the inward call or to the outward one, it should be used on both the dialer interface and the physical interface.

Dialer Map-class

Dialer map-class is an arbitrary element in the dialer prototype, and it can define a concrete call feature for the call to the destination designated by a dialer string.

The commands:

Command	Description
dialer fast-idle seconds	Prescribes all the clock value of the fast idle timeout, and the default is 20s.
dialer wait-for-carrier-time seconds	Prescribes the time used to wait for carrier waver. If no carrier waver is examined, the call will be discard.
dialer idle-time seconds	Prescribes the clock value of the idle timeout used by dialer, and the default is 120s.

Dialer Pool

Each dialer interface can refer to a dialer pool, which is a group of one or more physical interfaces associated with the dialer prototype.

A physical interface can belong to several dialer pools, and priority (Optional) can be configured for the physical interfaces included in the dialer pool to decide the sequence for choosing the interfaces.

Physical Interface

A physical interface is a real interface, and it is the command "dialer pool-member" that is used to associate a physical interface with a dialer pool, (of course, a physical interface can be associated with many dialer pools).

The commands on the physical interface:

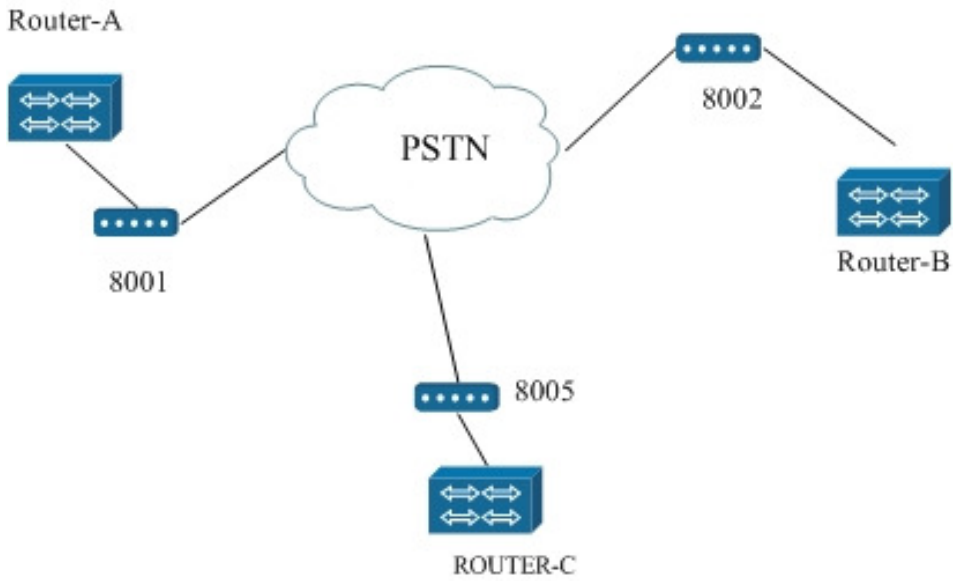
Command	Description
dialer pool-member number	The parameter "number" is the number of the dialer pool and is a decimal number within the range from 1 to 255.

priority priority	Configures the priority of the physical interfaces in the dialer pool. Choosing the interface with high priority to dial.
ppp authentication chap	Configures authentication.

Authentication needs to be configured on the physical interface;

The interface dialer of the dialer prototype supports PPP protocol.

Sample Configuration



In this figure, the router MP2600-1 connects with MP2600-2 and the MP2600-3 via a physical interface. You can use two dialer map of DDR to configure it. Of course, you can also choose our flexible DDR (dialer prototype) to achieve this function.

In such a small network, you may not feel the flexibility of the dialer prototype. But you will feel it in a large one because you can configure different parameters on different dialer interfaces so as to achieve different dialer aims without dialing circularly.

The configuration is as follows:

The configuration of router-1:

Command	Task
user goat password 7 [WOWWWNXSX	Configures the user name.

user Signamax password 7 [WOWWWNXSX user cisco password 7 [WOWWWNXSX	
ip access-list extended 1001 deny ip any 224.0.0.0 0.255.255.255 permit ip any any exit dialer-list 1 protocol ip list 1001	Defines a dialer access list and rules of it, only the data stream answering for related rule can dial.
interface dialer1 ip address 10.0.0.2 255.0.0.0 dialer remote-name Signamax dialer pool 1 dialer-group 1 encapsulation ppp dialer string 8005 exit	Defines a dialer interface: the remote-end authentication name is Signamax; the dialer pool is 1, and the dialed telephone number of the opposite end is 8005.
interface dialer2 ip address 20.0.0.2 255.0.0.0 dialer remote-name cisco dialer pool 2 dialer-group 1 encapsulation ppp dialer string 8001 exit	Defines a dialer interface: the remote-end authentication name is cisco; the dialer pool is 2, and the dialed telephone number of the opposite end is 8001.
interface serial3 physical-layer async speed 115200 databits 8 stopbits 1 parity none flow-control none dialer pool-member 1 dialer pool-member 2 ecapsulation ppp ppp authentication chap ppp chap hostname goat modem outer exit	Defines a physical interface that is associated with two dialer pools. Parameters of dialer pool 1 or 2 can be called, namely calling parameters of dialer1 port or dialer2 port that are associated with the dialer pools.

The configuration of SIGNAMAX ROUTER-2 and SIGNAMAX ROUTER-3:

SIGNAMAX ROUTER-2	Signamax router-3
user goat password 7 [WOWWWNXSX ip access-list extended 1001 deny ip any 224.0.0.0 0.255.255.255 permit ip any any exit dialer-list 1 protocol ip list 1001	user goat password 7 [WOWWWNXSX ip access-list extended 1001 deny ip any 224.0.0.0 0.255.255.255 permit ip any any exit dialer-list 1 protocol ip list 1001

Defines a dialer interface interface dialer1 ip address 10.0.0.1 255.0.0.0 dialer remote-name goat dialer pool 1 dialer-group 1 encapsulation ppp dialer string 8006 exit Associating the physical interface with the dialer interface interface serial3 physical-layer async speed 115200 databits 8 stopbits 1 parity none flow-control none dialer pool-member 1 encapsulation ppp ppp authentication chap ppp chap hostname Signamax modem outer exit	Defines a dialer interface. interface dialer1 ip address 20.0.0.1 255.0.0.0 dialer remote-name goat dialer pool 1 dialer-group 1 encapsulation ppp dialer string 8006 exit Associating the physical interface with the dialer interface interface serial3 physical-layer async speed 115200 databits 8 stopbits 1 parity none flow-control none dialer pool-member 1 encapsulation ppp ppp authentication chap ppp chap hostname cisco modem outer exit

In a large dialer network, you can use the dialer prototype to configure many dialer interfaces (dialer interface).

The ISDN network also supports the dialer prototype, and it can employ PPP multilink to bind many ISDN interfaces.

Configuring Snapshot Routing

This chapter explains how to configure snapshot routing on a router. Snapshot routing can be used to permit a single router in the active-time to exchange route information with a remote node and forbid the router in the quiet-time to exchange route information.

The main contents of this chapter are:

Related Description of snapshot routing configuration commands

An example of snapshot routing configuration

Debugging snapshot routing

Snapshot Routing Configuration Commands

clear snapshot quiet-time *interface*

The command can be used to end the quiet-time of CLIent router in two minutes.

Syntax	Description
interface	The interface name.

(By default) The interface makes transformation according to the time of snapshot status.

(Command mode)the global configuration mode

dialer map snapshot sequence-number dial-string
no dialer map snapshot sequence-number dial-string

The command can be use to define a dialer mapping for the snapshot routing protocol of client router connecting with the DDR interface, use the command. And use the negation of the command to delete a defined snapshot routing dialer mapping.

Syntax	Description
sequence-number	A number within 1 and 254, used to identify a unique dialer mapping.
dial-string	A phone number of a remote snapshot server. Dial up the number in the active-time.

(By default) No map is configured.
(Command mode)the interface configuration mode

snapshot client active-time quiet-time [suppress-statechange-updates] [dialer]

no snapshot client

Syntax	Description
active-time	The active time for regularly exchanging route upgrade between CLIent and server (by minute). Its value range is from 5 to 1000, and no default value is configured. 5 minutes is a used-usually value.
quiet-time	The quiet time there exists no route change. Its value range is from 8 to 100000, and no default value is configured. The minimal quiet time is active time+3.
suppress-statechange-updates	Deny the exchange of route upgrade when line protocol change from "non-active" to "active" or from "dialer pseudo" to "full-active."
dialer	If CLIent router should dialup to the remote router when there exists no routine information flow.

(By default) The snapshot routing is disabled.
(Command mode)the interface configuration mode

snapshot server active-time

no snapshot server

the command is used to configure a service router for snapshot routing. The negation of the command is used to deny the service router.

Syntax	Description
active-time	The active time for regularly exchanging route upgrade between CLIent and server (by minute). Its value range is from 5 to 1000, and no default value is configured. 5 minutes is a used-usually value.

Snapshot is supported only in the DDR dialup mode.

Snapshot Routing

As shown in figure above, the interface S1/0 of the router R1 connects with the interface of router R2 via PSTN. The RIP routing protocol is enabled on the link, snapshot routing is used to realize that the route information can be exchanged only in the active-time, and the RIP protocol is used to discover the route from the opposite end to the loopback interface L0.

R1 serves as the snapshot routing client, and R2 serves as the snapshot routing server. Related configuration is described as follows:
R1 is configured as follows:

Command	Task
In the global mode	
R1(config)#router rip R1(config-rip)#network 1.0.0.0 R1(config-rip)#network 4.0.0.0 R1(config-rip)#exit	Configure the RIP protocol.
R1(config)#ip access-list extended 1001 R1(config-ext-nacl)# deny ip any host 255.255.255.255 R1(config-ext-nacl)# deny ip any 224.0.0.0 0.255.255.255 R1(config-ext-nacl)# permit ip any any R1(config-ext-nacl)# exit R1(config)#dialer-list 1 protocol ip list 1001	Define DDR triggering data flow, shield broadcast and multicast packets so that they have no way to trigger DDR dialup.
In the interface configuration mode.	
R1(config-if-serial1/0)#ip add 1.1.1.1 255.255.255.0 R1(config-if-serial1/0)#dialer in-band R1(config-if-serial1/0)#dialer-group 1 R1(config-if-serial1/0)#dialer string 602	Configure related DDR operations, and set phone number and IP address.
R1(config-if-serial1/0)#phy async R1(config-if-serial1/0)#speed 115200 R1(config-if-serial1/0)#modem outer	Configure the modem (The ISDN dialup mode can also be adopted. About related configuration, refer to sections related with interface configuration)
R1(config-if-serial1/0)#snapshot client 5 600 dialer	Enable the Snapshot client, set active-time and quiet-time respectively as 5 minutes and 8 minutes.

R2 is configured as follows:

Command	Task
In the global configuration mode.	
R2(config)#router rip R2(config-rip)#network 1.0.0.0 R2(config-rip)#network 5.0.0.0 R2(config-rip)#exit	Configure the RIP protocol.
R1(config)#ip access-list extended 1001 R1(config-ext-nacl)# deny ip any host 255.255.255.255 R1(config-ext-nacl)# deny ip any 224.0.0.0 0.255.255.255 R1(config-ext-nacl)# permit ip any any R1(config-ext-nacl)# exit R1(config)#dialer-list 1 protocol ip list 1001	Define DDR triggering data flow, shield broadcast and multicast packets so that they have no way to trigger DDR dialup.
In the interface configuration mode	
R1(config-if-serial1/0)#ip add 1.1.1.2 255.255.255.0 R1(config-if-serial1/0)#dialer in-band R1(config-if-serial1/0)#dialer-group 1	Configure related DDR operations, and set phone number and IP address.
R1(config-if-serial1/0)#phy async R1(config-if-serial1/0)#speed 115200 R1(config-if-serial1/0)#modem outer	Configure the modem (The ISDN dialup mode can also be adopted. About related configuration, refer to sections related with interface configuration)
R2(config-if-serial1/0)#snapshot server 5	Enable the Snapshot server, set active-time as 5 minutes.

Monitoring & Debugging Snapshot Routing

show snapshot

The command is used to display the configuration information and status of Snapshot.

(Command mode)the privileged user mode

The following information will be displayed via the command:

```
serial4/2   Snapshot client
```

Options: Stay asleep on carrier up Dialer support

```
Length of active period:5
Length of quiet period:200
Length of retry period:8
 state: active, remaining time: 2 minutes
```

Explanations: The serial-interface s4/2 is CLIent and the snapshot status upgrade is denied when the interface is up. The snapshot is permitted to trigger DDR dialup. The status is the active time and remained time is 2 minutes.

debug snapshot
no debug snapshot

The command is used to enable/disable snapshot debugging information.
(Command mode)the privileged user mode

debug dialer
no debug dialer

The command is used to enable/disable DDR event debugging information.
(Command mode)the privileged user mode

debug dialer packet
no debug dialer packet

The command is used to enable/disable DDR packet debugging information.

(Command mode)the privileged user mode

debug dialer timer
no debug dialer timer

The command is used to enable/disable DDR timer debugging information.
(Command mode)the privileged user mode

PPPoE Configuration

Main contents of this section:

PPPoE Brief introduction

PPPoE basic command description

PPPoE client end and server configuration example

PPPoE monitoring and debugging

PPPoE protocol is a protocol which realizes PPP connection on Ethernet. A typical PPPoE application is PC connects LAN port via PPPoe dialing.

PPPoE basic command description

Command	Description	Configuration mode
pppoe enable	Enable PPPoE server	config-if-××
pppoe-client dial-pool-number *number*	Configure PPPoE client end	config-if-××
pppoe-client auto-start	Configure PPPoE auto dial	Config-if-XX
vpdn enable	*enable VPDN	config
vpdn-group *number*	Configure VPDN group	config
accept-dialin	*configure VPDN accepting dial-in	config-vpdn
protocol pppoe	*configure VPDN application protocol	config-vpdn-acc-in
virtual-template *number*	*configure VPDN accepting template number	config-vpdn-acc-in
local name *host-name*	Configure VPDN equipment name	config-vpdn

"*" before command means it has configuration example description.

configuration mode is: config, config-if-××(interface name) config-××(protocol name) etc.

pppoe enable

Use this command to monitor PPPoE packet from; or use no to forbidden. usually this command is used for PPPoE service end.

```
pppoe enable
no pppoe enable
(Default status)no definition
```

pppoe-client dial-pool-number

Use this command to monitor PPPoE packet and initiate PPPoE calling; no is used for forbidden. This command is usually used for PPPoE client end.

```
pppoe-client dial-pool-number pool-number
pppoe-client dial-pool-number pool-number ac-name ac-name
no pppoe-client dial-pool-number pool-number
```

Command	Description
pool-number	Dial pool number
ac-name	Access controller name(peer PPPoE server name)

(Default status)no definition

pppoe-client auto-start

auto dial function, PPPoE auto connects server when it is cut off. no is used for forbidden. This command is usually used for PPPoE client end.

```
no pppoe-client auto-start
```
(Default status)no definition

dialer idle-timeout time

Command	Description
time	Configure over time <0-2147483>

(Default status)2 minutes by default
vpdn enable

Enable VPDN function in order to user this function; no is used for forbidden.

```
vpdn enable
no vpdn enable
(Default status)no definition
```

vpdn-group

In order to use different VPDN mode, define vpdn-group; no is used for forbidden.

```
vpdn-group vpdn-group-number
no vpdn-group vpdn-group-number
```

Syntax	Description
vpdn-group-number	VPDN group name

(Default status)no definition

accept-dialin

Use this command to enable VPDN accepting dial-in function.

(Default status)no definition

local name

Use this command to differentiate other PPPoE server equipment; no is used for forbidden.

```
local name host-name
no local name host-name
```

Syntax	Description
host-name	LAC name

```
(Default status)no definition
```

protocol

Use this command to use special application protocol on VPDN; no is used for forbidden.

```
protocol pppoe
no protocol pppoe
```

Syntax	Description
vpdn-protocol	VPDN load application protocol (use PPPoE)

(Default status)no definition

virtual-template

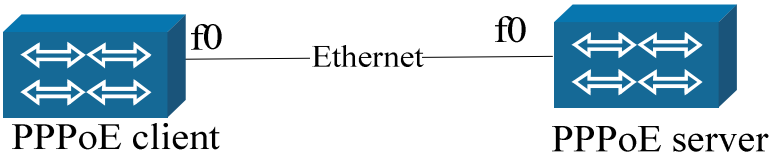
Use this command to configure VPDN load application parameters; no is used for forbidden.

```
virtual-template virtual-template-number
no virtual-template virtual-template-number
```

Command	Description
virtual-template-number	Designate virtual template number in the process of setting up dialogue.

(Default status)no definition

PPPoE configuration example



seeing as above, PPPoE client end connects PPPoE server Ethernet port via Ethernet.

PPPoE client end configuration

Command	Description
Router (config)#dialer-list 1 protocol ip permit	Configure dialer data type
Router (config)#interface dialer0	Configure dialer interface
Router (config-if-dialer0)#ip address negotiated	Configure IP address
Router (config-if-dialer0)# encapsulation ppp	Encapsulate PPP protocol
Router (config-if-dialer0)#dialer in-band	Enable DDR dialer
Router (config-if-dialer0)#dialer-group 1	Dialer list
Router (config-if-dialer0)#dialer pool 1	Configure dialer pool
Router (config-if-dialer0)# dialer idle-timeout 25	Configure timeout. 0 means no timeout.
Router (config-if-dialer0)#exit	Exit to interface
Router (config)#interface fastethernet0	Enter Ethernet interface
Router (config-if-fastethernet0)# pppoe-client dial-pool-number 1	Configure PPPOE client end, put F0 to dialer pool 1.
Router (config-if-fastethernet0)# pppoe-client auto-start	Configure auto dialer mode. if not, adopting data Dialing mode.
Router (config-if-fastethernet0)#exit	Exit to interface
Router (config)#ip route 0.0.0.0 0.0.0.0 dialer0	Configure default routing

PPPoE server configuration example:

Command	Description
Router(config)#int loopback 0	Configure loopback 0
Router(config-if-loopback0)#ip address 12.1.1.1 255.0.0.0	Configure loopback IP address
Router(config-if-loopback0)#exit	
router(config)# ip local pool pppoe-pool 172.16.20.10 172.16.20.100	Configure address pool
Router (config)#int virtual-template 1	Configure PPPoE virtual template interface
Router (config-if-virtual-template1)#ip unnumber loopback0	Configure interface IP address
Router (config-if-virtual-template1)#encapsulation ppp	Encapsulate PPP protocol
Router (config-if-virtual-template1)#peer default ip address pool pppoe-pool	Distribute IP address pool to client end
Router (config-if-virtual-template1)#exit	
Router (config)#vpdn enable	Enable VDPN virtual channel
Router (config)#vpdn-group 1	Set up virtual channel group
Router (config-vpdn)#local name pppoe-server	Use this command when configuring ac-name
Router (config-vpdn)#accept-dialin	Configure VPDN as accepting dial-in
Router (config-vpdn-acc-in)#protocol pppoe	Designate VPDN load application protocol
Router (config-vpdn-acc-in)#virtual-template 1	Designate PPPoE dialogue virtual template interface number
Router (config-vpdn-acc-in)#exit	
Router (config-vpdn)#exit	
Router (config)#interface fastethernet0	Configure fastethernet0 as PPPoE server port
Router (config-if-fastethernet0)#pppoe enable	Enable PPPoE protocol
Router (config-if-fastethernet0)#exit	

PPPoE monitoring and debugging

debug pppoe packets

Observe PPPoE negotiation packet status.
(command mode)privileged user mode

debug pppoe errors
(command mode)privileged user mode

debug pppoe events
Display event information in PPPoE negotiation process.

(command mode)privileged user mode

show pppoe session count
Display PPPoE dialogue statistics
(command mode)privileged user mode

show pppoe session information
Display PPPoE dialogue information.
(command mode)privileged user mode

IP Telephone Configuration

IP telephone configuration generally refers to the system that processes voice communication on an IP network. An IP telephone system has been integrated into Signamax's MP series routers. Users can use the IP telephone module provided by the router to process voice communication.

Signamax routers support the H.323 protocol family, the mainstream protocol of the IP telephone system. H.323 protocol family comprises H.225-Call Control Protocol, H.245-Multimedia Control Protocol, and RTP/RTCP --Realtime Transmission Protocol/Realtime Transmission Control Protocol.

This chapter explains how to configure the Signamax voice card, including how the FXS card accesses the PSTN/PBX via the FXO card, how the FXS cards intercommunicate between them, how to configure a Signamax router as the H.323 voice gateway, and some optional extended configurations.

The main contents of this chapter are as follows:

Configuring the voice card interface

Configuring voip

Configuring the Signamax router as the H.323 voice gateway

The Debugging Switch of IP telephone

Configure Voice Card Interface

Signamax's MP router series supports two kinds of voice cards:

FXS - Foreign eXchange Station interface card is used to connect general telephone or the exterior line of a mini PBX.

FXO — Foreign eXchange Office interface card is used to connect a PSTN telephone line or the interior line of a mini PBX.

The main topics discussed in this section are as follows:

commands

A simple configuration example

Commands

Command	Description
Codec <g723 / g729 / g711a>	This command is used to configure voice-coding type. There are G.723, G.729 and G.711a, to be selected, which correspond to different codings and compression algorithms. The typical ones are G.729 and G.723. If a kind of voice coding is selected, the router will negotiate voice coding first.
Volume <Number>	This number is the volume coefficient within the range 0-63. The larger the coefficient, the higher the volume.
connection-plar <STRING>	It is used only in the FXO card; string represents a telephone number. After the configuration is finished, once a ringing is detected on the FXO port, the telephone number is used as the called number and a call is directly originated to the remote terminal.
[no] shutdown	Configures opening/shutting down the voice port.
hot-line number <phonenum >	Configure hotline dial, only for FXS card.
hot-line wait-time <1-5>	Configure hotline waiting time, and the unit is second. Only for FXS card, together with hotline call command.
Jbuf <0_16>	Sets voice dynamic jitter buffer
maxpayloadnum <1-4>	Configure voice packet size
scf { disable | enable }	Configure whether enabling static voice compression. Disable this function by default.

voice-service fax-protocol t38	Configure IP phone fax protocol
voice-service t38-fax redundancy <0-2>	Configure IP phone fax protocol T38 redundancy
voice-service h323-start { fast| slow}	Configure voice gateway H323 protocol negotiation mode

Configuration

Configuring the FXS card (supposing that a new version router is being used)

Command	Task
Router(config)#voice-port 0/0	Configures the voice port 0/0.
Router(config-voice-port)#volume 28	Configures the volume coefficient as 28.
Router(config-voice-port)#codec g729	Configures the voice coding type as g729
Router(config-voice-port)#no shutdown	Opens the voice port.

The default configuration of voice port is shutdown.

Configuring VoIP

In the VoIP (Voice over IP) configuration, there is a conception dial-peer that is used to distinguish different types of session segments. There are two kinds of dial-peers:

POTS — A traditional telephone network peer, such as commonly used telephone interfaces, PSTN telephone line interface (Z interface), etc.

VoIP — IP network peers (passing via the IP network, related with the remote telephone segment.)

The main topics addressed in this section are:

commands
Usage of the basic commands
Usage of the extended configuration
A configuration example

Seeing the two kinds of dial-peers at the caller:

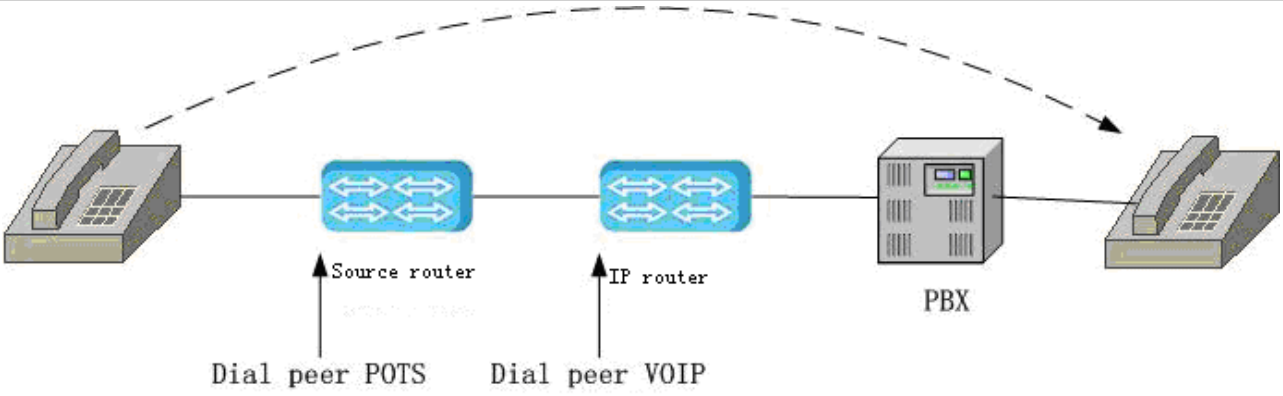
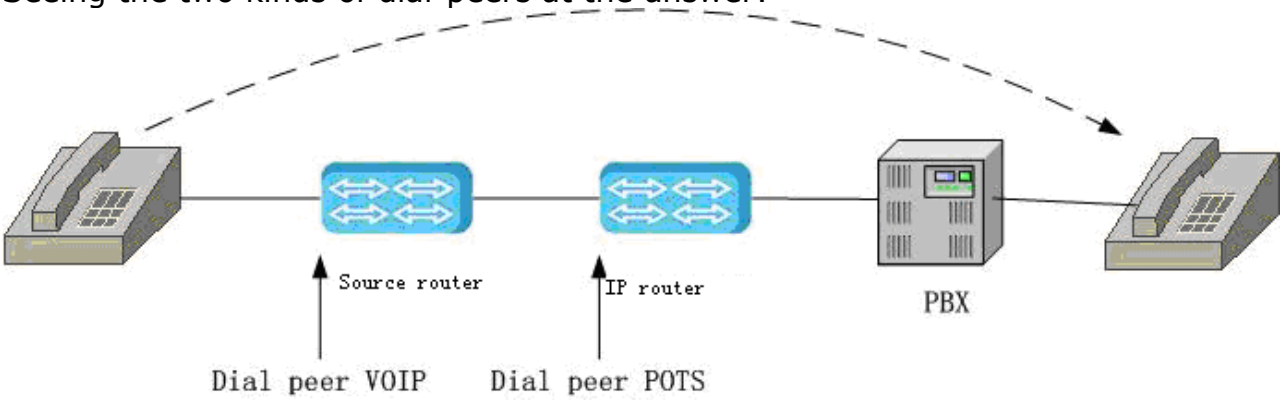


Figure 15-1

Seeing the two kinds of dial-peers at the answer:



Commands

```
Router#conf t
Router(config)#?
```

Command	Description
dial-peer <1_255> <pots/voip>	Configures the dialing map; 1-255 is the number of the session segment number; make configurations to the pots end or the voip end.

Configuring the pots end:

```
Router(config)#dial-peer 1 pots
Router(config-dial-peer)#?
```

Command	Description
destination-pattern <STRING>	Configures E.164 telephone number.
port <STRING>	Configures the voice port related to the pots end.

Configuring of the voip end:

```
Router(config)#dial-peer 1 voip
Router(config-dial-peer)#?
```

Command	Description
destination-pattern <STRING>	Configures E.164 telephone number.
session-target <STRING>	Configures IP address of the VoIP end.
dt	Configures the abbreviated dialing string or the extended dialing string.
req-qos { best-effort | controlled-load| guaranteed-delay }	Configure VOIP peer requiring QOS
supported-prefix <phonenum >	Configure VOIP phone number prefix supporting
dialplan terminator {*|#|time <1-10>|<CR>}	Configure local dial plan

VoIP Configuration Example

Configure POTS

```
Router(config)#
```

Command	Description
Dial－peer 1 pots	Enters the local number configuration mode.
destination-pattern 111	Configures the local number as 111.
Port 0/0	Configures the number 111 to be related with the voice port 0/0.

Configure VoIP

```
Router(config)#
```

Command	Description
Dial－peer 1 voip	Configures the opposite H.323 gateway/terminal.
destination-pattern 111	Configures the number of the opposite terminal as 111 (the number to be called).

Extended Configuration

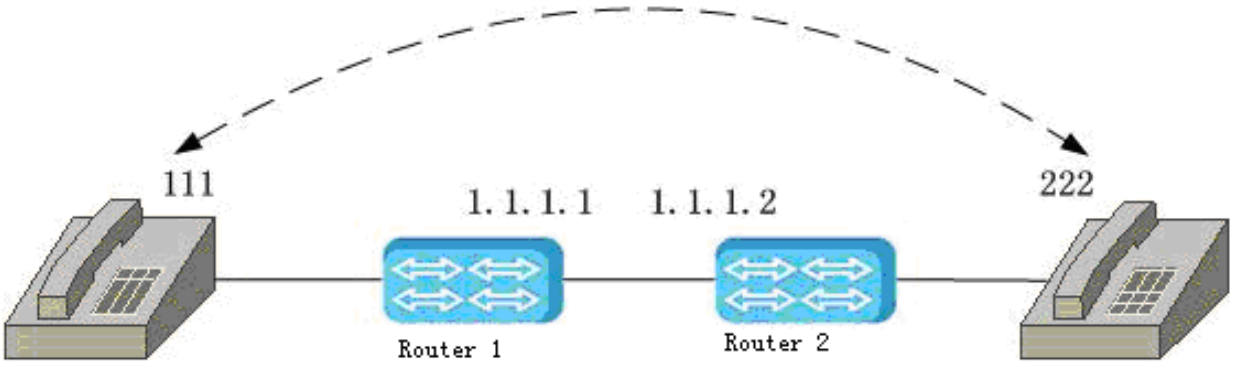
The explanations above describe the basic configuration of dialing an IP telephone, and the basic configuration used to achieve the voice communication on the IP network. For further understanding, below we provide some optional configurations. For example:

Abbreviated number dialing/extended number dialing

- Abbreviated number dialing
  Extension dialing allows users to really dial a longer number. For example, user dials 111, he can dial on 5148111.

Extended number dialing
It can satisfy the requisition that the numbers the mini switch prescribes are comparatively short and users get accustomed to dialing a certain format of number. For example, when users want to dial 5148222, they can simply dial the extension 222. Users will not notice the existence of the inner switch, instead, they will feel as though they are connecting directly with the PSTN network.

Example:



Router2 uses the abbreviated number dialing:

Command	Description
Router(config)#dial－peer 1 voip	Configures the opposite H.323 gateway/terminal.
Router(config)#destination-pattern 1	Configures the number to be dialed as 1.
Router(config)#session-target 1.1.1.1	Configures the IP address of opposite terminal.
Router(config)#dt 111	Configures the number related with the dialing1 as 1.

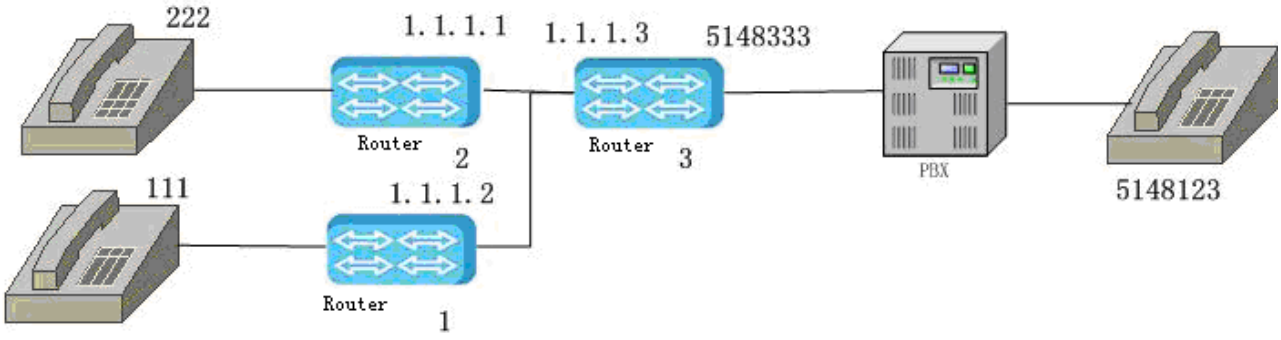
Router1 uses the extended number dialing:

Command	Description
Router(config)#dial－peer 1 voip	Configures the opposite H.323 gateway/terminal.
Router(config)#destination-pattern 5148222	Configures the number to be dialed as 5148222.
Router(config)#session-target 2.2.2.2	Configures the IP address of opposite terminal.
Router(config)#dt 222	Configures the number related with the dialing 5148222 as 222.

When a user dials the number "5148222", in fact he dials the telephone "222".

When a user dials the number after destination-pattern, in fact they are dialing the number after dt.

Configuration



In the above figure of configuration, both router1 and router2 have the built-in FXS modules, while router3 has a built-in FXO module. Supposing they are the new version of routers, and all the IP telephone modules are inserted in the port s2 and they use the channel 1.

This is an example about the intercommunication between the FXS module and the FXO, about the second dialing, and about the direct extension dial. When they are configured, the following tasks should be finished:

Configuring the pots end and the voip end

Configuring the voice interface

The appendix is about the usage of the extended configuration.

Configuring the pots end and the voip end

First, configure parameters of router1

Command	Task
Router#con t	
Router(config)#dial-peer 1 pots	Enters the local number configuration mode.
Router(config-dial-peer)#destination-pattern 111	Configures the local number as "111".
Router(config-dial-peer)#port 2/1	Configures the number "111"to correspond with the channel 2/1.
Router(config-dial-peer)#exit	
Router(config)#dial-peer 2 voip	Enters the voip configuration mode.
Router(config-dial-peer)#destination-pattern 222	Configures the number to be dialed.
Router(config-dial-peer)#session-target 1.1.1.2	Configures the IP address of the end to be dialed.
Router(config-dial-peer)#exit	
Router(config)#dial-peer 3 voip	
Router(config-dial-peer)#destination-pattern 9.....	Configures the opposite telephone number; the wildcard is used to match any number string.
Router(config-dial-peer)#session-target 1.1.1.3	Configures the IP address of the end to be dialed.
Router(config-dial-peer)#exit	

Second, configure parameters of router2:

Command	Task
Router#con t	
Router(config)#dial-peer 1 pots	Enters the local number configuration mode.
Router(config-dial-peer)#destination-pattern 222	Configures the local number as "222".
Router(config- dial-peer)#port 2/1	Configures the number "222" to correspond with the channel 2/1.
Router(config- dial-peer)#exit	
Router(config)#dial-peer 2 voip	Enters the voip configuration mode.
Router(config-dial-peer)#destination-pattern 111	Configures the number to be dialed.
Router(config-dial-peer)#session-target 1.1.1.1	Configures the IP address of the end to be dialed.

Router(config-dial-peer)#exit	
Router(config)#dial-peer 3 voip	
Router(config-dial-peer)#destination-pattern 9.....	Configures the opposite telephone number; the wildcard is used to match any number string.
Router(config-dial-peer)#session-target 1.1.1.3	Configures the IP address of the end to be dialed.
Router(config-dial-peer)#exit	

To configure parameters of router3:

Command	Task
Router#con t	
Router(config)#dial-peer 1 pots	Enters the local number configuration mode.
Router(config-dial-peer)#destination-pattern 9.....	Configures the local numbers as the wildcard strings beginning with "9".
Router(config- dial-peer)#port 2/1	Configures the number "9....."to correspond with the channel 2/1.
Router(config- dial-peer)#exit	
Router(config)#dial-peer 2 voip	Enters the voip configuration mode.
Router(config-dial-peer)#destination-pattern 111	Configures the number of the interior extension to be dialed on.
Router(config-dial-peer)#session-target 1.1.1.1	Configures the IP address of the end to be dialed.
Router(config-dial-peer)#exit	
Router(config)#dial-peer 3 voip	Enters the voip configuration mode.
Router(config-dial-peer)#destination-pattern 222	Configures the number of the interior extension to be dialed on.
Router(config-dial-peer)#session-target 1.1.1.2	Configures the IP address of the end to be dialed.
Router(config-dial-peer)#exit	

Configuring the voice interface
Router1 configuration is the same as that of router2

Command	Task
Router(config)#voice-port 2/1	Enters related voice port.
Router(config-voice-port)#codec g729	Configures the coding mode as g729.
Router(config-voice-port)#no shutdown	Activates the voice port.

The configuration of router3 is different depending on the modes of secondary dialing and direct extension dialing.

Command	Task
Router(config)#voice-port 2/1	Enters related voice port.
Router(config-voice-port)#codec g729	Configures the coding mode to be g729.

Router(config-voice-port)#no shutdown	Activates the voice port.
★Router(config-voice-port)#connection－plar 111	Once the exterior line dials up 5148333 successfully, the extension 111 will be connected directly.
★Router(config-voice-port)#connection－plar 222	Once the exterior line dials up 5148333 successfully, the extension 222 will be connected directly.
Router(config-voice-port)#exit	

If the command sentences are configured with "★" label, it is in the direct connection mode. The advantage of this mode is that it is easy for a user to operate, once the user successfully dials 5148333, he can dial 111/222 directly. The disadvantage is that it is fixed to dial up only one extension, namely that one voice interface only corresponds to only one connection-plar.

If the command sentences are not configured with the "★" label, it is in secondary dialing mode. After the exterior line successfully dials 5148333, he can choose the extension 111 or the extension 222 according to the record prompt (if there is record).

All numbers configuration can use the wildcard.

Appendix: Usage of the extended configuration:
The extended configuration of the router1 (using abbreviated number dialing/extended number dialing)

Command	Task
Router#con t	
Router(config)#dial-peer 1 pots	Enters the local number configuration mode.
Router(config-dial-peer)#destination-pattern 111	Configures the local number as "111".
Router(config- dial-peer)#port 2/1	Configures the number "111"to correspond with the channel 2/1.
Router(config- dial-peer)#exit	
Router(config)#dial-peer 2 voip	Enters the voip configuration mode.
Router(config-dial-peer)#destination-pattern 5148222	Configures the number to be dialed.
Router(config-dial-peer)#session-target 1.1.1.2	Configures IP address of the end to be dialed.
Router(config-dial-peer)#dt 222	Configures the number "222" that really corresponds to the number "5148222" dialed by users.
Router(config-dial-peer)#exit	
Router(config)#dial-peer 3 voip	

Router(config-dial-peer)#destination-pattern ...	Configures the telephone number of the opposite end and use the wildcard to match any number string.
Router(config-dial-peer)#session-target 1.1.1.3	Configures the IP address of the end to be dialed.
Router(config-dial-peer)#dt 95148...	Configures addition of "9" to any 7 bit number dialed by users.

The extended configuration of the router2 (using the dialing terminator):

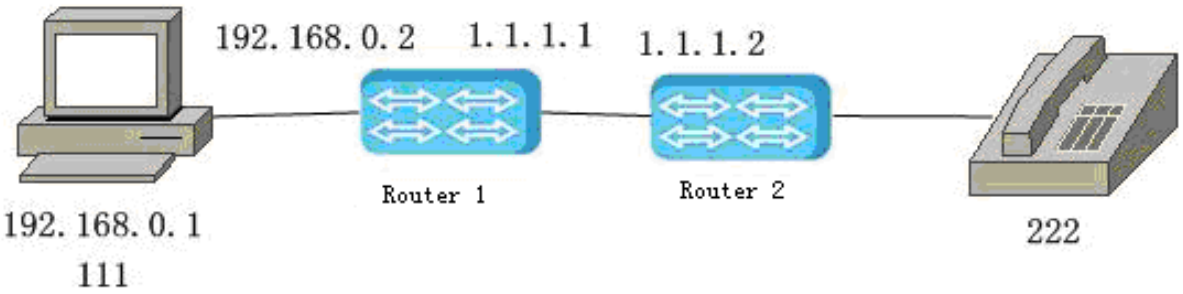
Command	Task
Router#con t	
Router(config)#dial-peer 1 pots	Enters the local number configuration mode.
Router(config-dial-peer)#destination-pattern 222	Configures the local number as "222".
Router(config-dial-peer)#port 2/1	Configures the number "222"to correspond with the channel 2/1.
Router(config-dial-peer)#exit	
Router(config)#dial-peer 2 voip	Enters the voip configuration mode.
Router(config-dial-peer)#destination-pattern 111	Configures the number to be dialed.
Router(config-dial-peer)#session-target 1.1.1.1	Configures IP address of the end to be dialed.
Router(config-dial-peer)#exit	
Router(config)#dial-peer 3 voip	
Router(config-dial-peer)#destination-pattern 9.....	Configures telephone number of the opposite end and use the wildcard to match any number string.
Router(config-dial-peer)#session-target 1.1.1.3	Configures the IP address of the end to be dialed.
Router(config-dial-peer)#exit	
Router(config)#voip_dial_terminator #	Configures the termination as "#".

When dialing "111", users should end it with "#", only so can the number really be dialed out.

When dialing 95148123 or 913912345678, users end it with "#", then the number will be sent out. This can achieve that all the numbers with different lengths can use the same one voip (the number of the wildcard point should be more than/equal to the longest number to be dialed, so does the pots wildcard of the router3)

If there is no dialing terminator, when users want to match both dialing of 5148123 and 139123456789, different voips need be configured. For example, the wildcard beginning with 8 matches the 7 bits numbers, while
the wildcard beginning with 9 matches the 11 bits numbers.

Configuration Example



In the above configuration, both Router 1 and Router 2 each contain built-in FXS modules. Supposing they are the new version of routers and two IP telephone modules are inserted into the interface S2 respectively and the channel 0 is employed.

This example is about the interconnection between the two FXS modules, when they are configured, the following tasks should be completed:

Configuring the pots end and the voip end

Configuring the voice interface

Configuring the pots end and the voip end

First configure parameters of router1:

Command	Task
Router#con t	
Router(config)#dial-peer 1 pots	Enters the local number configuration mode.
Router(config-dial-peer)#destination-pattern 111	Configures the local number as "111".
Router(config-dial-peer)#port 2/0	Configures the number "111" to correspond with the channel 2/0.
Router(config-dial-peer)#exit	
Router(config)#dial-peer 2 voip	Enters the voip configuration mode.
Router(config-dial-peer)#destination-pattern 222	Configures the number to be dialed.
Router(config-dial-peer)#session-target 1.1.1.2	Configures the IP address of the end to be dialed.
Router(config-dial-peer)#exit	

Second configuring parameters of router2:

Command	Task
Router#con t	
Router(config)#dial-peer 1 pots	Enters the local number configuration mode.
Router(config-dial-peer)#destination-pattern 222	Configures the local number as "222".
Router(config-dial-peer)#port 2/0	Configures the number "222"to correspond with the channel 2/0.
Router(config-dial-peer)#exit	
Router(config)#dial-peer 2 voip	Enters the voip configuration mode
Router(config-dial-peer)#destination-pattern 111	Configures the number to be dialed.
Router(config-dial-peer)#session-target 1.1.1.1	Configures the IP address of the end to be dialed.
Router(config-dial-peer)#exit	

Configuring the Voice Interface
Router1 configuration is the same as that of router2

Command	Description
Router(config)#voice-port 2/0	Enters related voice port.
Router(config-voice-port)#codec g729	Configures the coding mode as g729.
Router(config-voice-port)#no shutdown	Activates the voice port.

Configuring Signamax Router as H.323 Voice Gateway

A Signamax router can be used as the H.323 voice gateway, and can be used for the voice intercommunication between many IP networks or between an IP network and a telecommunications network, such as PSTN network etc. Signamax routers supports the RAS (Registration, Admission, Status) protocol, which is used to exchange information with the gatekeeper. Other functions, such as security, charging and Supplementary Services, will be provided in the subsequent version.

RAS Overview

RAS protocol:
RAS (Registration, Admission, Status) protocol is a protocol that runs between the H.323 gateway and the gatekeeper, and is used for call control and management, which comprises address resolution, address mapping, bandwidth management, call control, route management and security management.

Configure RAS Command List

A network interface is configured as the RAS protocol interface of the voice gateway, only one network interface can be configured as the voice interface. Configure the multicast mode on the network interface (for example, Ethernet interface) supporting multicasting to search for the gatekeeper. On the network interface (for example, WAN port) which does not support multicasting, only the designated gatekeeper IP address can be configured.

Router(config)#int s0

Command	Description
h323-gateway voip bind srcaddr <A.B.C.D>	Configure H323 gateway source IP address
h323-gateway voip interface	Designates this interface as the RAS protocol interface of the voice gateway.
h323-gateway voip h323-id <STRING>	Configures the gateway interface identifier that is used for the gatekeeper to identify the gateway interface.
h323-gateway voip id <STRING> <ipaddr/ multicast> <STRING/CR>	The first string is the gatekeeper ID, while the second string is the IP address that is configured after the ipaddr mode is chose.
h323-gateway voip supported-prefix <STRING>	Configures the gateway ID-prefix that is used for the gateway to process the session route, namely that the gatekeeper will route the telephone number beginning with this prefix to the gateway.
gateway	Enable H323 voice gateway function

H323 Voice Gateway Configuration Example

Command	Task
Router(config)#dial-peer 1 pots	Configures the pots end.
Router(config-dial-peer)#destination-pattern 7# 5219609	Configures the local gateway identifier as "7#" and the number as 5219609.
Router(config-dial-peer)#port 0	The number is bound with the voice interface 0.
Router(config-dial-peer)#exit	
Router(config)#dial-peer 2 voip	Configures the voice port of the opposite end.
Router(config-dial-peer)#destination-pattern 5213541	The opposite telephone
Router(config-dial-peer)#supported-prefix 8#	The destination gateway prefix identification
Router(config-dial-peer)#session-target ras	Designates that the RSA protocol is used to get the IP address of the destination telephone.
Router(config-dial-peer)#exit	
Router(config)#int f0	Configures the voice gateway interface.
Router(config-if-fastethernet0)#ip address 128.255.255.244 255.255.0.0	
Router(config-if-fastethernet0)#h323-gateway voip h323-id mp	Configures the gateway interface identifier.
Router(config-if-fastethernet0)#h323-gateway voip id gk multicast	Designates that the multicasting mode is used to search the gatekeeper.
Router(config-if-fastethernet0)#h323-gateway voip supported-prefix 7#	Configures the gateway identification prefix as "7#"
Router(config-if-fastethernet0)#h323-gateway voip interface	Designates that this interface is used as the RAS protocol interface of the voice gateway.
Router(config-if-fastethernet0)#no shutdown	
Router(config-if-fastethernet0)#exit	
Router(config)#gateway	Starts the voice gateway.

IP Telephone Debugging Switch

Command	Description
debug voipdrv <STRING> <all/busytone/events/resource/status>	Turns on an interface debugging switch. <String> is the voice interface to be monitored, the following words that can chosen are busytone, event or status of the monitoring interface, choosing all means turning on all the voipdrv debugging information of the interface.
debug phoneshell	Enable phone dial information debugging switch
debug h225 { asn1| events}	Enable H225 protocol debugging switch. events means signal negotiation process, ASN1 is the coding of H225 signal negotiation.
debug h245 { asn1| events}	Enable H245 protocol debugging switch. events means signal negotiation process, ASN1 is the coding of H245 signal negotiation.
debug h245 { sigs| events}	Enable H323 protocol debugging switch
autoscanbusytone voipdrv <STRING1> < STRING2>	Scan for busy tone. <STRING1>: VOS port connected PBX on router; <STRING2>: dial number, 1) PBX test method In config mode, input autoscanbusytone */* ??? (*/* is to access PBX VOS port, ??? is the number not existed on PBX) waiting for test result. 2) PBX test method In config mde, input autoscanbusytone */* ??? (*/* is to access PBX VOS port, ??? is extension number on PBX)

The voice interface monitored should be continuous up to a certain channel. For example, if there is a new version router, the voice interface should be of the form "0/1"; while if there is a old version router, then it should be of the form "0", "1" or "2" etc. The principle is that this voice interface form should be the same as that voice interface form seen by the command show run.

The wire order of the new version IP telephone:

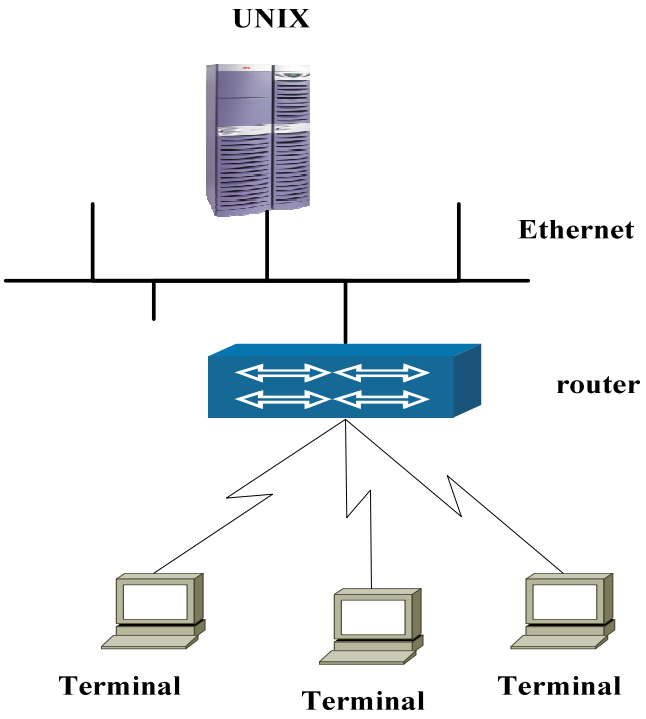
2vop and 2vos: RJ45 line with 8 wires, line4 and lind5 related to the channel 0; and line3 and lind6 related to the channel 1.

The IP telephone module with single port: RJ45 line with 8 pins of which the fourth and the fifth ones are used.

Terminal Confuguration

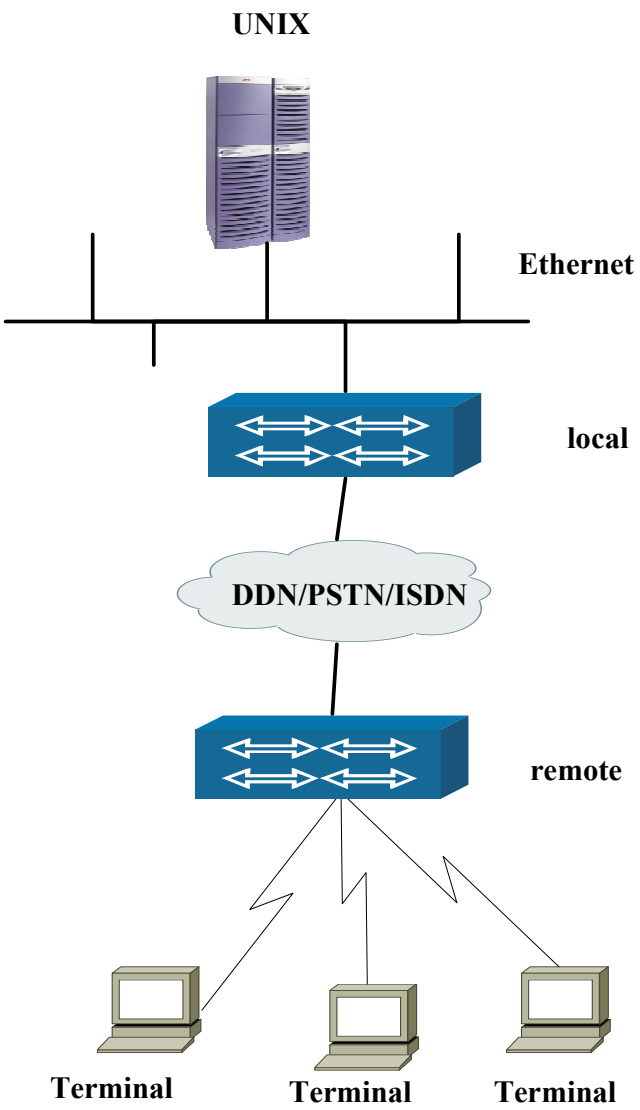
This chapter explains how to configure terminal, X.3 PAD on router. And also introduces ITEST server software configuration and usage suggestion of terminal.

Terminal Protocol



Terminal protocol working mode (local mode)

The figure above is the topology of the local terminal operation mode: the local router accesses the Ethernet via the Ethernet and connects with the Unix server; the synchronous/asynchronous interface or asynchronous interface encapsulates the terminal protocol and connects with the terminals.



Terminal protocol operation mode (the remote mode)

The figure above is the topology of the remote terminal operation mode: the remote router accesses the WAN via the WAN interface and connects with the local router via which the remote router connects with the Unix server. On the remote router, the synchronous/asynchronous interface or asynchronous interface encapsulates the terminal protocol and connects with the terminals.

Compared with the previous terminal access mode of Signamax router, the terminal protocol has gotten much enhancement at the aspects of function and flexibility and overcomes the limitation that nothing but the asynchronous interface module can access the terminal.

As long as the interface module supported by Signamax router can operate in the asynchronous mode (For example: frequency-band MODEM interface, high-speed synchronous/asynchronous serial interface), the interface can encapsulate the terminal protocol for terminal access.

The terminal protocol can, according to the user configuration or terminal service, specify the service-port of the host service for the establishment of TCP connection. When the client service data arrives, the router encapsulates the terminal data into TCP/IP messages, and sends them to host server via the TCP connection; at the same time, the terminal protocol monitors the data the server send, and the terminal protocol encapsulates the TCP/IP message and sends the service data to the terminal when the router receives the data sent from the server.

The terminal protocol can establish multiple TCP connections and realize the service switch of the terminal. Moreover, the terminal protocol can assist Itest or other fix-terminal program to realize the fix terminal-number access and data encryption and compression transmission, which can enhance service security.

Terminal Commands

Command	Description	Config mode
terminal template template-name	* set up terminal template	config
terminal local local-ip-address	*configure template local IP address	config-terminal-template
terminal remote host-number host-name host-ip-address domain-name {fix-terminal | telnet | rlogin}	*configure template remote service	config-terminal-template
terminal remote host-number host-name host-ip-address fix-terminal { tcp-port | authentication | compress | encrypt password | start-chars | negotiate-port | server}	*configure fixed terminal type service	config-terminal-template
terminal remote host-number host-name host-ip-address telnet { tcp-port | ANSI | VT100 | xenix }	*configure telnet type service	config-terminal-template
terminal remote host-number host-name host-ip-address rlogin [remote-user-name]	* configure rlogin type service	config-terminal-template
terminal auto-linking {host-number | off}	Auto linking (forbidden by default)	config-terminal-template
terminal { disable-remote-switch | enable-remote-switch }	Disable/enable user switching host (enable by default)	config-terminal-template
terminal hesc-chars [host host-number hesc-chars]	Terminal service switching and service shortcutting switching characters configuration (default is trl+G+D)	config-terminal-template
terminal print { on | off }	Print prompting and help information on	config-terminal-

	terminal (enable by default)	template
terminal redraw {host-number | console } redraw-char	Terminal redraw function	config-terminal-template
terminal retry-times retry-number	Terminal retry times (3 times by default)	config-terminal-template
terminal rx-delay	Accepting waiting (not wait by default)	config-terminal-template
terminal [rbufsize | tbufsize] buffer-size	TCP accepting and sending buffer size (accepting buffer is 2048 and sending buffer is 8192 by default)	config-terminal-template
terminal inactive-lock-time lock-time	Terminal inactive lock time (0 by default)	config-terminal-template
terminal close-after-switch	Close switched service connection.	config-terminal-template
encapsulation terminal	* interface encapsulates Terminal protocol	config-if-××
terminal noise-filter { ENABLE | DISABLE }	Whether enable the interface noise filter	config-if-××
terminal apply template-name interface1 interface2	Apply terminal template to protocol interface.	config
terminal restart { all | interface }	Restart terminal service	config
show terminal [activesocket | semaphore]	Display terminal socket or signal status	enable
debug terminal interface [[capability [{terminal | socket} [read | write | rw]] | [{terminal | socket} [read | write | rw]]]	Debug terminal interface information	enable
show ip sockets	Display system socket connection information	enable

Create Configuration Terminal Template

To make the router support the terminal access, it is necessary to configure terminal service parameters, such as the local IP address, remote service IP address and TCP port-number, and save the configuration into the terminal template.

After a terminal template has been created, all protocols supporting the terminal access, such as Terminal、MPDLC and X.25 PAD, can apply the template . And the modification of the template configuration can also update the status of the protocols applying the template.

Terminal template template-name

In the global configuration mode, use the command terminal template to create or enter a template. The parameter template-name is the template name. When there exists no the template, the template will be created and the user can enter the terminal template configuration mode(config- terminal-template). Use the command no terminal template template-name to delete the template.

The terminal name is case sensitive.
In the terminal template configuration mode, parameters related with terminal services can be configured, and the following commands can be supported.

Configure Terminal Local Address

Terminal local local-ip-address
Configure the local IP address of the template as the IP address of some interface of the router (generally the local IP address is the IP address of the loopback interface). The terminal protocol can regard the IP address as the source address and establish the TCP connection with the server.

Configure Terminal Remote Service

Terminal remote

- `terminal remote host-number host-name host-ip-address domain name{fix-terminal | telnet | rlogin}`

Syntax	Description
host-number	The remote service number, and its value scope is from 0 to 9.
host-name	The remote service name, displayed on the terminal selection interface.
host-ip-address	The IP address of the remote service.
domain name	The host domain name of the remote service.
fix-terminal	The remote service works in the fix-terminal mode (By default) .
telnet	The remote service works in the telnet mode.
rlogin	The remote service works in the rlogin mode.

When working in the fix-terminal mode, the remote service can support the following options:

- `terminal remote host-number host-name host-ip-address fix-terminal { tcp-port | authentication | compress | encrypt <string> | start-chars | negotiate-port | server}`

Syntax	Description
tcp-port	The TCP port number of the remote fix-terminal itest service. Its value range is from 1 to 65535 and the default port-number is 3051.
authentication	Router ID authentication (Namely the previous MAC address authentication, and no authentication is configured by default.)

compress	Compress the data
encrypt	Encrypt the data in the fix-terminal mode. After that, the key is also encrypted.
start-chars	The Fix-terminal auto-screen-brush character. It need be consistent with that the Itest configuration (nothing is configured by default.)
negotiate-port	Specify the negotiation port number for terminal connection in the fix-terminal mode.
server	The router serves as the server of the TCP connection and waits for client connection.

When the function of the auto-screen-brush is employed, parameters -r –k a1:a2:a3 need be configured when Itest starts. The parameter "-r" means enabling the screen memory. For —k a1:a2:a3, a1, a2 and a3 are hexadecimal numbers, and "0xa1 0xa2 0xa3" is configured behind "start-chars";

When the function of data compression is adopted, the option compress need be added into the Itest configuration file (itest.conf), and its format is described as follows:
/dev/ttyp53 196.72.167.4 com1 term2 compress;

When the encryption function is adopted, the option key=x (x represents the key value) need be added into the Itest configuration file (itest.conf), and its format is described as follows:
/dev/ttyp53 196.72.167.4 com1 term2 key=a;

In view of the security, the System ID related to the router can be configured on Itest. Only the terminal connecting with the specified router can log in the Unix server. It is necessary to add a MAC address into the Itest configuration file (itest.conf), and its format is described as follows:
/dev/ttyp53 196.72.167.4 com1 term2 mac 00017a450312;

The last item is the System ID of the router. It can be displayed by means of executing the command 'show version' on the router.

When the fix-terminal server is adopted, no remote address need be configured. The address used for TCP connection monitoring is the terminal local address. The remote address can be filled with any format of valid IP address.

When the fix-terminal server is adopted, no switching of service host need be performed usually. It is recommended that only one remote host need be configured. When working in the Telnet mode, the remote service supports the following options:

- `terminal remote host-no host-name host-ip-address telnet { tcp-port | ANSI | VT100 | xenix }`

Syntax	Description
tcp-port	The TCP port-number of the remote service. Its value range is from 1 to 65535 and the default value is 23.
ANSI	Telnet operates in the ANSI mode.
VT100	Telnet operates in the VT100 mode(By default) .
Xenix	Telnet operates in the xenix mode.

When working in the rlogin mode, the remote service supports the following options:

- `terminal remote host-no host-name host-ip-address rlogin remote-user-name`

Syntax	Description
Remote-user-name	The remote username of rlogin logon.

Configure Terminal Controlling Parameter

In the terminal template configuration mode, related configuration commands are described as follows:

- `terminal {auto-linking <0～9> | hesc-chars | host <0～9> hesc-chars | print { on | off } | redraw {<0～9> | console } <STRING> | retry-times <1～65535> | rx-delay | rbufsize <128～16384> | tbufsize <2048～16384> }`

Syntax	Description
auto-linking	Automatically establishing a link (Disabled by default)
hesc-chars	The terminal service switch character (the default character is "Ctrl+G+D")
host	The hot key of terminal host switch.
print	Print information about prompts and helps on the terminal (permitted by default)
redraw	The terminal redraw (the field STRING is the terminal screen-brush key, and different terminals define different terminal screen-brush keys)
retry-times	The retry times of establishing a link (three times by default).
rx-delay	The receiving delay, applied to the situation of using a card reader (no delay is configured by default).

tbufsize	The size of TCP transmitting buffer(8192 by default)
rbufsize	The size of TCP receiving buffer(2048 by default)

Interface Encapsulation Terminal Link Protocol

In the interface configuration mode, configure the command encapsulation terminal.

terminal noise-filter
The command is used to enable/disable the noise-filter of the interface. After the noise-filter is enabled, the noise interference, which is on the floating line and results from closing the RX/TX/GND terminal connection, can be avoided. The noise-filter is enabled by default.
terminal noise-filter { ENABLE | DISABLE }

(Command mode)the interface configuration mode.

The terminal protocol should operate in the asynchronous mode. For the synchronous/asynchronous serial interface mode, the configuration command physical async should be used to convert the physical layer into the asynchronous mode.

Neither IP address nor other IP property parameters can be configured;

After the terminal protocol is encapsulated, the default configuration tx-on dsr can be adjusted according to the physical signals of the terminal interface, such as tx-on dcd-dsr or tx-on cts;

No flow-control is configured by default. Generally, a terminal can receive nothing but the receiving, transmitting and GND signals, and support no hardware flow-control. The flow-control configuration can be modified according to the line condition and terminal performance.

The command terminal noise-filter can be used to filter out the start-character 00 or ff. In some applications, the 00 or ff character can be sent out in the beginning. Here, the noise-filter is disabled.

Applying Terminal Module to Terminal Protocol Interface

Adopt the command terminal apply template-name <interface1> <interface2> to apply the terminal template to the Terminal protocol interface <interface1> and<interface2>.

When a terminal template is applied to multiple interfaces, such as the two interfaces above, interface1 and interface2 should be two interfaces in the same slot.

Terminal Protocol Configuration Example

The local-end encapsulating the terminal protocol is configured as follows:

Configuring the interface parameters:

Command	Task
Router#config terminal	
Router(config)#int f0	Enter the configuration mode of the interface f0.
Router(config-if-fastethernet0)#ip add 129.255.24.100 255.255.0.0	Configure the Ethernet address of the router/ terminal server.
Router(config-if-fastethernet0)#exit	
Router#(config)interface serial0/0	The configuration mode of the serial-interface s0/0.
Router(config-if-serial0/0)#physical-layer async	The serial-interface s0/0 is configured as the asynchronous mode.
Router(config-if-serial0/0)#tx-on dcd	Configure the dcd signal to judge physical signal up.
Router(config-if-serial0/0)#encapsulation terminal	Encapsulate the terminal protocol.
Router(config-if-serial0/0)#exit	

The above is the configuration of encapsulating a high-speed serial interface as the terminal protocol, and the configuration of 8/16SA is the same as that of the high-speed serial interface.

Command	Task
Router#(config)interface serial1/0	The configuration mode of the serial-interface s1/0.
Router(config-if-serial1/0)#physical-layer async	
Router(config-if-serial1/0)#tx-on dcd	Configure the dcd signal to judge physical signal up.
Router(config-if-serial1/0)#encapsulation terminal	Configure the interface s1/0 (built-in modem) to encapsulate the terminal protocol.
Router(config-if-serial1/0)#modem party originate	Configure the built-in modem as the origination.
Router(config-if-serial1/0)#modem line leased	Configure the built-in modem as the automatic leased line mode.
Router(config-if-serial1/0)#modem async direct	Configure the built-in modem as the direct asynchronous mode.
Router(config-if-serial1/0)#modem enable	
Router(config-if-serial1/0)#exit	

The above is the configuration of the automatic leased line mode in which the built-in modem encapsulates the terminal protocol. The usage of this mode needs the cooperation with the mp56/336B external modem.

Command	Task
Router#(config)interface serial1/0	
Router(config-if-serial1/0)#physical-layer async	
Router(config-if-serial1/0)#tx-on dcd	Configure the dcd signal to judge physical signal up.
Router(config-if-serial1/0)#encapsulation terminal	
Router(config-if-serial1/0)#modem party originate	Set the built-in modem as call origination.
Router(config-if-serial1/0)#dialer string 123	Set the built-in modem as the dialup mode.
Router(config-if-serial1/0)#modem async error-correct	Set the built-in modem as error asynchronic.
Router(config-if-serial1/0)#modem enable	
Router(config-if-serial1/0)#exit	

The above is the configuration of the dialup mode in which the built-in modem encapsulates the terminal protocol. The usage of this mode needs the cooperation with the mp56/336B external modem.

Configuring Template Parameters:

Command	Task
Router(config)#terminal template signamax	Establish a template whose name is signamax.
router(config-terminal-template)#terminal local 129.255.24.100	Set the local IP address (the address of the interface f0).
router(config-terminal-template)#terminal remote 0 fix 129.255.100.101 fix-terminal	Set service 0 as the fix-terminal mode, the IP address as the IP of the Unix FEP (Front End Processors).
router(config-terminal-template)#terminal remote 1 telnet 129.255.100.101 telnet	Set service 1 as the telnet mode.
router(config-terminal-template)#terminal remote 2 rlogin 129.255.100.101 rlogin	Set service 2 as the rlogin mode.
router(config-terminal-template)#terminal remote 3 input 129.255.100.101 fix-terminal 7	Set service 3 as the echo mode. (Optional)
router(config-terminal-template)#terminal remote 4 fix-2 129.255.100.101 fix-terminal 3052 negotiate-port 3652	Set service 4 as 2nd fix-terminal mode. In the mode, Two itests are configured for Unix: data port—3052, and negotiation port—3652.
router(config-terminal-template)#exit	

Applying the template to an interface

Command	Description
Router(config)# terminal apply signamax serial0/0	Apply the template to the interface s0/0.

Terminal Debugging Commands

show terminal

debug terminal <interface>

terminal restart { all | <interface> }

show ip socket

Terminal Configuration

The configuration of encapsulating terminal:
Configure interface parameter:

Command	Description
Router#config terminal	
Router(config)#int f0	Enter interface f0 configuration mode
Router(config-if-fastethernet0)#ip add 129.255.24.100 255.255.0.0	Configure router/terminal server Ethernet address
Router(config-if-fastethernet0)#exit	
Router#(config)interface serial0/0	Serial s0/0 configuration mode
Router(config-if-serial0/0)#physical-layer async	Serial s0/0 configuration mode is asynchronous mode
Router(config-if-serial0/0)#tx-on dcd	Configure dcd physical signal up
Router(config-if-serial0/0)#encapsulation terminal	Encapsulate terminal protocol
Router(config-if-serial0/0)#exit	

Above is the configuration for high speed serial encapsulating terminal protocol, the configuration of 8/16SA is the same with high speed serial.

Command	Description
Router#(config)interface serial1/0	Serial s1/0 configuration mode
Router(config-if-serial1/0)#physical-layer async	
Router(config-if-serial1/0)#tx-on dcd	Configure dcd physical signal up
Router(config-if-serial1/0)#encapsulation terminal	Configure s1/0(built-in modem encapsulating terminal protocol
Router(config-if-serial1/0)#modem party originate	Configure built-in modem originated.
Router(config-if-serial1/0)#modem line leased	Configure built-in modem auto leased mode
Router(config-if-serial1/0)#modem async direct	Configure built-in modem directly asynchronous mode
Router(config-if-serial1/0)#modem enable	
Router(config-if-serial1/0)#exit	

Above is built-in modem encapsulating terminal protocol auto leased line mode, together with mp56/336B out-built modem.

Command	Description
Router#(config)interface serial1/0	
Router(config-if-serial1/0)#physical-layer async	
Router(config-if-serial1/0)#tx-on dcd	Configure dcd physical signal up
Router(config-if-serial1/0)#encapsulation terminal	
Router(config-if-serial1/0)#modem party originate	Configure built-in modem as dialing party
Router(config-if-serial1/0)#dialer string 123	Configure built-in modem dialer number
Router(config-if-serial1/0)#modem async error-correct	Configure built-in modem asynchronous error
Router(config-if-serial1/0)#modem enable	
Router(config-if-serial1/0)#exit	

Above is built-in modem encapsulating terminal protocol dialer mode, together with mp56/336B modem.

Template parameter configuration:

Command	Description
Router(config)#terminal template signamax	Create a template named signamax
router(config-terminal-template)#terminal local 129.255.24.100	Configure local ip address (f0 address)
router(config-terminal-template)#terminal remote 0 fix 129.255.100.101 fix-terminal	Configure service 0 as fixed terminal mode, ip address is unix ip
router(config-terminal-template)#terminal remote 1 telnet 129.255.100.101 telnet	Configure terminal remote 1 telnet
router(config-terminal-template)#terminal remote 2 rlogin 129.255.100.101 rlogin	Configure terminal remote 2 rlogin mode
router(config-terminal-template)#terminal remote 3 input 129.255.100.101 fix-terminal	Configure terminal remote 3 fixed terminal mode
router(config-terminal-template)#terminal remote 4 fix-2 129.255.100.101 fix-terminal 3052 negotiate-port 3652	Configure terminal remote 4 the second fixed terminal mode, and under this configuration, unix needs to configure two itest, for data and negotiation port 3052 and 3652.
router(config-terminal-template)#terminal remote 5 fix-3 fix.server.com fix-terminal	Configure terminal remote 5 the third fixed terminal mode, and under this configuration, configure service as fixed terminal, and the domain name can be local domain name and DNS domain name (if configuring DNS server address) .
router(config-terminal-template)#exit	

Apply template to interface:

Command	Description
Router(config)# terminal apply signamax serial0/0	Apply template to s0/0

Configure DNS server address:

Command	Description
router(config)# ip name-server 129.255.100.200	Configure DNS server address as 129.255.100.200

X.3 PAD Terminal

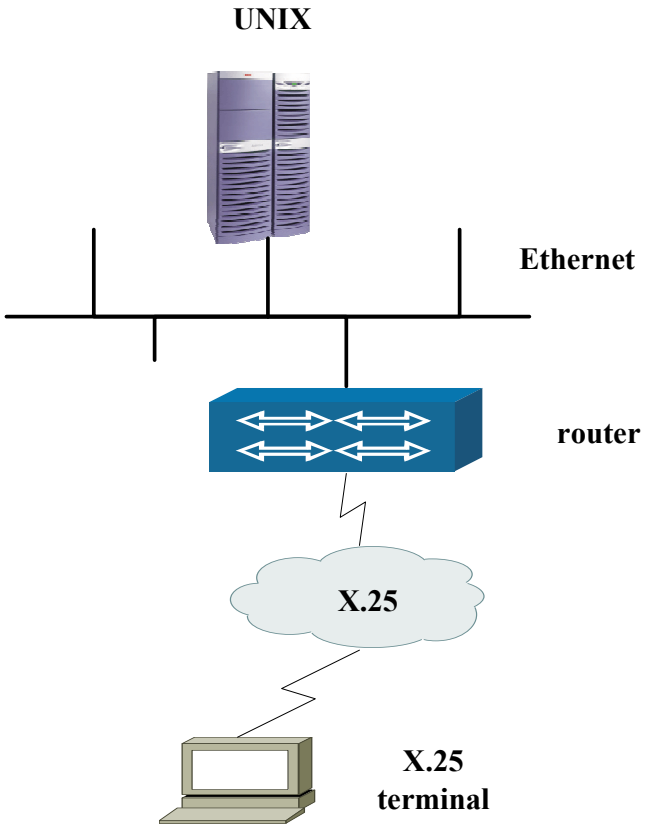
Main contents of this section:

Brief introduction of X.3 PAD

X.3 PAD basic command description

X.3 PAD configuration example

X.3 PAD Overview



X.3 PAD terminal network mode

X.3 PAD Terminal Commands

Command	Description	Config mode
terminal x.121-addr template-name COM TERM	* Apply terminal template to X.3 PAD.	config
debug x25 pad { packet | event }	Enable x.25 debugging information.	enable

show terminal	Display terminal information.	enable

Other configuration refers to the description of terminal part.

Creating/Configuring Terminal Template

The terminal template used by the X.3 PAD terminal is the same as the Terminal protocol. And about how to create and configure a terminal template.

Configuring X.25 Link-layer Protocol

Encapsulate X.25 link-layer protocol on the interface and configure related parameters.

Applying Terminal Template to X.3 PAD

In the global configuration mode, configure the command terminal x.121-addr template-name COM TERM and apply the terminal template template-name to X.PAD.

Command	Description
x.121-addr	The x.121 address of the remote PAD logon equipment.
template-name	The name of the applied terminal template.
COM	The COM number (user-defined) for using the function of fix-terminal.
TERM	The TERM number (user-defined) for using the function of fix-terminal.

Debugging Commands of X.3 PAD Terminal

debug x25 pad {packet | event }

show terminal

X.3 PAD Terminal Configuration

The configuration of the router and related explanation are described as follows:

Encapsulating related X.25 parameters (including X.25 address, DCE/DTE operation mode and internal/external clock) of a WAN interface;

The configuration commands of a terminal template are listed as follows:

Command	Description
terminal template <Temp-Name>	Create/configure a terminal template (the global mode command).
terminal local <ip-address>	Configure the local IP address.
terminal remote <0-9> Host-Name <ip-address>[telnet][rlogin][fix-term]	Configure the remote services: ten different services (0～9), telnet/rlogin/fix-term mode can be supported.
terminal hesc-chars	Configure the switching character string. And the default is "Ctrl+G+D".
terminal rx-delay	Set the receiving delay mode. The default mode is no delay.
terminal rbufsize <32-8192>	Set the size of the TCP receiving buffer. The default size is 2048 bytes.
terminal tbufsize <32-8192>	Set the size of the TCP receiving buffer. The default size is 8192 bytes.
terminal print <on/off>	Set terminal print as on: the prompts are printed on the terminal. The default configuration is ON.
terminal retry-times <1-255>	Set the maximal retry-times of establishing a link. The default value is 3 (times).

The coincidence relations among the terminal X.25 source address, terminal template and port number are listed as follows:

Command:	Task
terminal <x121-addr> <Temp-name> <com> <term>	<x121-addrs> : the X.121 address of the remote x25 equipment <termplate-name>:the name of the template used by the terminal <com> and <term>: parameters used by the fix-terminal. It should be consistent with the configuration of the application itest.

A configuration example:

Command:	Task
Router#(config)#interface fastethernet0	Configure the Ethernet address of the router.
Router(config-if-fastethernet0)#ip address 10.1.1.1 255.0.0.0	
Router(config-if-fastethernet0)#exit	
Router(config)#interface serial0/0	
Router(config-if-serial0/0)#physical-layer sync	Configure the synchronous mode.
Router(config-if-serial0/0)#clock rate 9600	Set the clock rate as 9600.
Router(config-if-serial0/0)#encapsulation x25	The interface is encapsulated with the X.25 protocol.
Router(config-if-serial0/0)#x25 dte	Configure the X.25 dte mode.
Router(config-if-serial0/0)#x25 address 1234567	Configure the X.121 address as 1234567.
Router(config-if-serial0/0)#exit	
Router (config) #terminal template signamax	Configure the template signamax.
Router (config-terminal-template) #terminal local 10.1.1.1	The local address of the template is 10.1.1.1.
Router (config-terminal-template) #terminal remote 1 fix-terminal 10.1.2.1 fix-terminal	The remote address of the terminal adopting the fix-terminal service is 10.1.2.1.
Router (config-terminal-template) #terminal remote 2 Telnet 10.1.3.1 telnet	The remote address of the terminal adopting the telnet service is 10.1. 3.1.
Router (config-terminal-template) #terminal remote 3 Rlogin 10.1.4.1 rlogin	The remote address of the terminal adopting the rlogin service is 10.1.4.1.
Router (config-terminal-template) #exit	
Router (config) #terminal 7654321 signamax 1 1	The x.121 address of the remote x.25 equipment is 7654321, and the name of the template used by the terminal is signamax, terminal com is 1 and terminal ter is 1.

ITEST Usage & Configuration

This section explains how to use ITEST service program and configure UNIX system, to realize fixed terminal and other functions, including the following contents:

ITEST program parameters

ITEST configuration file

ITEST security control

ITEST terminal management

TELNET fixed terminal

UNIX system(SCO,AIX,SUN,HP,LINUX etc.) configuration

UNIX system Administrate

ITEST Program Parameters

To realize the fixation of terminal equipment-number for TELNET, use the function of TELNET fix-terminal. For example, to fix the connection that adopts the telnet mode between 128.255.2.2 and the service port of Itest as "ttyp21", add the following row of configuration to the configuration file itest.conf:

```
/dev/ttyp21  128.255.2.2  comx  termx
```

Notice that what following com and term should be "x". and the other configuration (such as the configuration of the table inittab) is the same as that in the fix-terminal mode.

To telnet the fix-terminal from the rotuer, add the option telnet into the template configuration of the router. And Itest service port 3051 need also be added. For example:

```
terminal  remote  5  tel  129.255.11.110  telnet 3051
```

To telnet the fix-terminal from a PC, execute the following command:

```
telnet 129.255.11.110  3051
```

multiple terminals can be distributed to one IP address. For example, use the following the command to distribute ttyp21,ttyp22 and ttyp30 to 128.255.8.8:

```
/dev/ttyp21   128.255.8.8   comx   termx
/dev/ttyp22   128.255.8.8   comx   termx
/dev/ttyp30   128.255.8.8   comx   termx
```

When multiple telnet terminals are distributed to one IP address, it can be realized that only network terminal equipments can be fixed.

ITEST Configuration File

ITEST by default uses /etc/itest.conf configuration file (designate via -c config parameter, hereinafter named itest.conf) ,the configuration file is to configure the relation between physical terminal and the virtual terminal equipment in UNIX system. when the terminal requires connection, ITEST checks the effectives of this connection, and distributes virtual terminal equipment to terminal.

itest.conf is a normal text file, which can be edited by any text editing tool, and the basic format for configuration is as following:

virtual terminal equipment number router (terminal router) IP address COM number
TERM number others
For example:

Virtual terminal device	IP address	COM number	TERM number	Others
/dev/ttyp11	128.255.11.1	com1	term1	Such as encryption, compression, access list etc.
/dev/ttyp12	128.255.11.1	com2	term1	
/dev/ttyp21	128.255.11.2	com2	term1	
/dev/ttyp22	128.255.11.2	com3	term1	

each segment meanings is:

Segment Name	Description
Virtual terminal device	The virtual terminal device distributed to physical terminal, and this equipment should be under the directory of /dev/; it can be written as /dev/ttyp11 and /dev/ptyp11.
Router(terminal server) IP address	Configure the router (terminal server) IP address, which is terminal local address.
COM number TERM number	Configure the virtual terminal physical terminal interface, it adopts COM, TERM for identification, the number of COM, TERM can be shown via show terminal.
Other option	Configure other options, such as encryption, authentication code, compression, access list etc. the options refers to ITEST security control.

ITEST Security Control

Authentication
ITEST configures the authentication to access device, so only the designated router terminal can access up side UNIX server.
Add mac systemID after authenticated terminal in itest.conf configuration file. systemID is the ID of accessing router, which can be examined via show version.

Configuration example:

```
/dev/ttyp12  128.255.11.1  com1  term1   mac  00017a450312
```

Configure both in itest.com configuration file and router (terminal server). Which means add authentication key word after service host, such as:

```
terminal remote 1 abs 128.255.44.21 fix-terminal
authentication
```

encryption:
In order to enhance service data security, ITEST fixed terminal service supports the data encryption between UNIX server and remote router (terminal server).

The encryption function should be in itest.conf configuration file, and use key to configure encryption, and the format is: key=<keypass>.

Configuration example is as following:

```
/dev/ttyp12  128.255.11.1  com1  term1   key=mdi3IO9al6dM
```

terminal remote 1 abs 128.255.44.21 fix-terminal encrypt mdi3IO9al6dM

Compression:
In service application, the data amount from service program is very large, and in order to save bandwidth, configure compression for the data transmission.

Use compression function in itest.conf configuration file, and add compress after terminal configuration.

Configuration example is as following:

```
/dev/ttyp12  128.255.11.1  com1  term1   compress
```

Add compress after service host configuration, as:
terminal remote 1 abs 128.255.44.21 fix-terminal compress

Invalid time control
based on security, ITEST provides closing terminal function in fixed time. Use invalid time control needs to define a configuration file time.conf,and the format is as following:

```
all  12:00 13:00  18:00 20:00
```

The terminal is invalid in the time of 12:00 ~ 13:00 and 18:00 ~ 20:00.

```
ttyp11:ttyp12 12:00 13:00
```

Terminal ttyp11 and ttyp12 is invalid in the time of 12:00 ~ 13:00.

Designate time.conf configuration file when starting itest.

```
UNIX#  itest  -T /etc/time.conf
```

Invalid time configuration file is also uses action as an unit; it can designate 5 time sects, and use : among different terminals.

Time area access list
ITEST provides powerful time control function, to smartly control the terminal working time and non-working time.

When using time area control function, first add time access list configuration in itest.conf configuration file, and apply access list to the needed terminal.

Time control list configuration format is:

Keyword	ID number	action	Starting & ending year	Starting & ending week	Starting & ending time
Access-list	1	permit	2005.xx.xx-2005.xx-xx	1-5	08:00-12:00

Each segment meaning:

Segment Name	Description
Key word	access-list,the configuration of time control list
ID number	Time control list ID, the integer number bigger than 0.
Action	Permit or deny connection
Starting and ending year	Use "." to isolate the starting and end year. "x" means any year, month or day.
Starting and ending week	Starting and end week. "x" means the day from Monday to Sunday.
Starting and ending time	Starting and ending time.

After adding time access control list in itest.conf, add acl=xxx after the terminal. For example,

```
access-list  7  permit  xxxx.xx.xx-xxxx.xx.xx  1-5  08:00-18:00
        access-list  7  permit  xxxx.xx.xx-xxxx.xx.xx  6-7  09:00-16:00
/dev/ttyp12  128.255.11.1  com1  term1   acl=7
```

User binding
ITEST fixed terminal realizes the binding between physical terminal and virtual terminal, the user binding means binding the special user and system virtual terminal device, to limit the terminal for the special user.

User binding function is realized via accessional control program, at present, it has sctty and imon control programs.

sctty control program
Configure the relation between user and terminal login time. when the user logs in, sctty checks the relation, to realize user binding.

imon control program
getty is to realize special user auto login etc.

ITEST Terminal Management

Itest is a multi-process service program that brings some difficulties for process management, so the management control is enhanced in the program. The management process of itest runs on the TCP interface 3055(Use the parameter -m to specify other port) and enters the management mode.

Execute on the Unix:

telnet localhost 3055
telnet 127.0.0.1 3055

Execute on the remote terminal:

telnet ip-address 3055	Ip_addr is the IP address of the UNIX server.

By default, no username or password need be input for logging in the management port. To limit login, in the default situation, a user can log in the managing port without input the user name and password. The command itest –s can be used to limit users logging in when itest starts.

When a user wants to log in the management port, he will be asked to input his user name and password. Different users have different management rights, while the user root have all rights.

After the user enters the management mode, the prompt itest> is displayed; and the command help can be used to examine the command format:

Command	Description
Help	Display the command and the simple prompt.
Task	Display the status of each task.
Kill	Kill the terminal process (This command can be executed only by the root user).
disable	Disable a certain terminal.
enable	Enable a certain terminal.
term	Display all the effective configuration read from the file itest.conf.
pid	Display the process number related to each terminal.
time	Display the configuration of shutting down a terminal regularly.
refresh	Refresh the file itest.conf. The command of itest4.5 or higher version can support adding/deleting/modifying contents of itest.conf. And the command of previous version can only support adding contents of itest.conf.
debug	Monitor the terminal information.
undebug	Stop monitoring the terminal information.
stop	Stop the itest service, namely killing all the itest processes (This command can be executed only by the root user).
exit	Exit from the management mode, but the service itest still goes on operating.

The command kill:kill {pid | dev_name | A.B.C.D}

If the equipment number of some terminal is pty53 and related process number is 2045 (can be known by means of using the command 'pid'), the command kill p53 or kill 2045 can be used to kill the terminal process.

To kill all the terminal processes of some IP address (Assuming that the IP address is 196.77.8.2), the command kill 196.77.8.2 can be used to do it.

The command debug:debug ptypXX
Its debug information is written into the file /tmp/itest_dbg/ttypXX. This can be examined by the commands, such as more, vi, cat, and etc.。

TELNET Fix-terminal

To realize the fixation of terminal equipment-number for TELNET, use the function of TELNET fix-terminal. For example, to fix the connection that adopts the telnet mode between 128.255.2.2 and the service port of Itest as "ttyp21", add the following row of configuration to the configuration file itest.conf:

```
/dev/ttyp21  128.255.2.2  comx  termx
```

Notice that what following com and term should be "x". and the other configuration (such as the configuration of the table inittab) is the same as that in the fix-terminal mode.

To telnet the fix-terminal from the rotuer, add the option telnet into the template configuration of the router. And Itest service port 3051 need also be added. For example:

```
terminal  remote  5  tel  129.255.11.110  telnet 3051
To telnet the fix-terminal from a PC, execute the following
command:
telnet 129.255.11.110  3051
```

multiple terminals can be distributed to one IP address. For example, use the following the command to distribute ttyp21,ttyp22 and ttyp30 to 128.255.8.8:

```
/dev/ttyp21  128.255.8.8  comx  termx
/dev/ttyp22  128.255.8.8  comx  termx
/dev/ttyp30  128.255.8.8  comx  termx
```

When multiple telnet terminals are distributed to one IP address, it can be realized that only network terminal equipments can be fixed.

UNIX System Configuration

Configuring SCO UNIX

The default number of SCO UNIX virtual terminals is 64. To increase the number, execute the command netconfig to modify the SCO TCP/IP parameters:

Syntax	Description
Pseudo ttys: 256	The value is the maximum number of the UNIX system virtual terminals, and it should be more than the number of the really existing terminals.

Copy the fix-terminal service program itest.sco and place the copy into the directory "/ect". If the copy is sent out via ftp, it should adopt the binary mode.

Syntax	Description
chmod 744 itest.sco	Add the right to execute it to the user root.

Add the following sentences to the file /ect/rc.d/8/userdef. In this way, when starting, the system will start itest.sco automatically.

Syntax	Description
echo MP-Router Itest starting …	The prompt information at the time of startup
/ect/itest.sco	Execute itest.sco.
route add –net 128.255.130.0 –netmask 255.255.255.0 16.28.3.4	The route added into the router.

The italic sections of the command route add –net are the addresses of the network segment, at which the router is located, and the IP address of the up-end router connecting with the network fragment, and its aim is to add a route to the router to the UNIX server. The factual configuration depends on your concrete network address and IP address.

Create and configure the table itest.conf, then place it at the directory /ect for itest to distribute the terminal numbers. And its format is listed as follows:

/dev/ttyp11	128.255.130.254	com1	term1
……	……	……	……
/dev/ttyp18	128.255.130.254	com8	term1
/dev/ttyp21	128.255.130.254	com9	term1
……	……	……	……
/dev/ttyp28	128.255.130.254	com16	term1

The meaning of each field in the table above is described as follows:

Field	Description
/dev/ttyp11	It is the terminal equipment number distributed for related physical port, and the number should exist in the directory "/dev".
128.255.130.254	The IP address of the router connecting with the terminal (namely the local address configured on the terminal server)
com1	The serial-interface number (consistent with the value of COM that is displayed by means of the command show terminal)
term1	The terminal number (consistent with the value of TERM that is displayed by means of

	the command show terminal)

Configure the table "/ect/inittab" so as to determine whether to send the login interface to the terminal.

p11:234:respawn:/ect/getty /dev/ttyp11 m
p12:234:off:/ect/getty /dev/ttyp12 m
……

The meaning of each field in the table above is described as follows:

Field	Description
p11	The ID domain. It can be defined by users and serve as the parameter following enable/disable. The manager can use the enable ID to activate this terminal and send the login interface.
234	The operation level. It specifies that when running in system running levels 2,3,4, the sentence is valid.
respawn/off	The action domain. When users adopt the login mode to log in, the domain need be configured as respawn, and when users want to send an application interface to the terminal, the domain need be configured as off.
/ect/getty /dev/ttyp11 m	The command domain. It specifies some action executed for some port-number. In this example, the login interface is sent to the terminal ttyp11, and m indicates that the terminal speed is 9600.

Configure the table /ect/ttytype so as to provide the terminal type configuration for application programs. The format is listed as follows:

Terminal Type	Terminal No
Vt1 00	ttyp11
Ansi	ttyp21

Configuring AIX UNIX

Increase the number of the BSD-style pseudo terminals:
Means:Use the command smit—Devices—Pty—Change/show Characteristies …— to modify the number of the BSD-style pseudo terminals more than the number of the really used terminals.

Copy the fix-terminal service program itest.aix and place the copy into the directory "/ect". If the copy is sent out via ftp, it should adopt the binary mode.

Command	Description
chmod 744 itest. aix	Add the right to execute it to the user root.

Add the following sentences to the file /ect/rc.tcpip. In this way, when starting, the system will start itest.aix automatically.

Command	Description
echo MP-Router Itest starting …	The prompt information at the time of startup
/ect/itest.aix	Execute itest.aix.
route add –net 128.255.130.0 –netmask 255.255.255.0 16.28.3.4	The route added to the router.

The italic sections of the command route add –net are the address of the network fragment at which the router is located and the IP address of the up-end router connecting with the network segment, and the aim of this section is to add a route to the router to the UNIX server. And the factual configuration depends on your concrete network address and IP address.

Create and configure the table itest.conf, then place it into the directory /ect for itest to distribute the terminal numbers. Its format is as follows:

/dev/ttyq0	128.255.130.254	com1	term1
……	……	……	……
/dev/ttyq7	128.255.130.254	com8	term1
/dev/ttyq8	128.255.130.254	com9	term1
……	……	……	……
/dev/ttyqf	128.255.130.254	com16	term1

The meaning of each field in the table above is described as follows:

Field	Description
/dev/ttyq0	It is the terminal equipment number distributed to related physical port, and it should exist in the directory /dev.
128.255.130.254	The IP address of the router connecting with the terminal (namely the local address configured on the router)
com1	The serial-interface number (consistent with the value of COM that is displayed by means of the command show terminal)
term1	The terminal number (consistent with the value of TERM that is displayed by means of

	the command show terminal)

Configure the table /ect/inittab so as to determine whether to send the login interface to the terminal:

Q1:234:respawn:/usr/sbin/getty /dev/ttyq1
Q2:234:off:/usr/sbin/getty /dev/ttyq2
……

The meaning of each field in the table above is described as follows:

Field	Description
Q1	The ID domain. It can be defined by users and serve as the parameter following penable/pdisable; The manager can use the penable ID to activate this terminal and send the login interface.
234	The operation level. It specifies that when running in system running levels 2,3,4, the sentence is valid.
respawn/off	The action domain. When users adopt the login mode to log in, the domain need be configured as respawn, and when users want to send an application interface to the terminal, the domain need be configured as off.
/usr/sbin/getty /dev/ttypq1	The command domain. It specifies some action executed for some port-number. In this example, the login interface is sent to the terminal ttyp11.

Configure the table /ect/ttytype so as to provide the terminal type configuration for applications. The format is described as follows:

Terminal Type	Terminal No
Vt100	ttyq1
Ansi	ttyq2
……	

Configuring SUN UNIX

Increase the number of the SUN system pseudo terminals. The default number of the SUN system pseudo terminals is 48. To increase the number, you can do according to the following steps (in this example, increasing the pseudo terminal number to 128):

Adding this line set npty=128 at the place of the file /ect/system where the core variable is changed.
Edit the file /ect/iu.ap, and modify ptsl 0 47 ldterm ttcompat as ptsl 0 127 ldterm ttcompat.
Execute the command boot –r to restart the system.

Copy the fix-terminal service program itest.sun and place the copy into the directory /ect. If the copy is sent out via ftp, it should adopt the binary mode.

Command	Description
chmod 744 itest.sun	Add the right to execute it to the user root.

Add a startup execution file Sitest (Noticing the capital letter S) into the directory of /ect/rc3.d, and add the right to execute it so that the fix-terminal service program itest.sun can start when the system starts. Contents of the file are described as follows:

Command	Description
echo MP-Router Itest starting …	The prompt information at the time of startup
/ect/itest.sun	Execute itest.sun.
route add –net 128.255.130.0 –netmask 255.255.255.0 16.28.3.4	Add the route to the router/terminal server.

The italic sections of the command route add –net are the address of the network fragment at which the router is located and the IP address of the up-end router connecting with the network segment, and the aim of this section is to add a route to the router to the UNIX server. And the factual configuration depends on your concrete network address and IP address.

In the SUN system, when the types of machines are different, some files may well run abnormally. Related execution file need be regenerated according to its type. To do it, please communicate with the technical staff of our company.

Create and configure the table itest.conf, then place it into the directory /ect for itest to distribute the terminal numbers. Its format is listed as follows::

/dev/ttyq0	128.255.130.254	com1	term1
……	……	……	……
/dev/ttyq7	128.255.130.254	com8	term1
/dev/ttyq8	128.255.130.254	com9	term1
……	……	……	……
/dev/ttyqf	128.255.130.254	com16	term1

The meaning of each field in the table above is described as follows:

Field	Description
/dev/ttyq0	It is the terminal equipment number distributed for related physical port, and it should exist in the directory /dev.
128.255.130.254	The IP address of the router connecting with the terminal (namely the local address configured on the terminal server)
com1	The serial-interface number (consistent with the value of COM that is displayed by means of the command show terminal)
term1	The terminal number (consistent with the value of TERM that is displayed by means of the command show terminal)

Configure the table /ect/inittab so as to determine whether to send the login interface to the terminal.

Q1:234:respawn:/usr/lib/saf/ttymon –g –h –p "`uname –n`login: " -T ansi –d /dev/ttyq1
Q2:234:off:/usr/lib/saf/ttymon –g –h –p "`uname –n`login: " -T ansi –d /dev/ttyq2
……

The meaning of each field in the table above is described as follows:

Field	Description
Q1	The ID domain. It can be defined by users and serve as the parameter following penable/pdisable； The manager can use the penable ID to activate this terminal and send the login interface.
234	The operation level. It specifies that when running in system running levels 2,3,4, the sentence is valid.
respawn/off	The action domain. When users adopt the login mode to log in, the domain need be configured as respawn, and when users want to send an application interface to the terminal, the domain need be configured as off.
/usr/lib/saf/ttymon –g –h –p "`uname –n`login: " -T ansi –d /dev/ttyq1	The command domain. It specifies some action executed for some port-number. In this example, the login interface is sent to the terminal ttyp11. ("`" of "`uname –n`" is not a single quotation marks but an inverse single quotation marks)

Configure the table /ect/ttytype so as to provide the terminal type configuration for applications. The format is described as follows:

Terminal Type	Terminal No
Vt100	ttyq1
Ansi	ttyq2

Configuring HP UNIX

Increase the number of the HP system pseudo terminals. To increase the number of the system pseudo terminals, you can do according to the following steps (in this example, increasing the pseudo terminal number to 128):

Use the command smitty and select "Devices → Pty→Change/Show Characteristies", modify the number of the BSD-style pseudo terminals as 128.

Copy the fix-terminal service program itest.hp and place the copy into the directory /ect. If the copy is sent out via ftp, it should adopt the binary mode.

Command	Description
chmod 744 itest.sun	Add the right to execute it to the user root.

In the HP system, when the types of machines are different, some files may well run abnormally. Related execution file need be regenerated according to its type. To do it, please communicate with the technical staff of our company.

Add a sentence into startup execution file /sbin/rc so that the fix-terminal service program itest.hp can start when the system starts. The added contents are described as follows:

Command	Description
echo MP-Router Itest starting …	The prompt information at the time of startup
/ect/itest.hp	Execute itest.hp.

Create and configure the table itest.conf, then place it into the directory /ect for itest to distribute the terminal numbers. Its format is listed as follows::

/dev/ttyq0	128.255.130.254	com1	term1
……	……	……	……

/dev/ttyq7	128.255.130.254	com8	term1
/dev/ttyq8	128.255.130.254	com9	term1
.....	.....	.....	.....
/dev/ttyqf	128.255.130.254	com16	term1

The meaning of each field in the table above is described as follows:

Field	Description
/dev/ttyq0	It is the terminal equipment number distributed for related physical port, and it should exist in the directory /dev.
128.255.130.254	The IP address of the router connecting with the terminal (namely the local address configured on the terminal server)
com1	The serial-interface number (consistent with the value of COM that is displayed by means of the command show terminal)
term1	The terminal number (consistent with the value of TERM that is displayed by means of the command show terminal)

Configure the table /ect/inittab so as to determine whether to send the login interface to the terminal.

Q1:234:respawn:/usr/lib/saf/ttymon –g –h –p "`uname –n`login: " -T ansi –d /dev/ttyq1
Q2:234:off:/usr/lib/saf/ttymon –g –h –p "`uname –n`login: " -T ansi –d /dev/ttyq2
……

The meaning of each field in the table above is described as follows:

Parameter	Description
Q1	The ID domain. It can be defined by users and serve as the parameter following penable/pdisable；The manager can use the penable ID to activate this terminal and send the login interface.
234	The operation level. It specifies that when running in system running levels 2,3,4, the sentence is valid.
respawn/off	The action domain. When users adopt the login mode to log in, the domain need be configured as respawn, and when users want to send an application interface to the terminal, the domain need be configured as off.
/usr/lib/saf/ttymon –g –h –p "`uname –n`login: " -T ansi –d /dev/ttyq1	The command domain. It specifies some action executed for some port-number. In this example, the login interface is sent to the terminal ttyp11. ("`" of "`uname –n`" is not a single quotation marks but an inverse single quotation marks)

After some kernel parameters are changed in some Unix systems (such as the SCO system), the kernel parameters need to be reconnected. Because each time the kernel is reconnected, the system will use "/ect/conf/cf.d/init.base" to conver init.base automatically, and and the manual configuration of the table will be lost. Thereby, after finishing the configuration, you should backup the table inittab. As long as you copy the table inittab to cover init.base, then the inittab configuration will not be lost when the system reconnects

In the course t, after itest started up, the modification made in the table itest.conf cannot take effect immediately unless using the command refresh in the managing mode

Whenever the configuration of the table inittab has been modified, to make the modification take effect in the situation UNIX doesn't restart, you should use the command init q to make the system scan the table again.

Once some Unix systems start up, they will occupy the pseudo terminals. So when the table itest.conf is configured, the pseudo terminal number should start behind the pseudo terminal number occupied by the system. And it is recommended that some numbers should be reserved.

UNIX system Administrate

When many terminals are connected with the UNIX server and there exist many services, it may occur that the default kernel resource of the server isn't enough, which will result in various kinds of bugs. To ensure the system to run securely and reliably, each kernel parameter of the UNIX server need be reconfigured and the distributed quantity of the resource should be increased.

Take how to adjust default kernel resource of the SCO UNIX 5 as an example:

Run netconfig and modify the two SCO parameters included by TCP/IP

Parameter	Description
TCP connections : 1024	The maximum connection number. In the version itest v3, each Itest terminal occupies a TCP connection after login. Because other system applications can also occupy TCP connections, so it is recommended that the parameter value is configured as more than 1024.
Pseudo ttys :256	The number of the system virtual terminals. It is recommended that the number is more than 256.

Run the command scoadmin-Hardware/Kernel Manager-Kernel|Tune Parameters… to enter the menu of the core parameters setting:
Select 7. Use the command User and group configuration to modify the following parameters:

Parameter	Description
NOFILES	The maximum number of the files each process can open. For every terminal in the version itest v3, after the terminal logs in, the number of the files opened by the process itest increases 2. It is recommended that the parameter should be 3 times of the number of terminals.
MAXUP	The maximum number of the processes. Because the system itself occupies some processes, it is recommended that the parameter value should be more than 800.

Select 12. Use the command Streams to modify the following parameters:

Parameter	Description
NSTREAM	The number of the stream header structures. If there are more than 150 terminals to be configured, it is recommend that the parameter should be configured as 6000.
NSTRPAGES	The number of the pages. 4k per page. If there are more than 150 terminals to be configured, it is recommend that the parameter should be configured as 3000.
STRSPLITFRAC	If this value is too little, the stream buffer of the system will become scraps soon. So it is recommend that the parameter should be configured as 80.

Select 3. Use the command TTYs to modify the following parameters:

Parameter	Description
NCLIST	The number of the character table buffers. it is recommend that the parameter should be configured as 2048.

The command netstat –m can be executed to examine the usage of the system stream resource. When some item occurs FAIL, the values of parameters NSTREAM and NSTRPAGES need be increased.

When there exists the prompt "Too many open files" in /tmp/itest.log, the value of the parameter NOFILES need be increased.

Comparison of New/ Old Version of IOS Configuration

Comparison of Terminal Number Distribution

For Signamax router, the distribution of COM/TERM number related to V2.X.X or previous version of terminals is different from that of V3.X.X or higher version. It is noticeable that related contents of the file itest.conf should be configured according to the COM/TERM number distributed to each interface. For V.X.X or higher version of IOS, the following two modes can be used to get the COM/TERM number distributed to an interface:

The fist mode: after the interface is encapsulated with the terminal protocol, the command show interface <> can be used to examine the COM/TERM number:

For example:mp2600#show intface s1/0

```
serial1/0:
     Flags: (0xd0) DOWN POINT-TO-POINT TRAILERS RUNNING
     Type: TERMINAL
     Queue strategy: FIFO Output queue: 0/40 (/max packets)
      ……..
     TERMINAL STATE:  CLOSE, Flag = 0x0, COM 34, TERM 1
      ……..
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up  TxC=up
```

The second mode: after the interface is encapsulated with the terminal protocol and executes the terminal template, the command show terminal <> can be used to examine the COM/TERM number:

```
      mp2600#shos terminal
TermService version: 2.41
-------------------------------------------------------------
----------
                Interface  Type   COM/TERM     State
Template   RH-State

[0123456789]
-------------------------------------------------------------
----------
          1:  async4/0    T       1/1      WAITING
itest43     D DDDDDDD
          2:  async4/1    T       2/1      WAITING
```

```
itest43      D DDDDDDD
          3:  serial1/0     T        34/1         CLOSE
-------------------------------------------------------------
----------
Type: T - Terminal,  M - MPDLC
RH-State:  D - DISCONNECT,  C - CONNECTING, * - CONNECT
```

Comparison of Interface Configuration

For the new version, after the interface is encapsulated with the terminal protocol, the command tx-on dsr will be added automatically. And the command can be removed by means of using the command no tx-on dsr. Notice that when the terminal interface is the modem interface or the interface connects with the external modem the command is tx-on dcd instead of tx-on dsr.

Configuration of Itest.conf Adopting Encryption and Compression

Itest4.2 or higher version of Itest can support data encryption and compression. The configuration of the router can refer to section 1.1.1. For the configuration of itest.conf on the Unix server, the following configuration need be added (Be care of case sensitive):

Data encryption: Add "key=x" behind comx termx of the file itest.conf. For example:

/dev/ttyp21	128.255.130.254	com9	term1 key=a

Data compression: Add compress behind comx termx of the file itest.conf. For example:

/dev/ttyp18	128.255.130.254	com8	term1 compress

Data encryption and compression: Add both "key=x" and compress behind comx termx of the file itest.conf.(There exists no requirement to the order of the added items) For example:

/dev/ttyp18	128.255.130.254	com8	term1 compress

Encryption compression and address authentication: Add both "key=x", compress and mac behind comx termx of the file itest.conf.(There exists no requirement to the order of the added items) For example:

/dev/ttyp11	128.255.130.254	com1	term1	compress key=a mac 3601000004d9

An integrated example:

/dev/ttyp11	128.255.130.254	com1	term1	compress key=a mac 00017a00a792
.....	.....	.....	.....	
/dev/ttyp18	128.255.130.254	com8	term1	compress key=a
/dev/ttyp21	128.255.130.254	com9	term1	key=a
.....	.....	.....	.....	
/dev/ttyp28	128.255.130.254	com16	term1	compress

Examples of New/Old Configuration of Signamax Router

A configuration file in the old configuration mode:

```
mp2600# show running-config
   ….
line 0 15 mode terminal
….
line 0 15 flowctl soft 180
terminal 0 15 local 129.255.8.43
terminal 0 15 remote 0 unix-1 129.255.24.100 fix-terminal
authentication
terminal 0 15 host 0 hesc-chars 8
terminal 0 15 hesc-chars 1
terminal 0 15 redraw console \E!9Q
terminal 0 15 redraw 0 \E!10Q
terminal 0 15 rbufsize 1024
terminal 0 15 tbufsize 2048
terminal 0 15 rx-delay on
terminal 0 15 print off
terminal 0 15 auto-linking 0
terminal 0 15 enable
```

A configuration file in the new configuration mode:

The interface is configured as follows:

```
mp2600#sho run int a4/0
Building Configuration...
 configuration:

interface async4/0
 speed 9600
 databits 8
 stopbits 1
 parity none
 flow-control software 180
 tx-on dsr
 encapsulation terminal
 exit
```

The terminal template is configured as follows:

```
terminal template itest43
terminal local 129.255.8.43
terminal remote 0 unix-1 129.255.24.100 fix-terminal
authentication compress encrypt a
```

```
terminal remote 1 telnet-unix 129.255.24.100 telnet
terminal remote 2 rlogin-unix 129.255.24.100 rlogin
terminal hesc-chars 1
terminal host 0 hesc-char C
terminal host 1 hesc-char P
terminal host 2 hesc-char V
terminal redraw console \E!8Q
terminal redraw 0 \E!9Q
terminal redraw 1 \E!11Q
terminal rbufsize 4096
terminal tbufsize 10000
terminal retry-times 6
terminal rx-delay on
exit
```

Apply the template to the interface:

```
terminal apply itest43 async4/0 async4/15
```

Quality of Service (QoS) Configuration

Intergrated Services, IntServ

The most popular protocol in integrated service is Resource Reservation Protocol, RSVP, it advertises QoS requirement of transmission equipment in the network (such as routers). RSVP provides two kinds of service:

Guaranteed Service, it provides reliable bandwidth and time delay limitation to satisfy the requirement of application program.

Controlled-Load Service, it provides service quality guarantee for network load. It means top provide low time delay and high passed quality guarantee when the network is busy. Especially suitable the high requirement application, such as VOIP etc.

RSVP (Resource Reservation Protocol)

RSVP (Resource Reservation Protocol), as a standard signaling protocol, is used to ensure the point-to-point network bandwidth for the IP network. It adopts basic route allocation protocols to determine where to transmit the reserved request. When the route allocation changes paths to accommodate to the change of the topology structure, RSVP can make its reserved request accommodate to the new paths.

This working mode doesn't incommode other route allocation services. RSVP provides transparent operations via supporting no RSVP router nodes, cooperating with the queuing mechanism instead of replacing it. RSVP applies for a specific queuing mechanism, but only a specific interface queuing mechanism can realize the reservation function.

RSVP Commands

ip rsvp

ip rsvp bandwidth reservable-bandwidth largest-reservable-flow

ip rsvp {burst *burst-factor*}| {delay *time-value*}| {neighbor *access-list*}| signaling {conform | exceed} {dscp *value* | precedence *value* }| {udp-multicasts *multicast-address*}

Command	Description
reservable-bandwidth	This is the reservable-bandwidth, and its value range is between 1 and 10000000 kbps
largest-reservable-flow	This is the largest reservable bandwidth of each flow, and its value range is between 1 and 10000000kbps.

Configure RSVP Proxy

The proxy configuration is used to replace a node that cannot send RSVP messages to send RSVP messages, so that other nodes can realize the RSVP reservation via receiving the RSVP proxy message that the router creates.

ip rsvp

ip rsvp { sender | sender-host | reservation | reservation-host }

(Command mode)The global configuration mode.

Syntax	Description
Sender	Configure the PATH message proxy, of which the followed parameters are as follows: the destination address reservable-flow, the resource address of reservable-flow, IP protocol number of reservable-flow, the destination port of reservable-flow, the source port of reservable-flow, the previous hop address of PATH message, the supposed receiving interface of PATH message, the reservable-flow bandwidth, the reservable-flow burst-size.
sender-host	Configure the PATH message proxy for the local application. And no receiving interface and previous hop addresses need be configured.
reservation	Configure the RESV message proxy, of which the followed parameters are as follows: the destination address a reservable-flow, the source address of a reservable-flow, IP

	protocol number of a reservable-flow, the destination port of a reservable-flow, the source port of a reservable-flow, the previous hop address of a RESV message, the supposed receiving interface of RESV message, the reservable share-style, the service that the reservable-flow applies for, the reservable-flow bandwidth, the reservable-flow burst-factor.
reservation-host	Configure the RESV message proxy for the local application. No receiving interface and the previous hop address need be configured.

Monitoring and Debugging RSVP (Resource Reservation Protocol)

show ip rsvp installed

This command is used to display information about the flows that succeeds in RSVP reserving.

show ip rsvp installed

(Command mode)The privilege user mode.

show ip rsvp neighbour

This command is used to display the RSVP neighbor list that switches the RSVP signaling with the local router.

show ip rsvp neighbour

(Command mode)The privilege user mode.

show ip rsvp sender

This command is used to display the list of the PATH messages that the local router received(PSB).

show ip rsvp sender

(Command mode)The privilege user mode.

show ip rsvp reservation

This command is used to display the list of the RESV messages that the local router received(RSB).

show ip rsvp reservation

(Command mode)The privilege user mode.

show ip rsvp blockade-state-block

This command is used to display the list of the RESV messages that are denied by the previous hop and RESVTEAR messages are received by the local router (BSB).

show ip rsvp blockade-state-block

(Command mode)The privilege user mode.

show ip rsvp timer

This command is used to display the list of the timers with each RSVP in the local router.

```
show ip rsvp timer
```

(Command mode)The privilege user mode.

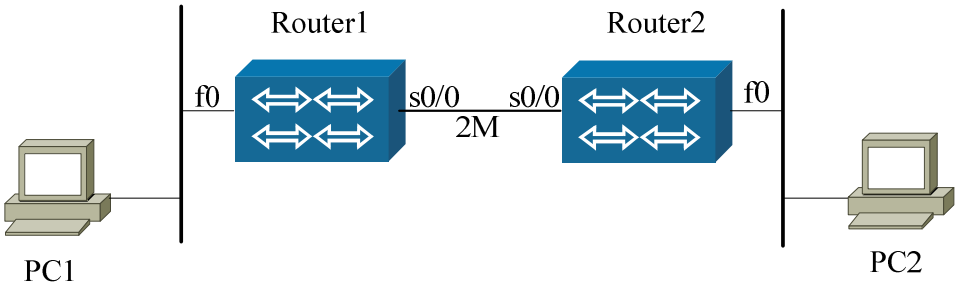
```
debug ip rsvp
```

This command is used to display the process that creates the RSVP reservation.

```
debug ip rsvp
```

(Command mode)The privilege user mode.

RSVP Configuration Example



Via the Ethernet, PC1 and PC2 connect with ROUTER1 and ROUTER2 respectively. ROUTER1 ROUTER2 adopt the PPP protocol to connect each other by means of one 2M private line over which all communication between two LANs respectively connected with PC1 and PC2. And network applications between PC1 and PC2 require a stable 40K bandwidth.

```
Configure ROUTER1 as follows:
```

Command	Description
route1#conf t	
router1(config)#interface s0/0	
router1(config-if-serial0/0)# **fair-queue**	Enable FQ.
router1(config-if-serial3/0)#**bandwidth 2000**	Designate the interface bandwidth to be 2M.
router1(config-if-serial0/0)#**ip rsvp bandwidth** 64 64	Enable the RSVP resource reservation function.
router1(config-if-serial0/0)#encapsulation ppp	
router1(config-if-serial0/0)#ip address 192.168.0.5 255.255.255.252	

Configure ROUTER2 as follows:

Command	Description
Route2#conf t	
Router2(config)#interface s0/0	
Router2(config-if-serial0/0)# **fair-queue**	Enable FQ
router2(config-if-serial3/0)#**bandwidth 2000**	Designate the interface bandwidth to be 2M.
Router2(config-if-serial0/0)#i**p rsvp bandwidth** 64 64	Enable the RSVP.
Router2(config-if-serial0/0)#encapsulation ppp	
Router2(config-if-serial0/0)#ip address 192.168.0.6 255.255.255.252	

Differentiated Services, DiffServ

For differentiated service, it differentiates each packet QoS level and provides the service according to the configured QoS mechanism. Sometimes this kinds of QoS plan is named COS. The most common used differentiated methods are: differentiating according to IP packet priority, packet source, IP address, port, protocol, packet sizes etc. The result is used for traffic monitoring, traffic shaping and queuing.

Bandwidth Management, BwMg

It has two aspects:

- Committed Access Rate
- Traffic Shape

Committed Access Rate

SIGNAMAX router uses Committed Access Rate(CAR) as the algorithm of bandwidth management. CAR algorithm allocates bandwidth to IP data-packet flows according to rate-limit rules.

CAR basic command description

Command	Description	
rate-limit ----rate-limit input ----rate-limit output	* configure rate limitation Rate limit input Rate limit output	config-if-xx config-if-xx config-if-xx
show interface interface-name rate-limit	Examine CAR working record	enable

rate-limit

rate-limit { input | output } [access-group access-list-name] cir conform-burst exceed-burst conform-action {actions [action-val] } exceed-action { actions [action-val] }

Command	Description
{input | output}	Apply the rule to ingress/egress packets
access-list-No	Specify an access-list no to match packets. If its default configuration is adopted, all ingress/egress packets of the interface should be matched. The value range is from 1 to 2000.
CIR	Define committed Information rate(bit/s), a value in 8000-1000000000
Conform burst	Define conform burst rate, the depth of conform bucket(byte), a value in 1500-5000000
Exceed burst	Define exceed burst rate, the depth of exceed bucket(byte), a value in 0-10000000
actions [action val]	Define actions of conform /exceed burst: continue : do nothing but continue matching next rule drop : drop this packet transmit : forward this packet set-prec-continue : set the precedence of a packet as <action val> and continue matching next rule set-prec-transmit : set the precedence of a packet as <action val> and forward this packet set-dscp-continue : set DSCP of a packet as <action val> and continue matching next rule set-dscp-transmit : set DSCP of a packet as <action val> and forward this packet

Signamax series router doesn't support QoS Group. But adds DSCP area t-dscp-XXX .

Signamax series router CAR supports rate limitation on sub-interface. And all the CAR will be cleared after the sub-interface is dealt with no.

Signamax series router CAR module doesn't support high speed forwarding. If configured CAR rule on the interface, the high sped forwarding function will be disabled, the system will not give any prompt. And this high speed forwarding function will be auto enabled after all CAR rules are deleted.

The three numerical parameters of CAR means the rate, level 1 Bc and level 2 Bc.

- **CAR monitoring and debugging**

Show

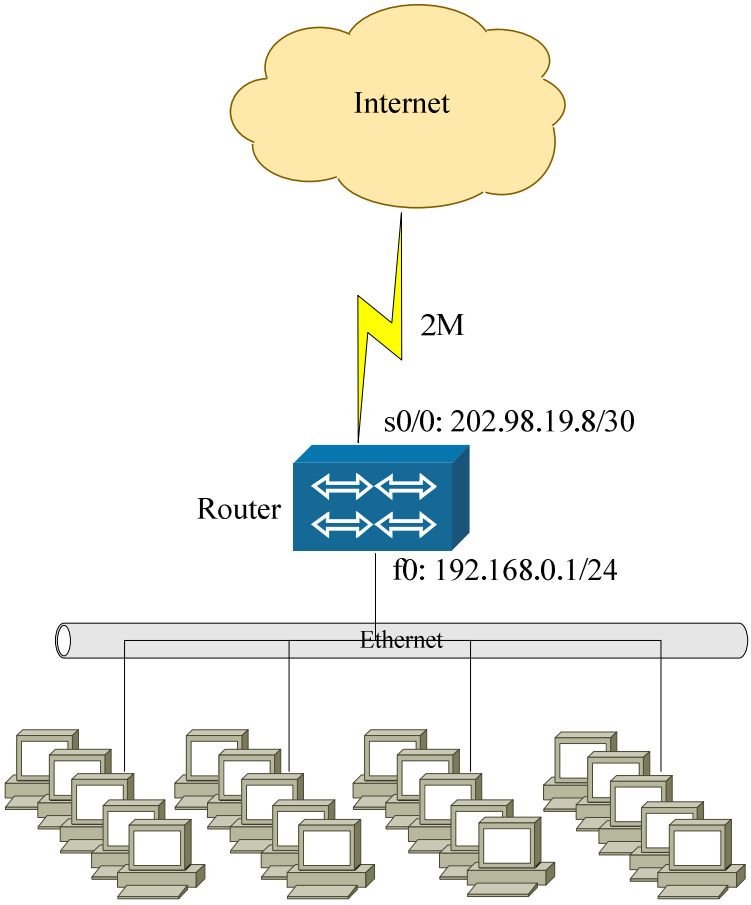
Use show to examine CAR working record.

```
show interface interface-name rate-limit [ { input | output} ]
```

Command	Description
interface-name	Designate the interface via interface-name
input | output	Designate examining input or output working record.

(Default status)not display
(command mode)privileged mode

CAR configuration example



Above is a typical condition is a small scale LAN connects INTERNET via NAT Router configuration:

Command	Description
router#configure terminal	
router(config)#access-list 1001 permit tcp any any eq 80	Configure the limited exit rate application type (WWW)
router(config)#access-list 1002 permit tcp any eq 80 any	Configure the limited entry rate application type (WWW)
router(config)#interface serial 0/0	
router(config-if-serial0/0)#encapsulation ppp	
router(config-if-serial0/0)#ip address 202.98.19.8 255.255.255.252	
router(config-if-serial0/0)#rate-limit output access-group 1001 1000000 20000 0 conform-action transmit exceed-action drop	Limit output WWW traffic bandwidth 1Mbps
router(config-if-serial0/0)#rate-limit input access-group 1002 1000000 20000 0 conform-action transmit exceed-action drop	Limit input WWW traffic bandwidth 1Mbps

Traffic Shaping

Traffic shaing is used to send packets at an average rate and smooth the egress flow when there exists data congestion.

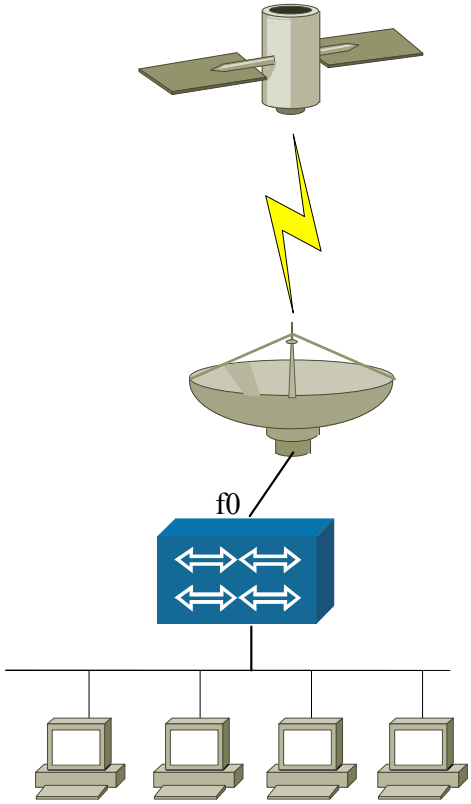
Configuring Traffic-Shape

`traffic-shape command`

`traffic-shape rate conform-rate permit burst`

Command	Description
conform-rate	Maximal bandwidth of the interface. Its value range is from 480 to 1000000000 bits/sec
permit burst	Burst bytes permitted in 1/60 second. Its value range is from 1600 to 50000000 bytes

`traffic shaping configuration example`



Above is a small scale LAN connects the external via satellite. Because the rate of the satellite is very low (9.6K), limit the rate on Ethernet. In order to use link bandwidth, here we decide to use traffic shaping.
Router configuration:

Command	Description
router#configure terminal	
router(config)# interface fastethernet 0	
router(config -if-fastethernet0)# traffic-sharp 9600 1600	Configure 9600 bits traffic shaping, permitting 1600 bytes outburst

Congestion Management, CgMg)

Signamax router has the following queuing methods: FIFO, PQ, CQ, FQ, CBWFQ, LLQ etc.

First In First Out (FIFO)

The default queuing function of your Signamax router is First In First out (FIFO), which is shown in the following Figure 1. Simply put, the router will filter data packets in the same order they enter, which is a very effective way of providing a large-scale service among a group of similar users with the fewest possible delays.

The downside, however, is that FIFO doesn't provide multiple Quality of Service levels for different kinds of users. For instance, a Telnet packet might be dropped by the system after receiving many FTP packets, which will delay the start of a Telnet session.

If this happens often, users trying to login via Telnet might start to complain about the delays on your network. For that reason, you may want to consider using the alternative queuing methods that are discussed in the remaining sections.

Priority Queuing (PQ)

With priority queuing, the router will send out a packet with the highest priority level before sending a packet with a lower priority. When the outbound interface is very congested, the packets will be queued from highest to lowest priority. If the interface isn't congested, then the router will send all of the packets forward at the same level of priority.

Distribute Packet Queue and Priority Class

In priority queuing, each interface has four queues:

High

Medium

Normal

Low

Normal is usually the default queue setting. A packet that isn't already classified or distributed to a specified queue in any router can be put into a queue.

Configure Priority Queuing

You can configure the router so that it can classify packets by:

TCP or UDP port numbers

Packet size

The arriving packet's interface

Any item described in a standard or extended access list

IP fragments

You can also choose to use the default scattered packet mode.

When you start PQ configuration, you should:

Define a priority list

Apply the defined priority list to an interface

To define a priority list, input:

Router config priority-list <list-number>

Define the priority list number between 1 and 16.

Command	Description
interface <interface > <high / medium / normal / low>	interface <interface >: Distributes the interface priority when the packet arrives. high / medium / normal / low: Defines the queue priority of queue.
default <high / medium / normal / low>	Default: Distributes a priority to any packet that doesn't match the appointed standard.
protocol ip <high /medium /normal / low> <fragments/ gt /lt /list /tcp/ udp>	protocol IP: Assigns the data packet using IP protocol. fragments: Assigns a priority by whether or not the data packet is fragmented. gt/lt: Assigns a priority by packet size. list: Assigns a priority by data according to the access list. tcp/udp: Assigns a priority by outbound tcp/udp port number.

To apply the defined priority list to an interface, input:

router config-if-xxx

Command	Description
Priority-group <list-number>	Assigns a priority list to an interface and activates the priority queuing.
no priority-group	Cancels the priority queue.

The same priority list can be applied to many interfaces. Different priority policies can also apply to different interfaces. You can only use one priority list for each interface.

Adjust Priority Queue Size

The priority queue default depth of a Signamax router, from high priority to low priority, is 15000, 30000, 45000 and 65535. This value can be changed when you input the following commands while configuring the router's priority queue size:

Router config priority-list <list-number>

Defines the priority list number between 1 and 16

Command	Description
queue-limit <0-15000> <0-32767> <0-45000> <0-65535>	queue-limit <high-limit> <medium-limit> <normal-limit> <low-limit>: Defines the depth of the four queues (high, medium, etc.). <0-15000>: The adjusted depth scope of high-priority queue is from 0 to 15,000 bytes. <0-32767>: The adjusted depth scope of medium-priority queue is from 0 to 32,767 bytes. <0-45000>: The adjusted depth scope of normal-priority queue is from 0 to 45,000 bytes. <0-65535>: The adjusted depth scope of low-priority queue is from 0 to 65,535 bytes.

Monitor & Debugging

Use in the privilege mode:

Command	Description
show pq	Displays router's relative PQ interface information.
show pq interface <interface>	Displays specified interface's relative PQ information.
debug pq	debug the router's relative PQ interface information
debug pq interface <interface>	debug the specified interface's relative PQ information.

Choose Packet Drop-type Algorithm

When a priority queue is full, packets will be tailed-dropped normally. But you can choose RED algorithm as packet drop-type:

```
Router config priority-list <list-number>
```

Defines the priority list number between 1 and 16

Command	Description
drop-type random-detect <RED group name>	Chooses RED algorithm as packet drop-type. <RED group name>: name of the RED group. The following will describe how to configure a RED group.
drop-type tailed-dropped	Chooses default tailed-dropped algorithm as packet drop-type.

Configure RED Group

Following explains how to configure a RED group:

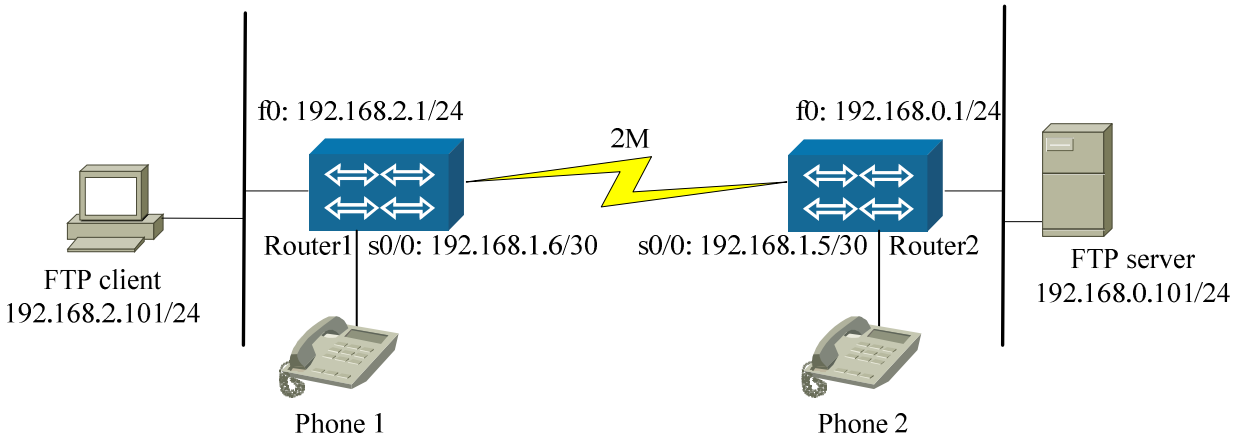
```
Router config random-detect-group <RED group name>
```

Defines some parameters of the RED group

RED group config:

Command	Description
exponential-weighting-constant <1-12>	Defines exponential weight factor. <1-12>:Integer in 1..12 used in weighted average to mean 2^number.
precedence <0-7> <0-65535> <0-65535> <1-99>	Defines IP precedence, minimum threshold, maximum threshold and probability denominator parameters. <0-7>: Defines IP precedence parameter, first 3 bits of TOS field in IP header. <0-65535>:Defines minimum threshold(bytes) of the queue. <0-65535>:Defines maximum threshold(bytes) of the queue. <1-99>: Defines probability denominator.

Example



Router1 configuration:

Command	Description
router1#configure terminal	
router1(config)#access-list 1001 permit ip host 192.168.1.6 host 192.168.1.5	Designate IP phone data
router1(config)#access-list 1002 permit tcp host 192.168.2.101 host 192.168.0.101 eq 21	Designate FTP management data
router1(config)#access-list 1002 permit tcp host 192.168.2.101 host 192.168.0.101 eq 20	Designate FTP application data
router1(config)#priority-list 1 protocol ip high list 1001	Put voice application data to higher priority queue.
router1(config)#priority-list 1 protocol ip low list 1002	Put FTP application data to priority queue

router1(config)#interface serial 0/0	
router1(config-if-serial0/0)#priority-group 1	Apply PQ to S0/0

Customer Queuing (CQ)

This system assigns a queue to each user session based on the amount of information that user needs access to. Like WFQ, these queues save the passing packets as they enter the router. The system will sort and queue a packet.

When the system de-queues, the system will start polling user information. According to the different configurations that each queue possesses, related total number of bytes taken from each user's queue will be different. The user who needs access to the greatest number of bytes will have the highest priority. (If the sorting rule allowing this to happen isn't configured, then the packet will enter the default queue.)

Assign Queue In CQ Mode

Sixteen queues can be defined for each interface here. Each queue is titled and simply identified with a number between 1 and 16. (The number doesn't have anything to do with queuing priority.)

Configure the router so it can sort packets according to the following standards:

Protocols (ICMP, IGMP, TCP and UDP) and TCP and UDP port numbers, Packet size.

The arriving packet's interface

Any item described by a standard or an extended access list

IP fragments

A packet's source address and destination address

Configure CQ

Configuring a CQ involves three steps:

Defining a CQ list.

Defining each queue's byte number.

Applying the defined list to an interface.

To define a customer queuing list, input:

```
Router config custom-queue-list <list-number>
```

Define a user-defined customer queuing list using a number between 1 and 16.

Command	Description
fragments <0-16,Min queue number> <0-16,Max queue number>	Fragments: Sets the queuing rule according to whether the packet is fragmented or not. <Min queue number>: Sets the minimal queue number that packet can enter. <Max queue number>: Sets the maximal queue number that packet can enter.
gt/lt/et <1-1500> <0-16,Min queue number> <0-16,Max queue number>	gt/lt/et: Sets the queuing rule according to the packet size. It can be more than, less than or equal to the size of the appointed packet. <1-1500>:Defines the packet size.
icmp/igmp/tcp/udp <0-16,Min queue number> <0-16,Max queue number>	icmp/igmp/tcp/udp: Sets queuing rule according to different protocol type.
tcp/udp <0-16,Min queue number> <0-16,Max queue number> keyword-value	keyword-value: Comprises the source/destination address or the network segment, address netmask and the source/destination port number. Sets the queuing rule according to these contents.
ip <0-16,Min queue number> <0-16,Max queue number> keyword-value	keyword-value: Comprises the source/destination address of an IP packet or network segment and address netmask. Sets the queuing rule according to these contents.
list <1-2000, ip access list-name> <0-16,Min queue number> <0-16,Max queue number>	list <ip access list-name>: The applied access list number. Sets the queuing rule according to these contents.
interface <interface > <0-16,Min queue number> <0-16,Max queue number>	interface <interface >: Sets the queuing rule according to the interface where the packet arrives.
default <queue-number>	Default: All packets that don't accord with the above rules will be put in the default queue.

To define the byte number of each queue

Router config custom-queue-list <list-number>

Command	Description
queue <0-16,Min queue number> <0-16,Max queue number> byte-count <byte-count>	queue <0-16,Min queue number> <0-16,Max queue number>: Specify queue size in bytes in the appointed scope. This parameter is used to decide the weight of each queue.

To apply the defined list to the interface

```
router config-if-xxx
```

Command	Description
custom-list <list-number>	Applies the defined list to the interface.
no custom-list	Cancels the user-defined customer queue.

Adjust CQ User Attributes

The default buffer size of the Signamax router user-defined queue interface is 65,535 bytes. The default buffer size of each queue from 0 to 16 is 65,535 bytes. The value of the parameter can be altered via the following command:

```
router config custom-queue-list  <list-number>
```

Command	Description
queue <0-16,Min queue number> <0-16,Max queue number> limit <size>	Set the buffer size of each queue from 0 to 16.

Choose Packet Drop-type Algorithm

When a customer queue is full, packets will be tailed-dropped normally. But you can choose RED algorithm as packet drop-type:

```
router config custom-queue-list  <list-number>
```

Note: Defines the custom-list number between 1 and 16

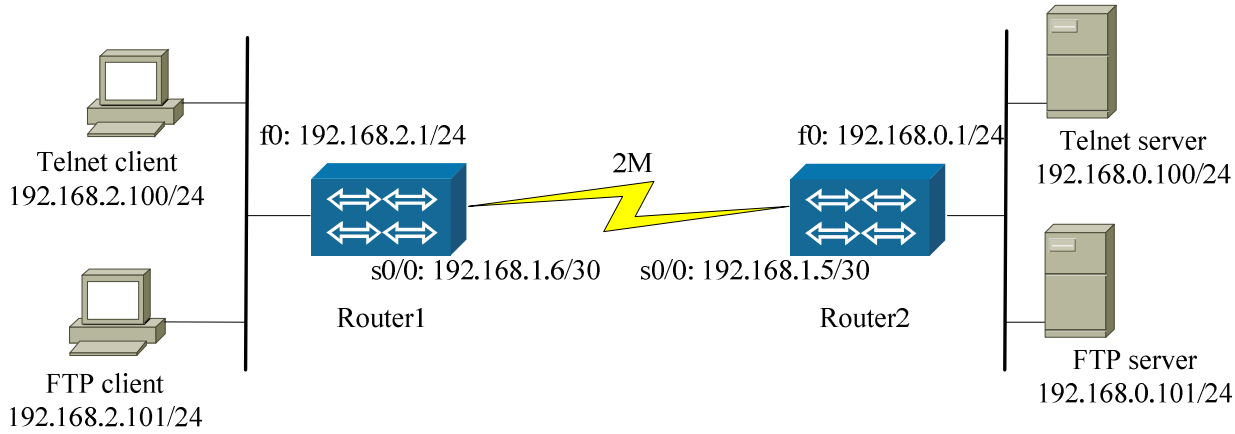
Syntax	Description
drop-type random-detect <RED group name>	Chooses RED algorithm as packet drop-type. <RED group name>: name of the RED group. Section 2.5 explains how to configure a RED group.
drop-type tailed-dropped	Chooses default tailed-dropped algorithm as packet drop-type.

Monitor and Debugging

After CQ has been configured, the following debugging command can be used to verify and check the action. The detailed commands are as follows:

```
center
```

Command	Description
show cq	Displays router's relative CQ interface information.
show cq interface <interface>	Displays specified interface's relative CQ information.
debug cq	Debug the router's relative CQ interface information.
debug cq interface <interface>	Debug the specified interface's relative CQ information.



Router1 configuration:

Command	Description
router1#configure terminal	
router1(config)#access-list 1001 permit tcp host 192.168.2.100 host 192.168.0.100 eq 23	Designate terminal data
router1(config)#access-list 1002 permit tcp host 192.168.2.101 host 192.168.0.101 eq 21	Designate FTP management data
router1(config)#access-list 1002 permit tcp host 192.168.2.101 host 192.168.0.101 eq 20	Designate FTP application data
router1(config)#custom-queue-list 1 list 1001 1 1	Put terminal data to CQ 1
router1(config)#custom-queue-list 1 list 1002 2 2	Put FTP data to CQ 2
router1(config)#custom-queue-list 1 queue 1 1 byte-count 6000	Configure queue 1 sending bytes as 6000
router1(config)#custom-queue-list 1 queue 2 2 byte-count 1500	Configure queue 2 sending bytes as 1500
router1(config)#interface serial 0/0	
router1(config-if-serial0/0)#custom-list 1	Apply CQ to interface

FQ(Fair Queueing)

Fair Queueing is a distributing rule, it is a complex queuing process.

- **FQ basic command description**

Command	Description	Configuration mode
fair-queue	* enable FQ on interface	config-if-xx
show wfq	Display FQ statistics information	enable
debug wfq	Display the packet queuing condition	enable

- **fair-queue**

```
fair-queue: enable FQ on interface
fair-queue {queue-nums | queue-limit queue-number queue-limit}
```

Syntax	Description
queue-nums	Apply FQ to interface, and designate queue number.
queue-limit queue-number queue-limit	Change FQ max length queue-no : designate queue number queue-limit: designate queue max length. And the unit is byte, default is 32767 bytes.

(Default status)not enable FQ
(command mode)interface configuration mode

FQ monitoring and debugging

show wfq

display WFQ queue statistics information

show wfq

(command mode)privileged user mode.

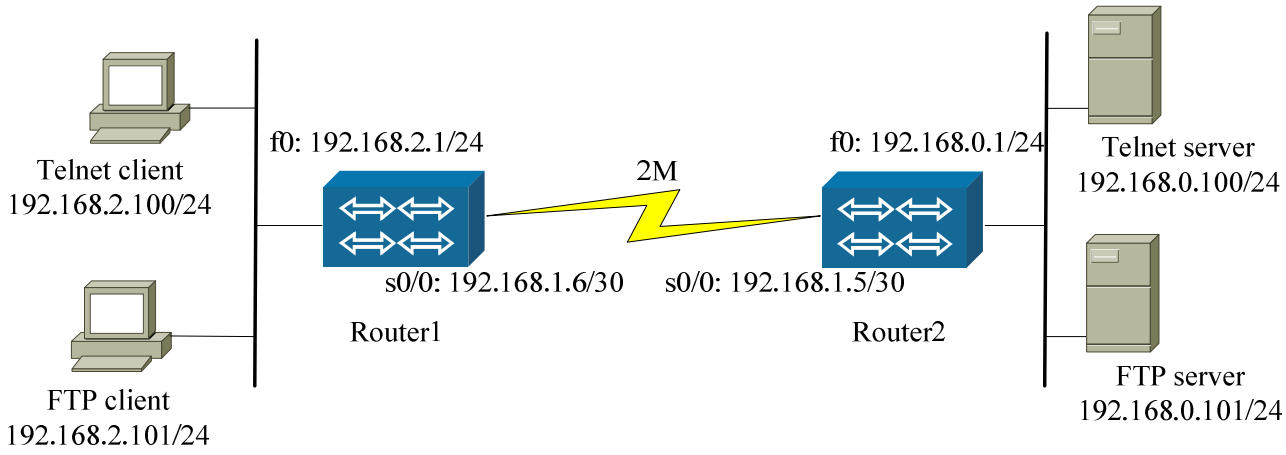
debug wfq

display the packet queue condition

debug wfq

(command mode)privileged user mode

FQ configuration example



Router1 configuration:

Syntax	Description
router1#configure terminal	
router1(config)#interface serial 0/0	
router1(config-if-serial0/0)#fair-queue	Enable FQ on interface

Class-Based Weighted Fair Queue(CBWFQ)

CBWFQ assigns a weight to different classes of IP packets. The bandwidth of the interface configured with CBWFQ will be allocated according to the weight.

```
class-map
class-map  [match-all | match-any]  class-map-name
```

Syntax	Description
match-all	All the rules should be matched.
match-any	Only needs to configure one rule
class-map-name	Configure the communication class named class-map-name

(Default status)not configure CBWFQ communication class
(command mode)global configuration mode

When establishing communication class, if the user doesn't designate match-all or match-any, the default is match-all.

The same strategy can be applied to many communication classes.

```
match
match       access-group  access-list-name
```

Syntax	Description
access-list-name	Match communication class via access list number or access list name.

```
match       input-interface  input-interface-name
```

Syntax	Description
input-interface-name	The matching name is input to data packet via input-interface-name

```
match       output-interface  input-interface-name
```

Syntax	Description
input-interface-name	The matching name is output to data packet via output-interface-name

```
match        ip precedence  ip-precedence
```

Syntax	Description
ip-precedence	The segment of Prededence is ip-precedence data packet, and the range is 0－7

```
match        ip dscp  ip-dscp
```

Syntax	Description
ip-dscp	DSCP segment is ip-dscp data packet, and the range is 0－63

```
match        protocol  protocol
```

Syntax	Description
protocol	Match the rule according to packet load protocol types.

```
match        class-map  class-map-name
```

Syntax	Description
class-map-name	Matching with another communication type

(Default status)not create CBWFQ communication class
(command mode)CBWFQ rule configuration mode

Signamax series router doesn't define special QOS group, but adopting access list. The access list definition should be permit, but not deny. The communication matching only supports BitTorrent protocol.

```
policy-map
Enter strategy configuration mode config-pmap
policy-map  policy-map-name
```

Syntax	Description
policy-map-name	Configure the strategy named policy-map-name.

(Default status)not configure CBWFQ strategy
(command mode)global configuration mode

```
class
```

```
Enter config-pmap-c from config-pmap. And in this mode, configure the bandwidth for strategy class.
```

```
class class-map-name
```

Syntax	Description
class-map-name	Configure the class named class-name.

(Default status)not enter class configuration mode
(command mode)strategy configuration mode

bandwidth
In the mode of config-pmap-c, configure bandwidth for communication class.
bandwidth percent bandwidth-in-percentage
or
bandwidth bandwidth-in-kbps total-in-kbps

Syntax	Description
bandwidth-in-percentage	Set the bandwidth percentage, and the value range is 1－100
bandwidth-in-kbps	Configure bandwidth using the unit kilobit/second.
total-in-kbps	Interface total bandwidth, and the unit is kilobit/second.

Generally, using percentage mode.
priority
please refer to LLQ configuration.

set
In the mode of config-pmap-c, designate configured label for communication class.

```
set {ip { precedence | dscp} val | mpls { experimental imposition | experimental topmost } val }
```

Syntax	Description
ip { precedence | dscp} val	ip top label precedence val:ip priority level. And the range is 0~7 dscp val:ip dscp segment. The range is 0~63
Mpls { experimental imposition | experimental topmost }	mpls exp segment experimental imposition val:configure all mpls labels. And the

val	range is 0~7 experimental topmost val:configure the level 1 label of mpls. And the range is 0~7

drop
In the mode of config-pmap-c, configure drop for dropping the matching packet.

drop

drop	Drop the matching packet.

service-policy
In the mode of config-pmap-c, use command service-policy to configure service policy.

```
service-policy policy-name
```

Syntax	Description
Policy-name	Configure the service policy named policy-name.

random-detect
Configure WRED queue.
random-detect [exponential-weighting-constant exponential-weighting-constant]

Syntax	Description
exponential-weighting-constant	Use exponential weighting constant 6. The range is 1—12

```
random-detect [precedence precedence minimum-threshold maximum-threshold [mark-probability-denominator]]
```

Syntax	Description
precedence	Match the data packet with the priority level precedence Rang is 0—7
minimum-threshold	Configure the minimum threshold value Range is 1—32767
maximum-threshold	Configure the maximum threshold value Range is 1—32767
mark-probability-denominator	Configure the mark probability denominator Range is 1—99

(Default status)not create CBWFQ rule
(command mode)CBWFQ rule configuration mode

Mark probability denominator 10.

We suggest the user using the default of WRED.
WRED drop strategy is to avoid the global synchronization.

service-policy
In interface configuration mode, the policy-name should be applied to input/output

```
service-policy {input | output} policy-name
```

Syntax	Description
policy-name	Configure the rule named *policy-name*

(Default status)not enable service policy on interface
(command mode)interface configuration mode

service-policy queue-limit queue-number queue-limit

Syntax	Description
queue-number queue-limit	Change queue number limit queue-number queue-limit: designate queue max length. And the unit is byte, default is 65535 bytes.

(Default status)disable
(command mode)interface configuration mode

```
cbwfq nums
```

This command is used to configure CBWFQ queue number.

```
cbwfq nums number
```

Syntax	Description
number	Change CBWFQ queue number

(Default status)CBWFQ queue number is 16.
(command mode)global configuration mode

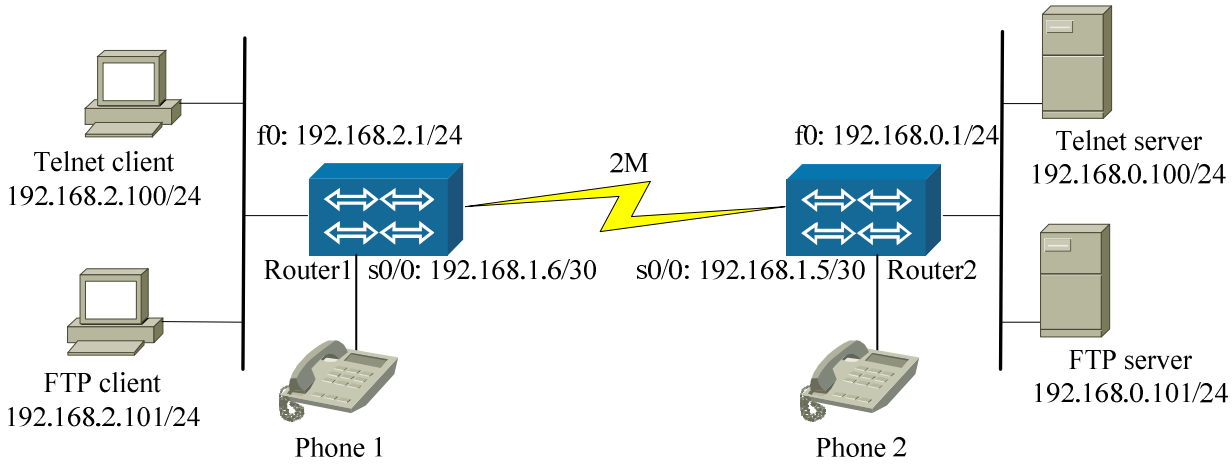
One interface or one sub-interface only has one strategy. When configuring another strategy, the original strategy will be auto cleared.
The strategy on interface input direction only uses to configure label or drop packet, but not to provide bandwidth guarantee. The command bandwidth, priority, random-detect etc. are not effective.

If CBWFQ queue is existing, the command cbwfq nums number will not change queue number, so service-policy should be deleted and then restarted, the new queue will be effective.

CBWFQ monitoring and debugging

```
show cbwfq
display  CBWFQ queue statistics information
show cbwfq
(command mode)privileged user mode
show policy interface
display  CBWFQ queue statistics information
show policy interface interface-name
(command mode)privileged user mode
debug cbwfq
display the packet queue status
debug cbwfq
(command mode)privileged user mode
```

CBWFQ configuration example



The two sites connect via 2M leased line, and this leased also loads voice, terminal and data transmission. CBWFQ is used to limit data transmission bandwidth.

Suppose FTP works on TCP port 20 and 21,and from client to server, and the left equipment is Router1.

Router1 configuration:

Command	Description
Router1#configure terminal	
router1(config)#access-list 1001 permit ip host 192.168.1.6 host 192.168.1.5	Designate IP phone data
router1(config)#access-list 1002 permit tcp host 192.168.2.100 host 192.168.0.100 eq 23	Designate terminal data
router1(config)#access-list 1003 permit tcp host 192.168.2.101 host 192.168.0.101 eq 21	Designate FTP management data
router1(config)#access-list 1003 permit tcp host 192.168.2.101 host 192.168.0.101 eq 20	Designate FTP application data
router1(config)#class-map voip	Define VOIP class
router1(config-cmap)#match access-group 1001	Designate VOIP class matching condition

router1(config)#class-map telnet	Define TELNET class
router1(config-cmap)#match access-group 1002	Designate TELNET class matching condition
router1(config)#class-map ftp	Define FTP class
router1(config-cmap)#match access-group 1003	Designate FTP class matching condition
router1(config)#policy-map one	Define strategy ONE
router1(config-pmap)#class voip	Enter VOIP class configuration mode
router1(config-pmap-c)#bandwidth percent 50	Distribute 50% bandwidth to VOIP
router1(config-pmap)#class telnet	Enter TELNET class configuration mode
router1(config-pmap-c)#bandwidth percent 20	Distribute 20% bandwidth to TELNET
router1(config-pmap)#class ftp	Enter FTP class configuration mode
router1(config-pmap-c)#bandwidth percent 5	Distribute 5% bandwidth to FTP
router1(config)#interface serial 0/0	
router1(config-if-serial0/0)#service-policy output one	Apply policy ONE to interface

LLQ (Low Latency Queuing)

Low Latency Queuing has some priority class on CBWFQ.
LLQ basic command description

Command	Description	Configuration mode
priority	* Configure priority class and distribute bandwidth	config-pmap-

priority
In the mode of config-pmap-c, configure its priority class and distribute the bandwidth.
priority bandwidth
or

```
priority percent bandwidth-in-percentage
```

Command	Description
bandwidth	Configure low latency queuing guaranteed bandwidth. Unit is byte/second. The range is 60-10000000
bandwidth-in-percentage	Configure the bandwidth percentage, and the range is 1—100

(Default status)not create LLQ CBWFQ rule
(command mode)CBWFQ rule configuration mode

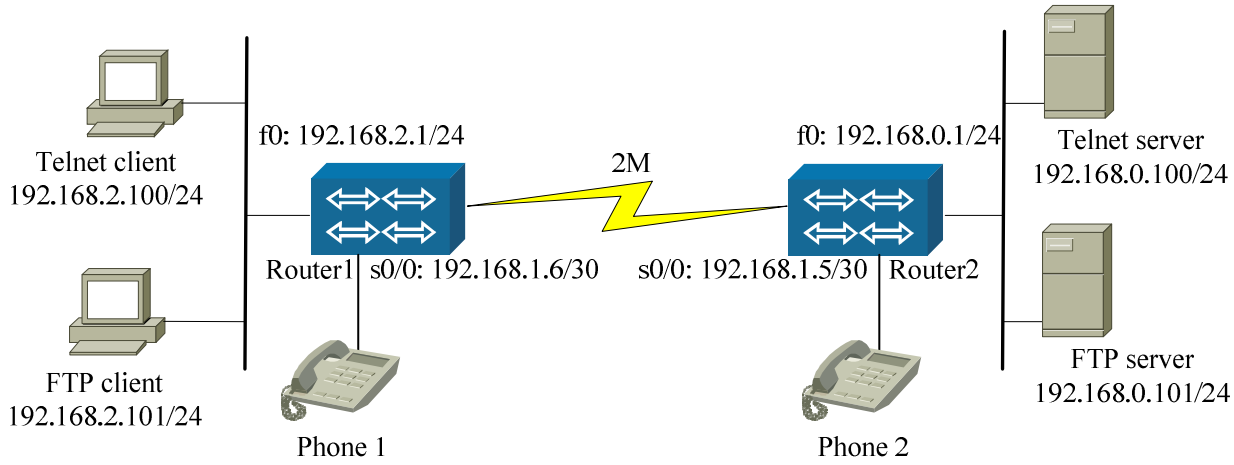
Note:

Generally, we suggest using absolute value bandwidth distribution mode. If adopting percentage configuration mode, the total percentage of CBWFQ is also 100.

LLQ monitoring and debugging
LLQ still uses CBWFQ monitoring and debugging command.

```
show cbwfq
display  CBWFQ queue statistics information.
show cbwfq
(command mode)privileged user mode
debug cbwfq
display the packets queuing status

debug cbwfq
(command mode)privileged user mode
```

LLQ configuration example



The two sites connect via 2M leased line, and this leased also loads voice, terminal and data transmission. CBWFQ is used to limit data transmission bandwidth.

Suppose FTP works on TCP port 20 and 21,and from client to server, and the left equipment is Router1.

Router1 configuration:

Command	Description
router1#configure terminal	
router1(config)#access-list 1001 permit ip host 192.168.1.6 host 192.168.1.5	Designate IP phone data

router1(config)#access-list 1002 permit tcp host 192.168.2.100 host 192.168.0.100 eq 23	Designate terminal data
router1(config)#access-list 1003 permit tcp host 192.168.2.101 host 192.168.0.101 eq 21	Designate FTP management data
router1(config)#access-list 1003 permit tcp host 192.168.2.101 host 192.168.0.101 eq 20	Designate FTP application data
router1(config)#class-map voip	Define VOIP class
router1(config-cmap)#match access-group 1001	Designate VOIP class matching condition
router1(config)#class-map telnet	Define TELNET class
router1(config-cmap)#match access-group 1002	Designate TELNET class matching condition
router1(config)#class-map ftp	Define FTP class
router1(config-cmap)#match access-group 1003	Designate FTP class matching condition
router1(config)#policy-map one	Define strategy ONE
router1(config-pmap)#class voip	Enter VOIP class configuration mode
router1(config-pmap-c)#priority 50000	Put VOIP class to LLQ, permitting bandwidth 50000 bytes/second
router1(config)#interface serial 0/0	
router1(config-if-serial0/0)#service-policy output one	Apply policy ONE to interface

Congestion Avoidence, CgAvD

Random Early Detect, RED

Random Early Detect, RED is a grouping drop policy, a queue management arithmetic, which is used to manage grouping and queue length. The traditional queue management uses simple end drop policy. Because the sending end may adopt congestion management mechanism, such as TCP, the traditional queue end drop policy may cause data source global synchronization.

Configuration command refers to WRED.

Weighted Random Early Detect (WRED)

A Weighted Random Early Detect (WRED) is just like FIFO except packet drop algorithm and the number of queues(10 queues). It selects RED as packet drop algorithm. It classifies packets according to IP priority (namely the first 3 bits of TOS field in IP header).

While WRED queuing is a complex procedure, but it needs little configuration.

WRED basic command description

Command	Description	Configuration mode
random-detect	* enable or configure WRED	config-if-xx
random-detect-group	Set WRED rule group	config
exponential-weighting-constant	Configure WRED weighting constant	config-wred-group
precedence	Configure WRED parameters for IP priority level.	config-wred-group
show wred	Display WRED queue statistics information	enable
debug wred	Display the packets queuing condition	enable

```
random-detect
```

```
Enable WRED.
```

```
random-detect [ { exponential-weighting-constant exponential-weighting-constant | precedence precedence minimum-threshold maximum-threshold [mark-probability-denominator] } ]
```

Syntax	Description
exponential-weighting-constant	Change interface RED average queue statistics weighting constant, default is 6.
Precedence	Designate IP priority Value range is 0—7
minimum threshold	Designate priority level queue minimum threshold value. Value range is 1000—65535
maximum threshold	Designate priority level queue max threshold value. Value range is 2000—65535
mark-probability-denominator	Mark probability denominator Value range is 1—100

(Default status)not enable RED on interface
(command mode)interface configuration mode

Mark denominator value 10.

- **random-detect-group**

Signamax series router WRED can be used together with CQ, PQ, CBWFQ and LLQ, as drop policy. The user configures RED group in global configuration mode. random-detect-group defines RED group.

```
random-detect-group random-detect-group-name
```

Syntax	Description
random-detect-group-name	Configure WRED group, designating group name.

(Default status)not create RED group.
(command mode)global configuration mode

```
exponential-weighting-constant weighted-num
```

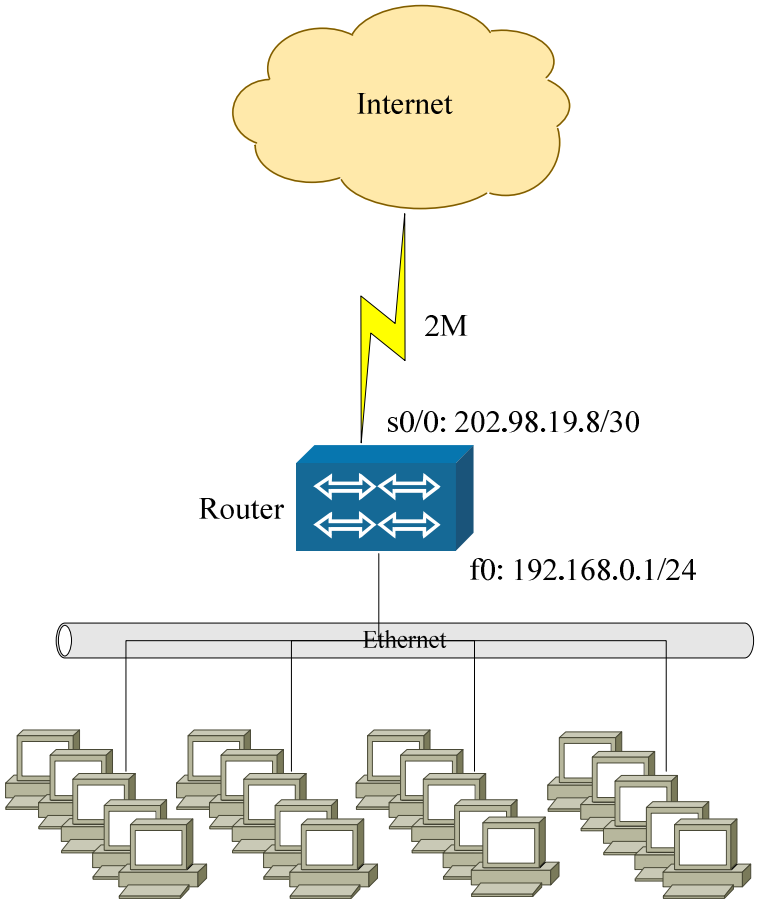
Syntax	Description
weighted-num	Configure WRED group average queue weighted constant, and the system default one is 6.

```
precedence precedence minimum-threshold maximu-threshold
[mark-probability-denominator]}]
```

Syntax	Description
precedence	Designate packet priority level
minimum-threshold	RED minimum threshold value.
maximu-threshold	RED maximum threshold value.
mark-probability-denominator	Mark probability denominator.

(Default status)not create RED group
(command mode)RED group configuration mode

```
WRED monitoring and debugging
show wred
display  WRED queue statistics information
show wred
(command mode)privileged user mode
debug wred
display packet queuing condition
debug wred
(command mode)privileged user mode

WRED configuration example
```



Above is a small scale LAN connects INTERNET via NAT. To avoid the global synchronization effect to network, we adopt WRED mode on s0/0.

Router configuration:

Command	Description
router#configure terminal	
router(config)#interface serial 0/0	
router(config-if-serial0/0)#random-detect	Enable WRED on interface

Selected Packet Drop

SPD differentiates the normal data and key service. It guarantees key service when the congestion happens, and drop the useless one. SPD has two parallel queues: normal queue and priority queue. Normal queue has two configuration parameters: minimum random drop threshold, maximum random drop threshold.

normal queue length dealt mode	< minimum threshold	Between minimum and maximum threshold	= or > maximum threshold

Normal data packet	Data packet entering normal queue	Data packet random drop	Directly drop data packet

Priority queue has only one configured parameter.

priority queue length dealt mode data packet type	<maximum queue length	= or > maximum queue length
Priority data packet	Data packet entering priority queue	Drop the data packet

- **SPD basic command description**

Command	Description	Config Mode
spd ---- spd ---- spd minthreshhold ---- spd mode ---- spd headroom ---- spd priority	SPD configuration command Enable SPD function Configure SPD normal queue dropped threshold Designate SPD dropped mode Designate SPD priority queue size Designate SPD key service type	config config config config config config
show spd [verbose]	Display spd statistics information	enable

- **spd**

The command is used to enable SPD or configure SPD parameters.

```
spd [ { headroom headroomnum | minthreshhold minimum-threshold maxthreshhold maximum-threshold
| mode aggressive | priority { access-list access-list-name | AH | BGP | ESP | IRMP | OSPF | PIM | RIP | RSVP } } ]
```

Command	Description
Headroom headroomnum	Designate SPD priority queue size
minthreshhold minimum-threshold maxthreshhold maximum-threshold	Modify normal queue drop threshold minimum threshold range is 1~ 200 maximum threshold range is 1~ 400
mode aggressive	Configure SPD as active drop mode
priority { access-list access-list-name | BGP | IRMP | OSPF | PIM | RIP | RSVP }	Explains key service type. The key service can be matched via access list, and the data packet. Key service configuration is parallel.

(Default status)not enable SPD
(command mode)global configuration mode

- **SPD monitoring and debugging**

```
show spd
display  spd statistics information.
show wred [verbose]
(command mode)privileged user mode.
```

SPD runs on network layer.

BitTorrent traffic control

BitTorrent (BT) is a P2P(Peer to Peer) software.
Main contents of this section:

- **BT traffic control mode**
- **BT traffic control parameter configuration**

BT traffic control mode

Use CBWFQ to control BT traffic.

- Drop BT traffic;
- Limit BT traffic rate.

BT traffic control configuration process comprises three steps, for example,

```
(1) configure a class-map,to match BT.
router(config)#class-map bittorrent
router(config-cmap)#match protocol bittorrent
router(config-cmap)#exit
(2) configure a policy-map,to drop BT traffic.
router(config)#policy-map drop-bittorrent
router(config-pmap)#class bittorrent
router(config-pmap-c)#drop
router(config-pmap-c)#exit
router(config-pmap)#exit
or configure a policy-map,to limit BT traffic bandwidth.
router(config)#policy-map limit-bittorrent
router(config-pmap)#class bittorrent
router(config-pmap-c)#bandwidth percent 1
router(config-pmap-c)#exit
router(config-pmap)#exit
(3) apply policy-map to router interface.
router(config-if-fastethernet0)#service-policy input drop-
bittorrent
router(config-if-fastethernet0)#service-policy output drop-
bittorrent
router(config-if-fastethernet1)#service-policy output limit-
bittorrent
```

The drop policy policy-map can be used both on input and output of interface. But the limited traffic policy policy-map is only applied to output on interface.

BT protocol is based on TCP, but because TCP port number is changeable, BT traffic cannot be marked via TCP port, but according to source IP address, destination IP address and destination TCP port number.

BT Traffic Parameter Configuration

- **BT traffic control parameters basic command description**

Command	Description	Config Mode
bittorrent ---- bittorrent max-connections ---- bittorrent time-out ---- bittorrent aging-interval	BT configuration command Configure system supported BT connection max number Configure BT connection aging time Configure BT connection aging check period	config config config config
show bittorrent pools	Display BT pool using condition	enable
show bittorrent connections	Display BT connection condition	enable

The below command is used for configuring BT connection parameters:

`bittorrent max-connections max-connections-num`

Command	Description
max-connections-num	Configure system supported BT connection max number. And the range is 200-20000,default value is 2000.

(Default status)system supports 2000 BT connection by default.
(command mode)global configuration mode

- **bittorrent time-out** *timeval*

Command	Description
timeval	Configure BT connection aging time, and the unit is second, range is 60-3600,default is 130.

(Default status)BT connection aging time default value is 130 seconds.
(command mode)global configuration mode

- **bittorrent aging-interval** *interval*

Command	Description
Interval	Configure BT connection aging check time period, unit is second and the range is 10-3600,default value is 60.

(Default status)BT connection aging check period default value is 60 seconds.
(command mode)global configuration mode

`show bittorrent pools`

This command is used to display system BT pool using condition and each BT pool empty connection number, to know the BT connection total number.

`show bittorrent connections`

This command is used to display BT connection condition.
For example,
router#show bittorrent connections

No.	Sip	Dip	Dport	PoolId	Age
1	55.0.0.5	22.0.0.2	1194	0	38
2	55.0.0.5	22.0.0.2	1197	0	18
3	55.0.0.5	22.0.0.2	1199	0	18
4	55.0.0.6	22.0.0.2	1202	0	18
5	55.0.0.6	22.0.0.3	1209	0	18

6	55.0.0.6	22.0.0.3	1210	0	18
7	55.0.0.6	22.0.0.4	1211	0	18
8	55.0.0.7	22.0.0.4	1217	0	18
9	55.0.0.7	22.0.0.4	1219	0	18
10	55.0.0.7	22.0.0.4	9417	0	105

No is BT connection number, Sip is BT connection IP address, Dip is destination IP address, Dport is
TCP port number, PoolId is buffer pool number, Age is the last BT connection time.

SNTP Configuration

Simple Network Time Protocol (SNTP) is a TCP/IP protocol that is used to distribute the exact time within the whole network, and it solves the problem to keep the clocks of all the routers within the network synchronous. All Signamax routers have their own system clocks and can save the date and time.

SNTP Configuration Command

Command	Description	Config mode
sntp server	*configure SNTP server address	config
sntp source	Configure SNTP packet sending source address interface	config
sntp broadcast	Configure SNTP client end whether sending and accepting NTP/SNTP broadcast packet	config
sntp interval	Configure SNTP client sending packet time interval	config
sntp timeout	Configure SNTP client end packet timeout	config
debug sntp	Debug SNTP	enable
show sntp	Display SNTP packet alternation and configuration	enable
show clock	Display system clock	enable
clock timezone	*modify system timezone	config

Configure SNTP

```
sntp server
```

This command can be used to configure the name or IP address of the used SNTP server, and the form no of this command can be used to remove the configured SNTP server.
sntp server ip-address

```
no sntp server
```

Command	Description
ip-address	The IP address of the SNTP server that CLIent uses.

(Default)No SNTP server is configured.
(Command mode)The global configuration mode.

sntp source
Use sntp source to designate SNTP client end request packet source address, and no is used to clear the address.

sntp source interface

Command	Description
interface	Client end designated sntp packet interface

(Default status)the source address is decided by the core.
(command mode) global configuration mode

sntp broadcast
This command can be used to control whether the SNTP client receives NTP/SNTP broadcast packet.
sntp broadcast {enable|disable}
(Default)The default is DISABLE.
(Command mode)The global configuration mode.

sntp interval
This command can be used to control the interval between two SNTP request packets, and the form no of the command can be used to reset the default value.

sntp interval time-value

Command	Description
time-value	The value of the interval between two SNTP request packets, and its value range is between 10s and 3600s.

(Default)The default value is 30 seconds.
(Command mode)The global configuration mode.

`sntp timeout`

This command can be used to control the interval for CLIent-side to wait the server response after it sends a request, and the form no of the command is used to reset the default value.

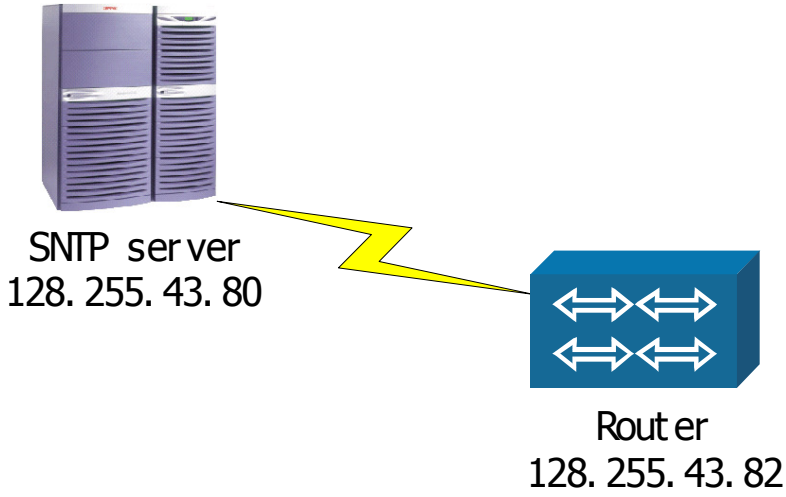
`sntp timeout time-value`

Command	Description
time-value	The value of the interval for CLIent to wait the server response after it sends a request, and its value range is between 10s and 600s.

(Default)The default value is 30 seconds.
(Command mode)The global configuration mode.

Configure SNTP

128.255.43.80 is SNTP server



Configure in global configuration mode (CONFIG mode):

Command	Description
Router(config)# sntp server 128.255.43.80	Configure NTP server IP address 128.255.43.80

After above configuration, executing show clock, you may find that time is synchronous with sntp server

Checking & Debugging SNTP

debug sntp
This command is used to open the switch of SNTP debugging information. The form no of the command is used to close the SNTP debugging function.

(Command mode)The privilege user mode.

show sntp
This command is used to display the SNTP packets that update the system time.

```
show sntp {status|config}
```

(Command mode)The privilege user mode.

```
show clock
```

This command is used to display the system time.
(Command mode)The common user mode.

The privilege user mode service timestamps debug datetime localtime msec show-timezone In DEBUG information, this command is used to display the time in the local time format and the time zone information, accurate to an extent of the millisecond.

(Command mode)The global configuration mode.

```
service timestamps log datetime localtime msec show-timezone
```

In the log, this command is used to display the time in the local time format and the time zone information, accurate to an extent of the millisecond.

(Command mode)The global configuration mode.

Configuring Time Zone

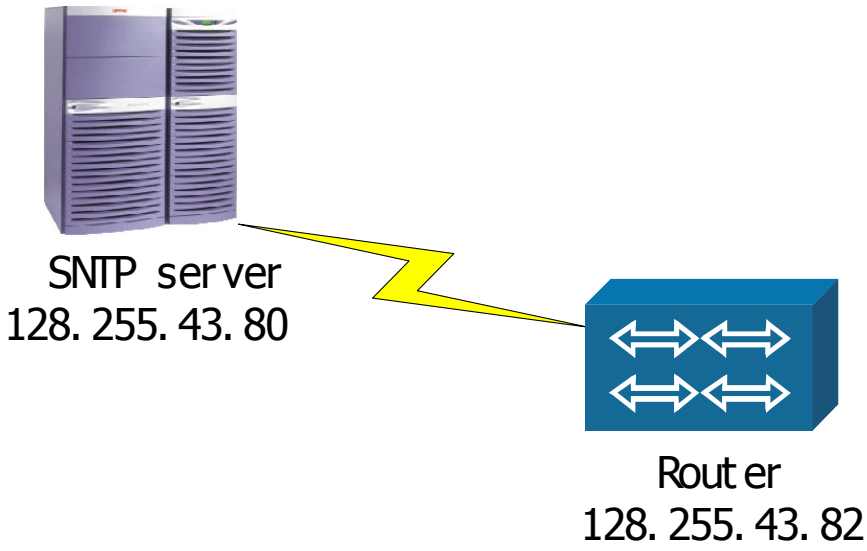
```
clock timezone
```

This command is used to switch the Universal Time Coordinated (UTC) in the displayed information into the time of the configured time zone.
clock timezone timezone-name hour-offset minute-offset

Syntax	Description
Timezone-name	The time zone name.
Hour-offset	The hour offset relative to UTC time, and its value range is between –23 and 23.
minute-offset	The minute offset relative to UTC time, and its value range is between 0 and 59.

Time Zone Configuration

As shown in the following figure, the Chengdu time zone is configured on the Signamax router that serves as the SNTP CLIENT, and its hour offset relative to UTC standard time on the SNTP server is 9.



Command	Description
Router(config)# clock timezone chengdu 9	Configure the hour offset relative to UTC standard time with 9.

Security Configuration

This chapter will describe how to operate the security configuration of your MP2600 Router.

Signamax Networks Routers offer comprehensive network security features like:

- PPP protocol supports (PAP and CHAP), which effectively prevents unauthorized connections.
  -
- Callback technology.
- An IP protocol layer providing firewall protection, which filters unauthorized data packets.
- Network Address Translation (NAT), which can hide your interior network and prevent exterior network attacks.
- Access Control Lists (ACL), which can sort end users into up to 15 different classes depending on your needs. These lists register a different series of commands available to individual users. They ensure that users with different rights will only be able to access certain commands.
- Encryption and key exchange technologies

Firewall Configuration

This section will look at:
- Firewall introduction
- Access Lists
- Correlative Firewall Configuration
- Applying Access Lists To An Interface
- Monitoring And Maintaining Your Firewall
- Access Channel Configuration
- Time Limit Packet Filtering
- Media Access Control (MAC) Address Packet Filtering
- A Few Points About Firewall Configuration

Overview

Access Lists

How To Edit A Standard Access List

A standard access list can filter your network communications based on packet header source addresses. You can define a standard access list with within the access-list command, and delete it at any time by placing the no command in front of the command in global configuration mode.

router(config)#access-list ?

Command	Description
<1001_2000>	The number range used in an extended access list.
<1_1000>	The number range used in a standard access list.

router(config)#access-list 1 ?

Command	Description
Deny	Denies access
Permit	Permits access.

router(config)#access-list 1 deny ?

Command	Description
A.B.C.D	Source address
Any	Any source host
Host	A single source host

router(config)#access-list 1 deny A.B.C.D ?

Command	Description
A.B.C.D	Wildcards applied to source address are expressed with dotted decimal notation. This masks rebel code. If a bit is marked 1, that means that the bit is indifferent.

router(config)#access-list 1 deny A.B.C.D a.b.c.d ?

Command	Description
Log	Logs output to the console about the access list. This is an optional function.

To define a standard access list:

```
router(config)#access-list <1_1000> ?
```

Command	Description
{deny | permit} source [source-wildcard] [log]	Source: the source address. Source-wildcard: the source address's wildcard.

Deleting an access list:

Command	Description
router(config)#no access-list list-number	This deletes an access list. List-number: the deleted access list's number.

You can define a standard access list named after a title or serial number with the following codes:

(You can delete this list by placing no in front of the command code part that's in bold type.)

router(config)#ip access-list ?

Command	Description
Extended	Designates an extended access list definition.
Standard	Designating a standard access list definition

router(config)#ip access-list standard ?

Command	Description
<1_1000>	List number
WORD	List name

Command	Description
router(config)#ip access-list standard 1	Enters the access list configuration mode.

router(config-std-nacl)#?

Command	Description
Deny	Denies access.
End	
Exit	
Help	
No	
Permit	Permits access.

router(config-std-nacl)#deny ?

Command	Description
A.B.C.D	Source address.
Any	Any source host
Host	A single source host

router(config-std-nacl)#deny A.B.C.D ?

Command	Description
A.B.C.D	The wildcard applied to the source address.

router(config-std-nacl)#deny A.B.C.D a.b.c.d ?

Command	Description
Log	Logs output to the console about the access list. This is an optional function.
router(config)#ip access-list standard {name | access-list-number}	Defines a standard access list in global configuration mode.
router(config-std-nacl)#{deny | permit} source [source-wildcard] [log]	Defines a rule in the list in access list configuration mode.
router(config-std-nacl)#no {deny | permit} source [source-wildcard] [log]	Deletes a rule from the list

Example: Construct an access list named number 2 (see following table), then define three rule items and apply this list 2 to Ethernet interface 0. Among the packets from Ethernet interface 0, those packets that come from the host 92.49.0.3 will be allowed. All the packets from any host within the subnet 92.48.0.0 will be permitted, too. All others will be denied.

Command	Task
router(config)# access-list 2 permit host 92.49.0.3 log	Permits the packets from the host IP 92.49.0.3.
router(config)# access-list 2 permit 92.48.0.0 0.0.255.255	Permits all packets from any host in the subnet 92.48.0.0.
router(config)# access-list 2 deny any	Denies other packets.
router(config)# interface ethernet 0	
router(config-if-ethernet)# ip access-group 2 in	Applies list 2 to Ethernet interface 0.

The following commands have the same effect:

Command	Task
router(config)# ip access-list standard 2	
router(config-std-nacl)# permit host 92.49.0.3 log	Permits the packets from the host IP 92.49.0.3.
router(config-std-nacl)# permit 92.48.0.0 0.0.255.255	Permit all packets from any host in the subnet 92.48.0.0.
router(config-std-nacl)# deny any	Denies other packets.
router(config-std-nacl)# exit	
router(config)# interface ethernet 0	
router(config-if-ethernet)# ip access-group 2 in	Applies list number 2 to Ethernet interface 0.

Use the following series of commands when only one rule is to be deleted:

Command	Description
router(config)# ip access-list standard 2	
router(config-std-nacl)# no permit host 92.49.0.3 log	
router(config-std-nacl)# exit	

How To Edit An Extended Access List

An extended access list can be used to filter IP communications not only according to the source address and the destination address of the packet header, but also according to the fields included into the IP, UDP, TCP, ICMP and IGMP packet headers.

The command router(config)#access-list 1001 ? 1001-2000 indicates an extended access list.

Command	Description
Deny	Denies access.
Permit	Permits access

router(config)#access-list 1001 deny ?

Command	Description
<0_255>	Number showing ALL kinds of protocols
ICMP	Internet Control Message Protocol (ICMP)
IGMP	Internet Group Management Protocol (IGMP)
IP	All Internet Protocols
TCP	Translation Control Protocol (TCP)
UDP	User Data Protocol (UDP)

You can define an extended access list on a number in extended access-list format.

You can delete the list with the no command in global configuration mode.

```
access-list access-list-number {deny | permit} protocol
source source-wildcard [operator port [port]] ] destination
destination-wildcard [ICMP-type] [igMP-type] [operator port
[port]] [ack / fin / established / psh / rst / syn / urg]
[precedence precedence] [tos tos] [log]
```

Syntax	Description
Access list number	List number
Protocol	Protocol
Source	Packet source address
Source-wildcard	Source address wildcard
Destination	Packet destination address
Destination-wildcard	Destination address wildcard
Precedence	Priority
TOS	Type of service
Log	Record permit or deny packets in the logging at several minutes interval
ICMP-type	Message type of ICMP
IGMP-type	Message type of IGMP
Operator	Port Comparison
Port	Port

Port Number	Port number
Ack / fin / established / psh / rst / syn / urg	TCP flag bit

You can define an extended access list based on a name or a number according to the following steps. (You can delete the whole list with the no command in global configuration mode.)

```
ip access-list extended {access-list-number/name}
```

Command	Description
access-list-number	An access list number, always a decimal number between 1001 to 2000

```
[no] [sequence] {deny | permit} protocol source source-
wildcard destination destination-wildcard [precedence
precedence] [tos tos] [log]
```

Syntax	Description
Sequence	Rule sequence
Deny	Denies access.
Permit	Permits access.
Protocol	The protocol's name or number. It may be one of the following keys: ICMP, IGMP, IP, TCP or UDP. Or it is expressed with a decimal number between 0 and 255. The IP keyword can match any protocol.
Source	The host or network that the packet is coming from, namely the source address of the packet. It can be expressed three ways: the first is via dotted decimal notation. The second is via the any keyword, which is the short form of the source address 0.0.0.0 and the source address wildcard 255.255.255. Thirdly, this can be expressed as the host source, or the source address with the 0.0.0.0 wildcard.
Source-wildcard	The wildcard applied to the source address. It can be expressed three ways. The first is via dotted decimal notation, or the network mask rebel code. (The bit marked 1 means that that bit is indifferent.) The second way this can be expressed is via the any command, which is the short form of noting the source address 0.0.0.0 and source address wildcard 255.255.255.255. Thirdly, this can also refer to the host source, which stands for the source address and the source address with the 0.0.0.0 wildcard.
Destination	The destination network or a host, namely the destination's address. It can be expressed three different ways, like the source address above. Please refer that definition.
Destination-wildcard	The wildcard applied to the destination address. It can be expressed three different ways, like the source address wildcard above. Please refer to that definition.
Precedence	The packet priority. It can be ranked by in number from 1 to 7, or the name of a priority. (The titles within can include: critical, flash, flash-override, immediate, internet, network, priority and routine.). Optional function.
TOS	The packet service type. It can contain a number from 0 to 15 or the name of a service type (The titles within it can include: max-reliability, max-viaput, min-delay, min-monetary-cost and normal). Optional function.

LCMP-type	The message type of an ICMP packet. It can be expressed via a number from 0 and 255 or the name of a message type. Optional function.
LCMP-code	The code type of an ICMP packet message type, which can be expressed with a number from 0 and 255. Optional function.
IGMP-type	An IGMP packet message type that can be expressed with a number from 0 and 255. Optional function.
Operator	Used to compare a source port and a destination port. There are five kinds of values that can be compared between the two ports: less than, more than, equal to, unequal to, and range. If the operational character comes after the source address and the source address wildcard, it is applied to the source port. If the operational character comes after the destination address and the destination address wildcard, it is applied to the destination port. Optional function.
Range	Used to define when the operator demands two port-numbers, and other operators demand one port number.
ack, fin, psh, rst, syn, ur	Used to match the TCP flag bit, including: Acknowledgement flag, finishing flag, promptly sending flag, restoration flag, synchronization flag, and urgency flag. Optional function.
Established	Indicates successful connection. If the TCP packet comprises ACK or RST, the packet will be matched. Only the packet for initial connection isn't matched. Optional function.
Name	Refers to the name of an access list. The name is used to distinguish it from other lists. It can't include any blank characters and the first character should be a letter.

Correlative Firewall Configuration

To display the access list log:

Command	Description
router# debug ip packet access-list	Permits access list display. In the privileged used mode, the default permits display.
router# undebug ip packet access-list	Doesn't permit list display.

When the access list log switch is open, the number of items displayed by each rule in the global configuration mode by default is, at best, 0. This means the number of displayed items isn't limited.

Command	Description
router(config)# firewall verbose-limit number	A number from 0 to 4,294,967,295.

Firewall Default Rules

Command	Description
router(config)# firewall default-deny	Denies all packets. In the global configuration mode, the default setting will automatically be set to deny all packets.
router(config)# no firewall default-deny	Permits all packets.

To filter all route recording packets:

Command	Description
router(config)# ip record-route	Permits packets with a route recording option. In the global configuration mode, the default will permit the packet with an IP recording route option (ie. recording routing or time label).
router(config)# no ip record-route	Denies all packets with a recording route option.

To filter all source routing packets:

Command	Description
router(config)# ip source-route	Permits all packets with source routing. In the global configuration mode, the default setting will permit a packet that has an IP source route option (ie. lose source routing or strict source routing).
router(config)# no ip source-route	Denies packets with a source route option.

To filter a directional broadcast packet:

Command	Description
router(config-if-xxx)# ip directed-broadcast	Permits the interface to send a directional broadcasting packet.
router(config-if-xxx)# no ip directed-broadcast	Denies the sending of a directional broadcasting packet. In the interface configuration mode, the default setting will deny a directional broadcasting packet.

To permit an interface or a sub-interface to send a mask-reply ICMP packet:

Command	Description
Router(config-if-xxx)# ip mask-reply	Permits an interface to send an ICMP mask-reply packet.
Router(config-if-xxx)# no ip mask-reply	Denies the sending of an ICMP mask-reply packet. In the interface or sub-interface configuration

	mode, the default setting will refuse to send an ICMP mask-reply packet.

To permit an interface or a sub-interface to send an ICMP redirecting packet:

Command	Description
router(config-if-xxx)# ip redirects	Permits the interface to send an ICMP redirecting packet. In the interface or sub-interface configuration mode, the default setting permits the interface to send an ICMP redirecting packet.
router(config-if-xxx)# no ip redirects	Doesn't allow the interface to send an ICMP redirecting packet.

To permit an interface to send an ICMP unreachable packet:

Command	Description
router(config-if-xxx)# ip unreachables	Permits the interface to send an ICMP unreachable-packet. In the interface or sub-interface configuration mode, the default setting will permit the interface to send an ICMP unreachable-packet.
router(config-if-xxx)# no ip unreachables	Doesn't allow the interface to send an ICMP unreachable-packet.

Applying Access Lists to Interface

After you construct an access list, it can be applied to a number of interfaces. The access list can be applied inward or outward. In the interface configuration mode, use the command IP access-group to control the interface access. Use the no command to remove the access list from the interface.

```
router(config-if-xxx)#[no] ip access-group {access-list-
number | name} {in | out}
```

Command	Description
Access-list-number	A number from 1 to 2,000.
Name	The access list name.
In	Filters the inward packet.
Out	Filters the outward packet.

After a packet is received to the inward standard access list, the packet source address will be checked against the access list. On an extended access list, the firewall will check fields such as the destination address and protocol other than the source address. If the packet is permitted by the access list, the routing software will process it successively. If the packet isn't permitted, the software will lose the packet.

After the packet is received and routed to an interface, to the outward standard access list, the firewall software checks the packet source address against the access list. To an extended access list, the firewall checks fields like destination address and protocol with the source address. If the packet is permitted by the access list, the routing software will transmit it. Or, the software will discard the packet. Note: If you haven't built an access list, all packets coming via the interface will be permitted.

For example, you can apply the extended access list 1,001 to the inward Ethernet interface 0 and the standard access list to the Ethernet outward interface 0. Then exit the interface configuration mode.

Command	Description
router(config)# interface ethernet 0	
router(config-if-ethernet0)# ip access-group 1001 in	Applies the extended access list 1,001 to the inward Ethernet interface 0.
router(config-if-ethernet0)# ip access-group 10 out	Applies the standard access list to the outward Ethernet interface 0.
router(config-if-ethernet0)# exit	

Firewall Security Check

Special Packet Check

According to switch check packet: source routing, recording routing, unnatural fragment, small packets, the user can permit or refuse these kinds of packets.

Command	Description	Config Mode
ip source-route	Whether filtering source routing packet	config
ip record-route	Whether filtering recording routing packet	config
ip fragment	Unreasonable fragment check filtering	config
ip small-packet	Whether filtering small fragment	config

```
ip source-route
 [no] ip source-route
```

Command	Description
source-route	Permit source routing packet passing (enable by default).
no	Refuse passing

(Configuration mode) global configuration mode
(Default status) permit passing

```
ip record-route
recording routing: this option is used for network testing and hacker.
[no] ip record-route
```

Command	Description
record-route	Permit recording routing packet passing (permit by default).
no	Refuse to pass.

(Configuration mode) global configuration mode
(Default status)permit passing

```
ip fragment
```

```
[no] ip fragment [max-off max-off-value]
```

Command	Description
no	Refuse IP total length larger than the fragment
max-off	IP total length larger than max configuration
max-off-value	IP total length max value

(Configuration mode) global configuration mode
(Default status)ip fragment max-off 65535,same value as ip fragment. Permit IP total length 65535 packets.

SSPING, Jolt2 and fragment attack: SSPING IP length will be larger than 65535, many system (such as Microsoft) will breakdown because of this.

```
ip small-packet
```

small packet: the short IP packet can be used for attacking, and the user can choose whether permitting the pass of this packet.

```
[no] ip small-packet [mini-length]
```

Command	Description
no	Not permit
mini-length	Configure packet minimum length.

(Configuration mode) global configuration mode
(Default status)not judge the length. ip small-packet

Pseudo Source Address Check

Pseudo source address is often being used in dialogue hijack, DOS attack etc. And for these check, the check is to configure access list, packet filtering, but this kind of check is limited; the check has following aspects:

Whether the accepting interface is correct, if the interface doesn't reach the source address routing, the routing is decided based on interface, and this packet will be held up;

The routing reaching to packet source address cannot be found from the router, and this packet is held up;

MAC address IP address is not the same with source address, and the

packet will be held up at this time;

If MAC cannot be found in ARP table, the packet will be held up;

If it is gateway routing according to source address, but MAC address is not the gateway physical address, the packet will be held up;

Other normal packets will be passed.

Command	Description	Config Mode
firewall check pseudo-address	Configure whether check pseudo source address	config

```
firewall check pseudo-address
```

check pseudo source address according to interface configuration;

```
[no] firewall check pseudo-address
```

Command	Description
no	Disable pseudo source address function

(Configuration mode) interface configuration mode
(Default status)not enable pseudo source address on interface

This function is only used on interface.

Attack Testing

Check the attack according to switch: ICMP flood, Smurf, Fraggle, SYN flood, LAND etc

Some attack packets testing (or monitoring)

Defense attack is passive, and so the attack being checked is so limited, but for other types attack, such as buffer area flood, password destroying etc., only the system itself can defense.

Command	Description	Config Mode
ip icmp intercept	icmp flood attack intercept	config
ip smurf intercept	Smurf attack intercept	config
ip fraggle intercept	Fraggle attack intercept	config
ip tcp intercept land	Land attack intercept	config
ip tcp intercept list	syn flood attack intercept	config

Note: 1, "*" before command means it has configuration example description.

2, configuration mode is: config, config-if-××(interface name) config-××(protocol name) etc.

`ip icmp intercept`

ICMP flood,this kind of attack sends amount of ICMP packets to destination server, occupying bandwidth, to cause the valid packet not to reach the destination server; when check, once the packet accepting frequency is higher than the normal range, the attack may exited, and the packet will be controlled strictly; but this kind of method has some limitations, and it only uses to protect the destination server.

`[no] ip icmp intercept list { access-list-number | access-list-name } [ maxcount ]`

Command	Description
access-list-number	Access list number. From 1 to 1000.
access-list-name	Access list name.
maxcount	Set check threshold value (500 by default), if he number is over that sending to destination host ICMP packet, it will be intercepted.

(Configuration mode) global configuration mode

`ip smurf intercept`

Smurf is another type of attack. The attacker uses the attacked host address to send ICMP response requirement to a broadcast address, and many computers will give response to the attacked host, and this kind of attack result is same a ICMP flood; this packet will be intercepted via two methods: the pseudo source address refuses the packet directly; another is to open smurf check switch, if source address is the protected destination server address, and the destination address is a broadcast address, the packet will be intercepted; smurf will extend its check to ICMP_TSTAMP ICMP_IREQ and ICMP_MASKREQ ;

```
[no] ip smurf intercept list {access-list-number | access-list-name } [ masklen {number} ]
```

Command	Description
access-list-number	Access list number, from 1 to 1000.
access-list-name	Access list name.
masklen	Destination network mask length (24 by default)

(Configuration mode) global configuration mode

```
ip fraggle intercept
```

```
[no] ip fraggle intercept list {access-list-number | access-list-name } [ masklen {number} ]
```

Command	Description
access-list-number	Access list number. From 1 to 1000.
access-list-name	Access list name.
masklen	Destination network mask length (24 by default)

(Configuration mode) global configuration mode

```
ip tcp intercept land
```

LAND attack uses another weakness of the system: many systems don't know how to deal with the SYN connection requirement, and so this kind of packet will be intercepted.

```
[no] ip tcp intercept land
```

Command	Description
Land	Land attack protection

(Configuration mode) global configuration mode

```
ip tcp intercept list
```

Waste system source attack, the most famous one is SYN flooding, it has two modes: intercepting mode and monitoring mode, and these two modes need to waste a large number of system resource, and we adopt two modes to check.

```
[no] ip tcp intercept list {access-list-number | access-list-name } [ maxcount {number} ]
```

Command	Description
access-list-number	Access list number, from 1 to 1000.
access-list-name	Access list name.
maxcount	Set check threshold value (1000 by default).

(Configuration mode) global configuration mode

Scan Protection

Scan check module checks address scan and port scan attack.

Command	Description	Config Mode
scanprotect	Configure scan protection function	config-if-××
show scanprotect	Display scan information	enable
clear scanprotect	Clear scan information	enable

`scanprotect`

check scan function on interface

```
[no] scanprotect interval { default | interval-value } addr-limit { default | max-addr-value } port-limit { default | max-port-value } ban-timeout { default | max-ban-timeout }
```

Command	Description
default	Adopt default value
scanprotect	Enable scan check function on interface
interval	Scan check time interval, the default is 1 second.
addr-limit	Define permitted scan max address number, default is 10.
port-limit	Define permitted scan max port number, default is 10
ban-timeout	After check scan attack, the source IP will be forbidden to access, and the default time is 15 seconds.

(Configuration mode) interface configuration mode
(Default status)not enable scan check function by default.

If adopting default parameters, use command scanprotect default to simplify the configuration. In the default configuration, scan check time interval is 1 second, address scan threshold value is 10, port scan threshold value is 10, ban time is 15 seconds.

```
show scanprotect
```

display scan check information

```
show scanprotect [ monitor ]
```

Command	Description
show scanprotect	Display scan protection parameter information.
monitor	Display network scan information

(Configuration mode) privileged mode

```
clear scanprotect
```

clear scan protection information

```
clear scanprotect
```

Command	Description
clear scanprotect	Clear scan statistics information

(Configuration mode) privileged mode

Firewall Log

Firewall log information adopts system log configuration, the following contents are being recorded in the log:

Filtering log based n access list: if access list rule has the option of log, this rule is considered to be used by firewall, and information will be recorded in log;

Special packet and pseudo source address check record: each special packet auto records log information to log system, and if the packet is over threshold limitation, there will be an added warning record in the log;

Warning threshold value adopts status switching mode, once the packet is over the fixed number, there will be a warning information;

The normal access list filtering log, special packet check and pseudo source address are saved in system log buffer.

Command	Description	Config Mode
firewall pseudo-address log	Pseudo source address protection switch	Enable
ip intercept log	Attack protection log switch	enable

```
firewall pseudo-address log
```

pseudo source address log has switch

```
[no] firewall pseudo-address log
```

(Configuration mode) privileged mode
(Default status)enable

```
ip intercept log
```

attack check record

```
[no] ip intercept log
```

(Configuration mode) privileged mode
(Default status)disable

Monitoring & Maintaining Firewall

To display contents of an access list in the privileged user mode:

```
router# show access-lists [access-list-number / name]
```

Command	Descri ption
access-list-number / name	The access list number or name.

If you don’t input a name or number, all of your access lists will be displayed.

To show certain access lists, input:

```
router# show access-lists
      Output result:
Extended ip access list: 1001
permit ICMP any any  8 0 log    4 matches
       permit tcp any any  syn log    1 matches
Extended ip access list: 1002
permit ICMP any any echo-reply log    4 matches
permit tcp any any established log    4 matches
```

Here, the matching times correspond to the filtered packet-matching rule. To display the an access list application to the interfaces:

```
router#sh ip int list
Output result:
Interface fastethernet 0
    Outgoing access list is 2
    Inbound access list is 1
Interface serial 2
    Outgoing access list is not set
Inbound access list is 1001
```

To clear the access list counter in the privileged user mode

```
router# clear access-list counters [access-list-number | name]
```

Without a name or number, all access list counters will be cleared. You can use the following command to clear access-list counters:

```
router# clear access-list counters
```

To show access lists, input:

```
router# show access-lists
```

Output result:

```
Extended ip access list: 1001
      permit ICMP any any 8 0 log    0 matches
      permit tcp any any syn log    0 matches
Extended ip access list: 1002
      permit ICMP any any echo-reply log    0 matches
  permit tcp any any established log    0 matches
```

Because the counter was set with a value of 0, the matching time is 0. You can also monitor and maintain the firewall by examining an access list log. Log records include information such as the source address, the destination address, the protocol type, the port number, and the sending and receiving interfaces, et cetera. To access this function, input:

```
router#debug ip packet access-list
```

Configuring Access Channel

Access Channel

Many interface channel rules should be configured in a certain order based on priority.

Try to avoid configuring a series of interfaces with channel rules. If a data packet passes via two interfaces with channel rule configurations, the data won't be permitted via the system until it passes examination by both sets of rules.

Please do not configure a firewall and an access channel on the router at the same time. This will cause a major malfunction.

An access channel can only adapt to a simple set of conditions. For more complex rules, please configure a firewall based on an access list.

Access Channel Configuration

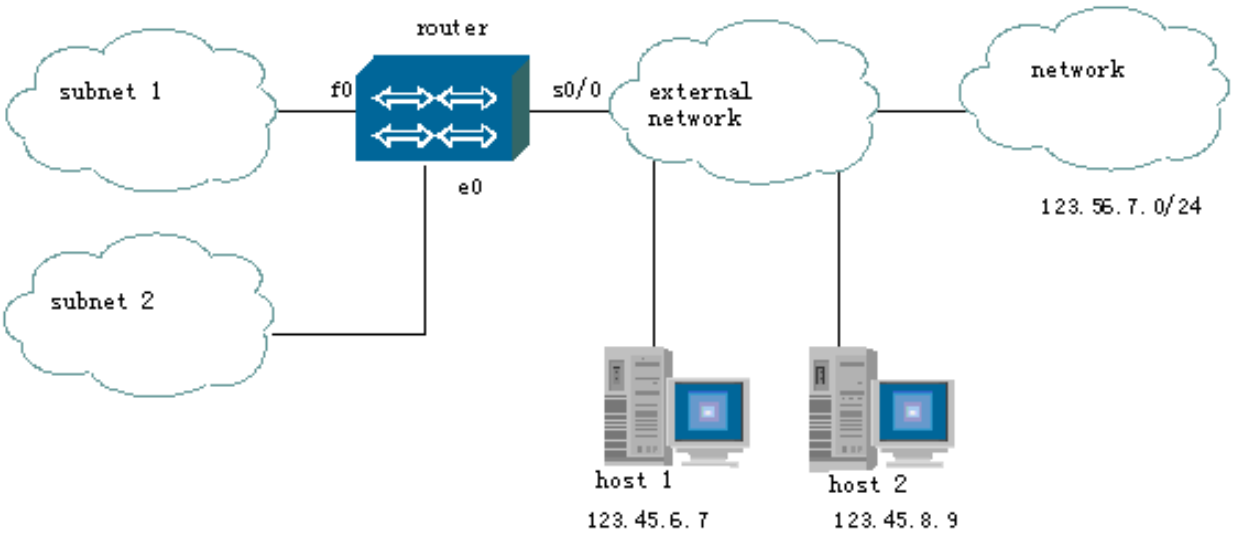
To add an interface configuration mode rule:

```
router(config-if)#[no] access-tunnel destination dest-mask [directly]
```

Command	Description
Destination	Destination address
Dest-mask	Mask
Directly	Used to mark the address's direction. If it is set, the direct connection will be located between the destination address and the interface (ie. the host IP address will be coming from the subnet connected to the interface), or else the indirect connection between them – ie. a router is between them. Optional function.
No	Deletes a rule.

Access Channel Configuration Example

Example one:



Access channel configuration example

Please examine Figure 2. If you want all the machines in the interior subnet1 and subnet2 to have permission to access the exterior host1 and host2, you would input the following configuration code:

Command	Description
router# config terminal	
router(config)# interface serial 0	Configures the interface s0.
router(config-if-serial0)# access-tunnel 123.45.6.7 255.255.255.255 directly	Accesses host1's access channel.
router(config-if-serial0)# access-tunnel 123.45.8.9 255.255.255.255 directly	Accesses host2's access channel.
router(config-if-serial0)# exit	
router(config)# exit	

Because the direct orientation access channel is configured on the interface s0, that interface will check whether or not the source address matches the channel address when s0 receives a data packet. When such a message is sent to the system, the destination address will be checked and the unmatched address packet will be denied.

Example two:
Please examine the following Figure 2. If you want subnet1 to access host 1, host 2 and the exterior network subnet 123.56.7.0/24 without restricting subnet 2's access, you would input the commands below. Note: In this example, the access channel can't be set on the exterior interface s0 – it should be set on the interface f0, which is connected to the subnet1.

Command	Description
router# config terminal	
router(config)# interface f0	Configures the interface f0.
router(config-if-fastethernet0)# acce 123.45.6.7 255.255.255.255	Accesses host1's access channel.

router(config-if-fastethernet0)# acce 123.45.8.9 255.255.255.255	Accesses host2's access channel.
router(config-if-fastethernet0)# acce 123.56.7.0 255.255.255.0	Accesses network 123.56.7.0's access code.
router(config-if-fastethernet0)# exit	
router(config)# exit	

Time Limit Packet Filtering

You might want to set your networks up so that all of the machines within a network fragment can access a server at a certain time, say the regular weekday business hours of your business. But, at the same time, you might want to permit exceptions to that rule, by allowing users to access your system on a Saturday afternoon, for example.

All the time-based demands you might have can be met via defining a time range in the router and activating security mechanisms to bind that time range to the packet filtering process.

Basic Commands

Time Range

A time range is, simply, a set of time segments of your choosing that allows users to access the network. There are two kinds of time segments: a relative time segment and an absolute time segment. The former refers to a weekly segment. The latter refers to a segment covering a certain date (ie. x month, x day, x year).

To define a time range in the configuration or interface mode:

Command	Description
Signamax26(config)# time-range time_range_name	This command will allow you to enter a time range configuration mode. If a time range doesn't already exist, a new one will be created.
Signamax26(config)# no time-range time_range_name	Deletes a time range via the command "no".

To define a relative time segment in the time segment configuration mode:

Command	Description
periodic [days-of-the-week] [hh:mm] to [days-of-the-week] [hh:mm]	This checks whether an equivalent structure has existed before you add a new time segment. If the time segment doesn't exist, a new one will be created. Note: You can delete a segment by imputing the no command. The date default is set daily. The time default is 0:00 and 24:00, respectively.

To define [days-of-the-week] [hh:mm], you can input, for example:

Command	Description
periodic 8:00 to 17:30	Sets the relative time segment from 8:00 to 17:30
periodic weekday Saturday 8:00 to 17:00	Sets the relative time segment on weekdays (Monday to Friday) and Saturday from 8:00 to 17:00.
periodic Friday 17:30 to Monday 8:00	Sets the relative time segment from 17:30 on a Friday to 8:00 the following Monday.

To define an absolute time segment:

Command	Description
absolute [start time date] [end time date]	Note: You can omit the start and end clauses by using the no command, which tells the system when it can start or stop allowing access.

To define [start time date] [end time date]:

Command	Description
absolute start 8:00 31 January 2004 end 8:00 15 February 2005	Sets the absolute time segment to 8:00 on January 31, 2004, to 8:00 on February 15, 2005.

Time Range Applications

Displaying a time range's status: Whether the time range works or not depends on its status (ON or OFF), regardless of the filtering rule or access list the time range might be bound to. That status will also correspond to its respective time segment status

Clearing or changing a time range status: A time range will be cleared within a minute in default mode. You may have to wait up to 60 seconds before any of your changes are applied to the system.

Cisco Configuration Comparisons

A Cisco router permits an absolute time segment rule within a time range, while a Signamax router can allow many absolute time segment rules within the system. The absolute time in Cisco systems is a genuine form of absolute time and the date should be set according to a rigorous format: day, month and year. But Signamax router products tells time in a kind of relative way, so the month and year in a date can be omitted.

Dealing With Time Judgment Issues

Binding Time Ranges To Packet Filtering

Packet filtering will work only when the time range status is ON. The command format is consistent with Cisco's setup. For example:

Command	Description
Permit any log time-range t_r_name1	
Access-list 1001 deny TCP any any time-range t_r_name2	

Add the time range name at the bottom of your filtering rules. Its position comes after the log file, just like in Cisco's router systems. Note: There isn't a special command that you can use to cancel the binding relationship. If you want to cancel the command, you first have to delete the filtering rule and then resubmit the same rule without imputing a time limit.

When the router compares a data packet against the filtering rules, the trange term will not participate in this matching process. In fact, when a time range is bound to two filtering rules, the rules are considered to be the same by the router. If there were two different filtering rules for the same task in an access list, then the time limit rule would not work at all.

Filtering:

Whether a filtering rule that's bound to a time range will work or not is dependant on the time range's status. When a data packet is filtered, each filtering rule in the access list you've applied will be matched against it one by one. If a filtering rule is bound to the time range, and the time range status is OFF, then the rule will be skipped in the system and the next filtering rule will be matched against it.

Note: If the time-range status is set to OFF, all of the bound time ranges will not work. (Please refer to Chapter 5, Environment Parameters.) All of the filtering rules, no matter whether they are bound to time ranges or not, will participate in the filtering procedure.

Binding a time range to an access list

Binding a time range to an access list is considered the equivalent of binding a time range to each filtering rule within the access list.

This operation's command is:

```
ip time-range time-range-name access-list a-l-name| a-l-number
```

Your can remove the binding by using the command no. When this type of access list filters a packet, the status of the time range should be the first thing to be examined by the system. If the status of the bound time range is set to OFF, all of the filtering rules will be ignored and this access list will be considered the equivalent of an empty list by the system.

Configuring time range environment parameters

The timelive time inverse accumulated counter default frequency is set at one minute.

The configuring command is as follows:

Command	Description
Set time-range frequency number	Number refers to the time difference between the two times being cleared by the system. The time difference unit is 60 seconds, and is stored at the "range-frequency" global variable.

The counter and system time difference is, by default, 100 seconds.

The configuring command is as follows:

Command	Description
Set time-range max-offset number	Once the time difference is overstepped, the status of every time range will be judged again. Timelive will be computed and the accumulated time of the counter will be updated. The max difference time is stored at the global variable: time_max_offset.

Time range enabling switch

When the default switch value is ON, every bound entity will have a time limit. If the status of the switch is set to OFF, every bound time range will not work, and all clauses with the name "time-range" to will be ignored by the filter. (To the access list, the binding relationship won't even exist.) The switch's status value is stored at the global variable named trange_enable.

Command	Description
Set time-range disable	[OFF]: Once the switch is set to OFF, the time range refreshing process that's running in the background will be aborted.
Set time-range enable	[ON]

Media Access Control (MAC) Address Packet Filtering

The MAC address can filter the source address of a data packet at the interface level.

Setting Access List

An access list can be added in the configuring mode. There are two kinds of adding modes:

Command	Description
Mac access-list standard 2001-3000 | name	This mode can locate the special access list and enter the configuration mode of the access list. If the access list does not exist, a new access list will be created. In the access list configuration mode, you can configure an access list's filtering rule.
Access-list number permit deny	This mode can add a filtering rule to a specified access list directly in configuration mode. If the access list doesn't exist, a new one will be created and the mode won't change.
No mac access-list standard number|name	Deletes the access list.
No access-list number	Deletes the access list.

Adding Filter Rules:

Command	Task
permit|deny any | host macaddress | macaddress macmask	This command can be executed in the access list configuration mode. You can delete a rule with the using the no command.

The second mode listed in the preceeding table [Access-list number permit deny] can also be used to add a filtering rule. (When using this command with a Cisco system, you can add an access list and a filtering rule. However, Cisco only provides a command to delete an access list. It doesn't provide a related command to delete a filtering rule.)

Command	Task
router(config)#mac access-list standard 2002 router(config-std-mac-nacl)#permit host 1.1.1	
router(config-std-mac-nacl)#permit 2.2.2 0.0.ffff	
router(config-std-mac-nacl)#deny any	

Binding an Interface

A binding can be configured in the interface mode. You can use the no command to remove it.

Command	Description
mac access-group number|name in|out	

Configuration example

On f0, refuse the packet 0005.5d5e.4129 from mac address.

Command	Description
router(config)#access-list 2001 deny host 0005.5d5e.4129	Configure an mac access list rule, and refuse Mac source address 0005.5d5e.4129 packet.
router(config)#interface f0	
router(config-if-fastethernet0)#mac access-group 2001 in	Binding to f0, in

Above command is same as:

Command	Description
router(config)#mac access-list standard 2001	Standard mac access list configuration
router(config-std-mac-nacl)#deny host 0005.5d5e.4129	Configure an mac access list rule, and refuse Mac source address 0005.5d5e.4129 packet
router(config-std-mac-nacl)#exit	
router(config)#interface f0	
router(config-if-fastethernet0)#mac access-group 2001 in	Binding to f0, in

Reflect Access List

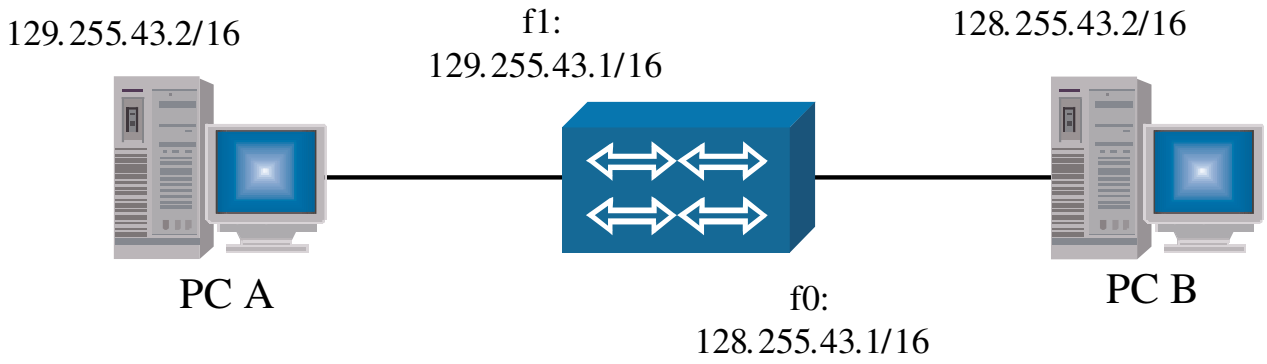
A reflect access list can be used to realize that: 1) the connection between network A and network B can be established via a router; 2) Network A can forwardly access network B, however network B cannot forwardly access network A.

The configuration commands of reflect access list are listed as follows:

Syntax	Description
ip access-list extended 1001 permit ip 129.255.0.0 0.0.255.255 128.255.0.0 0.0.255.255 reflect AtoB exit	Add a keyword reflect behinds the extended access list, and name the reflect access list after AtoB.
ip access-list extended 1002	Create an additional access list, and configure

evaluate AtoB exit	an item to refer to the reflect access list AtoB that has been defined above.

The following case of simple configuration is used to describe the configuration and usage of the reflect access list.



To realize that PC_A can access PC_B and PC_B has no way to access PC_A, MP router should be configured as follows:

Syntax	Description
router# config terminal	
router(config)# ip access-list extended 1001	Define the extended access list 1001.
router(config-ext-nacl)# permit host 129.255.43.2 host 128.255.43.2 reflect AtoB	Define the reflect access list AtoB.
router(config-ext-nacl)# exit	
router(config)# ip access-list extended 1002	
router(config-ext-nacl)# evaluate AtoB	
router(config-ext-nacl)# exit	
router(config)# interface fastethernet1	
router(config-if- fastethernet1)# ip access-group 1001 in	
router(config-if-ethernet)# exit	
router(config)# interface fastethernet0	
router(config-if- fastethernet0)# ip access-group 1002 in	
router(config-if- fastethernet0)# exit	

Configuration & Usage of Security Accounting

"Security Accounting" is a special function of MP router cooperating with MP "security accounting server", applied to user charge, user bandwidth control and user authentication control etc.

Generally, the topological structure is : the user of the network connecting with some interface of the router cannot access Ethernet until he passes the user authentication successfully. Generally, the interface cannot support direct-connection users except the direct-connection servers.

Configure a direct-connection server:

If the user cannot pass the user authentication successfully, all packets of the user are denied. But some connection with some servers, such as DHCP server, DNS server and authentication server should be permitted. A system manager can, via the router, perform the direct-connection configuration of those servers and packets communicating with the servers are permitted to pass:

```
Use the following command to configure a server.
flux-control  server [addr1 addr2…….]
Use the following command to delete some direct-connection server:
no  flux-control  server [addr1 addr2….]
```

Configuring an internal interface:
An internal interface is a restricted interface, via the interface the internal user can connect to the router. And "Security and Accounting" can take effect on nothing but the packets entering the internal interface.

```
fluc-control interface [interface1 interface2….]
Use the following command to cancel an internal interface.
no  fluc-control  interface [interface1 interface2….]
```

Configure the Web authentication server (Authentication interception):
To configure the transparent authentication, that is to say that the system can automatically send the authentication page to the user when the user tries to connect to Ethernet, please use the following command to configure the Web authentication server on the router.

```
flux-control  web-server  addr  [port  server-port  ] [interface interface-name]
```

When the server is configured as the Web authentication server, the

server can also serve as the direct-connection server .
Recommend: the interface parameter, which is used to connect the server and the router, had better follow the command; or, the system will, according to the route, automatically judge the network segment, at which the router is located, and determine the connection interface. And if firewall configuration precedes route configuration, some unexpected errors may happen and "authentication interception" will be unsuccessful.
Use the following command to delete the configuration:

```
no  flux-control  webserver
```

"Authentication interception" will be closed automatically and the direct-connection server with the same address will be deleted.

1) Open "Security accounting":

```
flux-control on
```

Close "Security accounting":

```
flux-control off
```

```
if "Security accounting" is opened again after closed, the configuration will not be lost.
```

Display related information:

```
Display the simple information:

show  flux-control

The command above is used to display  basic configuration, status and user IP addresses of authenticated users.

For example:

router#show flux-control
  flux-control server 128.255.253.80 128.255.250.170
  flux interface ethernet0
  Web_server:   128.255.250.170:8000      connet   interface: ethernet0  redirect flag :1
   flux-control state: ON


   login user IP:
   128.255.251.89
        128.255.252.61


Display the detailed information::

show flux-control detail

If the detailed information is displayed, the packet filtering rules of the user passing user authentication will also be displayed.

For example:
```

```
router#show flux-control detail
  flux-control server 128.255.253.80 128.255.250.170
  flux interface ethernet0
  Web_server:   128.255.250.170:8000      connet   interface:
ethernet0  redirect flag :1
   flux-control state: ON

   login user IP:
   128.255.251.89
     rule no:0 PERMIT dst range:0.0.0.0 - 255.255.255.255
     Send: 417 / 417 bytes;  Receive: 1389 / 1389 bytes.
        128.255.252.61
     rule no:0 PERMIT dst range:0.0.0.0 - 255.255.255.255
     Send: 782 / 782 bytes;  Receive: 5628 / 5628 bytes.
```

Display the record of Web authentication address translation:

```
show flux-control redirect
```

The system will display a record of address translation, of which, scr-ip and src-port are user source address and user source port, dst-ip and dst-port are user destination address and user destination port, state represents the record state (0 means that only one syn message of the user is received and 1 means that multiple messages have been received or a connection has been established), age represents the aging time (by second) in which the connection is live.

If the user and server follow the same interface, termp-in and termp-port, which serve as frame-relay address and port temporarily, will be displayed.

For example:

```
router#show flux-control redirect


src-ip           src-port   dst-ip           dst-port   temp-ip
temp-port  state  age
128.255.251.89 1035     192.168.1.200 80         128.255.251.88
54345      1    24
128.255.251.89 1034     192.168.1.200 80         128.255.251.88
54089      1    24
```

About bandwidth limit:
When the authentication server performs bandwidth limit for some user, the bandwidth limit is realized factually on the router.

Its mechanism is that the flow limit is performed in unit time. When there exists the limit, the bi-directional flow in the unit time cannot exceed the bandwidth limit.

By default, the flow limit of a message is performed only for egress messages. This is because that: when performing the flow limit, ISP allows for the bandwidth of the egress line connecting with a router; since there exist ingress user messages, which have consumed the bandwidth of the egress line in fact; it is unreasonable to deny the ingress messages after the comprehensive consideration. So, when there exist some user ingress messages, whether the used bandwidth has exceeded the bandwidth limit or not, these messages will be permitted

When the system adopts the default configuration, the factual flow permitted will be more than the bandwidth control in a small degree if the quantity of user messages is by far more than its bandwidth limit. The deviation between the factual flow and the bandwidth limit depends on network delay and the configured unit time.

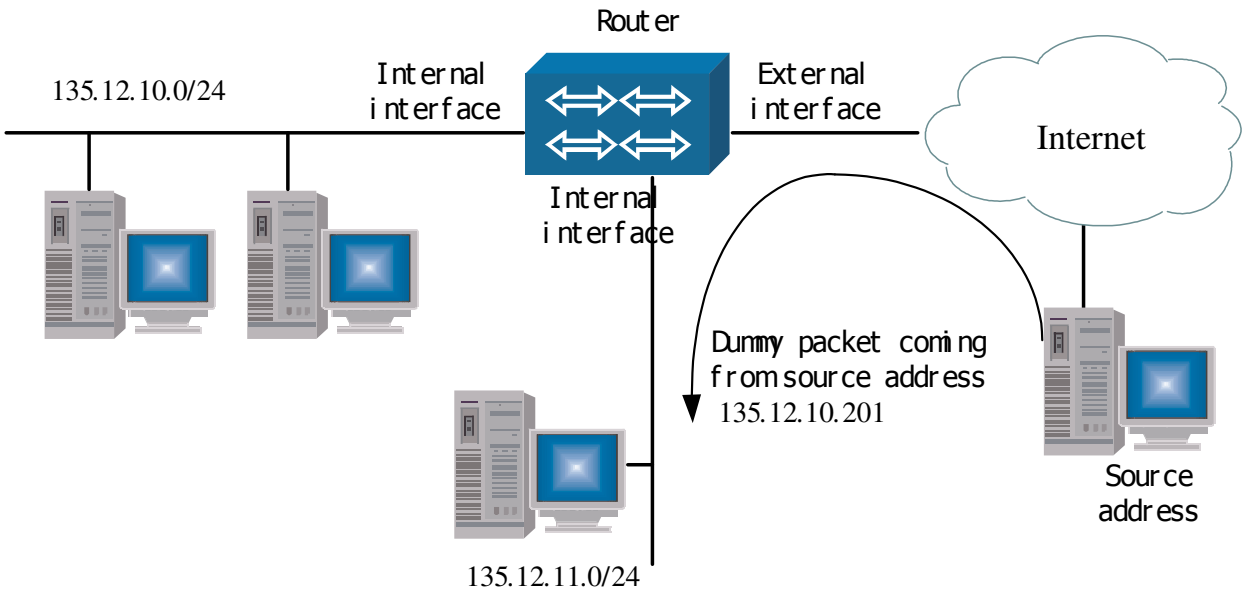
To perform the bandwidth limit for ingress messages, use the following command.

```
flux-control  band-in
use the following command to cancel the configuration.
no  flux-control  band-in
The unit time of bandwidth sampling is 3 seconds by default.
Use the following command to change the unit time:
flux-control  cell-time  number
```

A Few Points About Firewall Configuration

Preventing Messages From Dummy Addresses

The packet filter sifts via data in the packet coming in, coming out or coming via the network in both directions. For reasons of efficiency, many packet filters only examine a data packet traveling in one direction.


Router
135.12.10.0/24
Internal interface
External interface
Internet
Internal interface
Dummy packet coming from source address 135.12.10.201
Source address
135.12.11.0/24

If the packet was filtered when it was sent out via a router, some information will be lost. This means that the interior network can easily be attacked by a user with a fake (or dummy) address, as shown in the preceding figure.

In that figure, the network 135.12.0.0 is connected to the Internet via a router. That interior network has two subnets. The network subnet masks to both subnet 10 and 11 have the following address: 255.255.255.0. A packet from the fake IP address 135.12.10.201 is shown coming from an exterior TCP/IP host.

It is then received by the router's exterior interface. If the router is set to filter incoming data packets, the dummy packet will be quickly noticed and it will be prevented from entering the network. Since the router knows that the network 135.12.10.0 is connected to a different (ie. interior) interface, it knows the packet can't be coming from an exterior interface.

But if the packet filter is only set to examine the outgoing data packets, the router won't be able to check the exterior interface and the message from the dummy address will enter the network.

In order to add more security to your network, you can add some 'anti-cheat' rules to your incoming access list to bind the filter to an exterior interface. The aim of this is to tell the router to refuse both interior network source addresses and invalid source addresses.

Invalid source addresses can include a non-registered address, a loop-back address and a broadcasting address. Hackers often use these types of source addresses to prevent them from being tracked and discovered by a network manager.

The following commands can be added to the inward access list that is applied to your exterior interfaces. They will prevent some dummy IP addresses.

```
access-list 1001 deny ip 135.12.10.0   0.255.255.255 any (an
interior network)

access-list 1001 deny ip 135.12.11.0   0.255.255.255 any (an
interior network)

access-list 1001 deny ip 10.0.0.0    0.255.255.255 any (a
reserved IP address)

access-list 1001 deny ip 172.16.0.0    0.31.255.255 any (a
reserved IP address)

access-list 1001 deny ip 192.168.0.0    0.0.255.255 any (a
reserved IP address)

access-list 1001 deny ip 127.0.0.0    0.255.255.255 any (a
reserved IP address)

access-list 1001 deny ip 224.0.0.0   31.255.255.255 any (a
reserved IP address)
```

These anti-cheat rules should be stored in your system before any other rules on the inward access list. This will ensure that only packets containing a valid IP address will be checked against the remaining rules.

Applying Access List

The task of applying an access list should immediately follow its construction. If the access list doesn't have any rules applied to an interface, any data – valid or invalid – can be permitted into your network.

Hint: You should not apply an access list without any interface definitions. You should remove an access list from the interface before any changes are made to the system.

Each interface can have an inward access list and an outward access list, but you can't have two or more kinds of the same list – inward and outward rules should be on the same list. When more than one access list is applied to the router, only the last access list you've added will work.

Locating Packet Filter

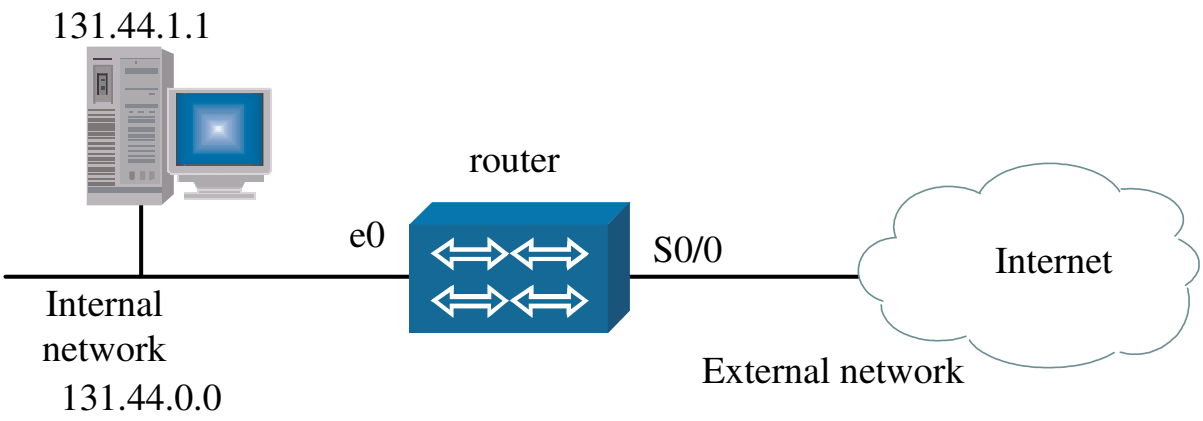
The security filter can often sift via data in an inward direction and drop distrustful-looking packets. This will prevent dummy addresses from cheating the system before all of the packets are routed. But a packet filter works in the opposite manner of a traffic filer, which examines information traveling out of the network and prevents needless packets from occupying a special data link.

You should consider your CPU resources for processing an access list and routing activity. If most of your packets are filtered out after they've been routed via the system – which is, of course, referred to as inward filtering – you will probably save some CPU space.

The standard access list should be placed as close to the source address as possible in order for your network to communicate quickly with another host or network. That way, when a packet is denied, bandwidth and CPU space that's being occupied by the packet won't be wasted.

Because an extended access list has the function of precisely identifying a packet, it should be used as close to a source address as possible in order to prevent the denied packet from occupying the bandwidth and CPU. On the other hand, because of the complexity of the extended list, you will be adding processing burdens to your bandwidth and CPU.

Configuration Example



Note: The above example illustrates a network with the following security policies in place:

All interior network hosts (131.44.0.0) can access any TCP Internet service.

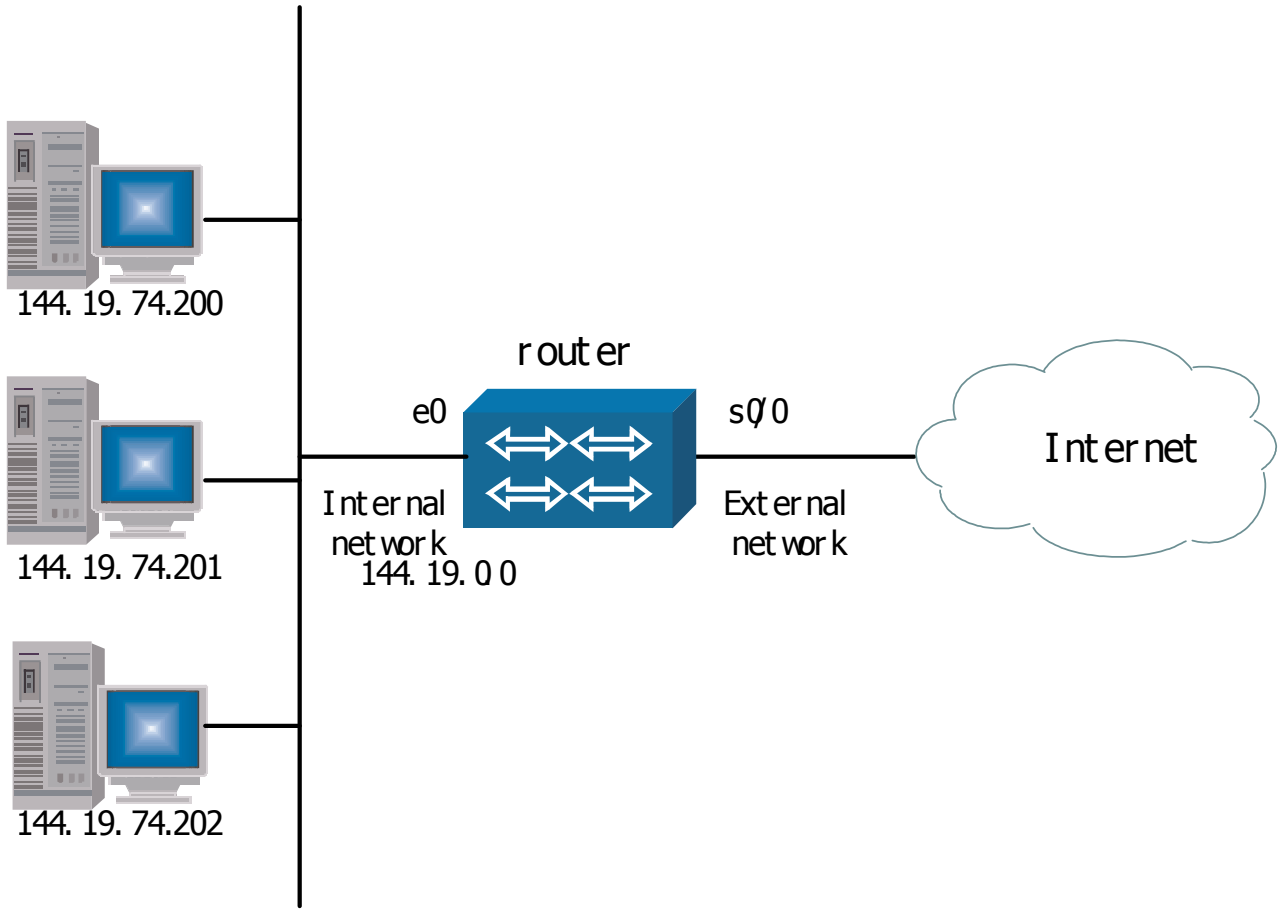
Exterior hosts can access the SMTP service in the mail gateway 131.44.1.1, but can't access the interior network itself.

All ICMP messages will be blocked.

These policies can be configured on the router by imputing the following series of commands:

Command	Task
router# config terminal	
router(config)# ip access-list extended 1001	Defines an extended access list as 1,001.
router(config-ext-nacl)# permit TCP 131.44.0.0 0.0.255.255 any	
router(config-ext-nacl)# permit ICMP any 131.44.0.0 0.0.255.255	
router(config-ext-nacl)# exit	
router(config)# access-list 1002 permit TCP any 131.44.0.0 0.0.255.255 established	
router(config)# access-list 1002 permit TCP any host 131.44.1.1 eq 25	
router(config)# interface ethernet 0	
router(config-if-ethernet0)# ip access-group 1001 in	
router(config-if-ethernet)# exit	

router(config)# interface serial 0	
router(config-if-serial0)# ip access-group 1002 in	
router(config-if-serial0)# exit	
router(config)#	



The above example illustrates a network with the following security policies:

The outer email and news servers can be permitted to access Interior Host 144.19.74.200 and Host 144.19.74.201.

DNS access in the gateway server 144.19.74.202 is permitted.

The interior hosts are permitted to access all TCP services in the exterior network, except Gopher and Web servers.

All above policies can be configured on the router as follows:

Command	Task
router# config terminal	
router(config)# ip access-list extended ether-in	
router(config-ext-nacl)# deny TCP 144.19.0.0 0.0.255.255 any eq 70	
router(config-ext-nacl)# deny TCP 144.19.0.0 0.0.255.255 any eq 80	
router(config-ext-nacl)# permit TCP any	
router(config-ext-nacl)# exit	
router(config)# ip access-list extended serial-in	
router(config-ext-nacl)# permit TCP any 144.19.0.0 0.0.255.255 established	
router(config-ext-nacl)# permit TCP any host 144.19.74.200 eq 25	
router(config-ext-nacl)# permit UDP any host 144.19.74.200 eq 119	
router(config-ext-nacl)# permit TCP any host 144.19.74.201 eq 25	
router(config-ext-nacl)# permit UDP any host 144.19.74.201 eq 119	
router(config-ext-nacl)# permit UDP any host 144.19.74.202 eq 53	
router(config)# interface ethernet 0	
router(config-if)# ip access-group ether-in in	
router(config-if)# exit	
router(config)# interface serial 0	
router(config-if-serial0)# ip access-group serial-in in	
router(config-if-serial0)# exit	
router(config)#	

Network Address Translation (NAT) Configuration

NAT uses to complete the translation between partial and global address. ◦

Basic Commands

router (config)#ip nat ?

Command	Description
Frequency	NAT translation timeout frequency
inside	Inside address translation
pool	Define pool of addresses
redirect-enable	NAT redirect enable
translation	NAT translation entry configuration

To define an IP address pool, use the global configuring command ip nat pool.

To delete this pool, use the command format: no ip nat pool.

```
router(config)#ip nat pool name start-ip end-ip
{netmask netmask | prefix-length prefix-length}
[type rotary]
```

Syntax	Description
Name	The Address Pool Name
start-ip	The Start Address
End-ip	The End Address
Netmask	Network Mask
prefix-length	The network mask digits signify which mask all addresses in the pool belong to.
type rotary	Indicates that the address pool scope has true hosts addresses. A TCP load will be assigned based to these hosts. (Optional function.) This pool type is only applied to incoming address NAT configuration.

Command	Description
router(config)#no ip nat pool name	Deletes the address pool.

The same address pool can't be referred to by two different NAT configurations. If two NAT definitions should be incorporated together, make sure you alter related access list rules. Also, the same IP address cannot be defined in two different pools. You may cause the system to malfunction if you do.

To build an interior source address NAT, use the global configuring command ip nat inside source.

To delete a static or dynamic translation, use the command format no ip nat inside source.

Construct a basic static translation with the static key.

```
router(config)#ip nat inside source list {access-list-number
| name} pool   name [overload]
```

Syntax	Description
access-list-number	The access list name or number
Name	The address pool name
Overload	Enables the router to use a global address in the place of many local addresses. When the overload parameter is configured, the TCP or UDP port number of each interior host is used to distinguish different sessions where the same local IP address was used. (Optional function).

```
router(config)#ip nat inside source static {tcp | udp} local-
ip local-port global-ip global-port
```

Syntax	Description
local-ip	Interior local address
global-ip	Interior global address
tcp | udp	Protocol
local-port	Interior local port number
global-port	Interior global port number

To start using the incoming NAT, type in the global configuring command ip nat inside destination.

To delete a dynamic translation, input no ip nat inside destination.

When the incoming NAT is used to share the TCP load use:

```
router(config)#ip nat inside destination list {access-list-number | name} pool name
```

Syntax	Description
Pool name	The pool name. The pool comprises a local address assigned in dynamic translation. The pool type is ROTARY, and the pool address is a true interior local host address.

To designate an interior or exterior NAT interface, use the interface configuring command ip nat.

To remove this function, enter no ip nat.

You can't use an interior and exterior interface at the same time.

```
router(config-if)#[no] ip nat {inside | outside}
```

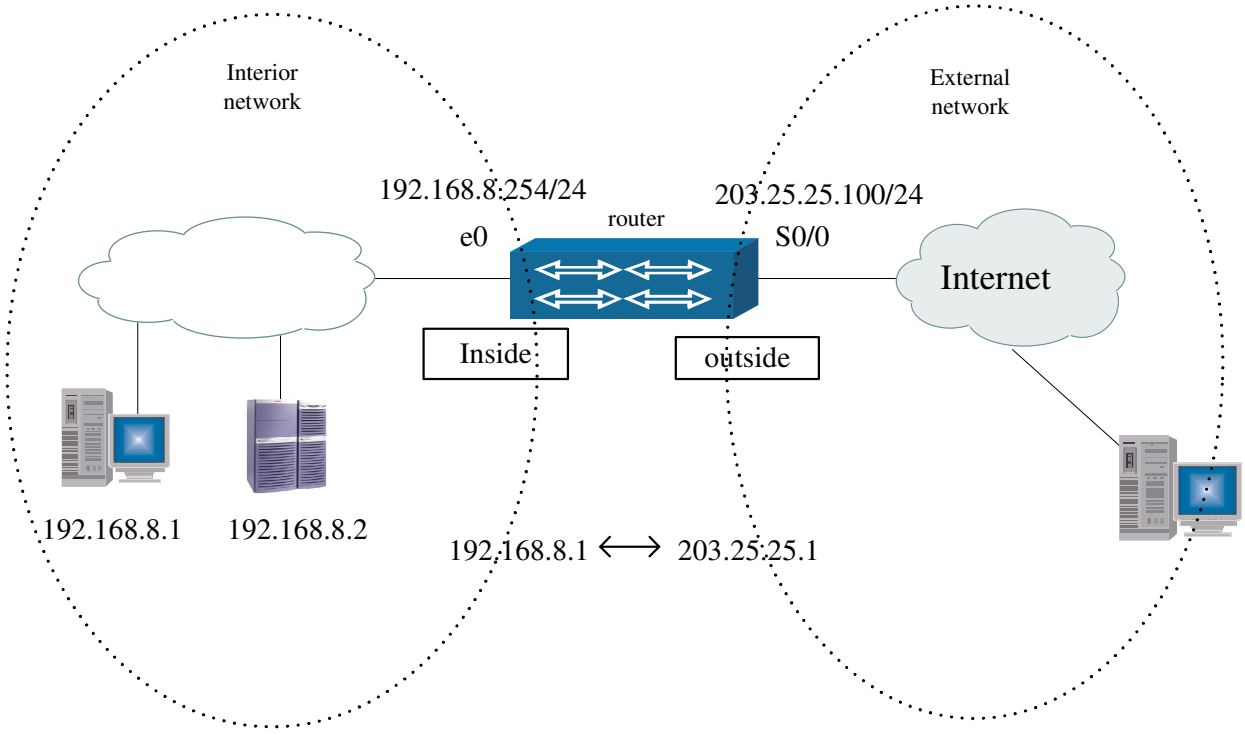
Syntax	Description
Inside	Designates the interface to connect with the interior network.
Outside	Designates the interface to connect with the exterior network.

Interior Source Address Translation

When communicating with the router, you can use this feature to change your IP address into an exclusive global IP address via static or dynamic translation. Static translation builds a one-to-one map between an interior local address and an interior global address, which is helpful when a fixed address wants to access an interior host from the outer network. Dynamic translation, on the other hand, maps an interior local address with a global address pool.

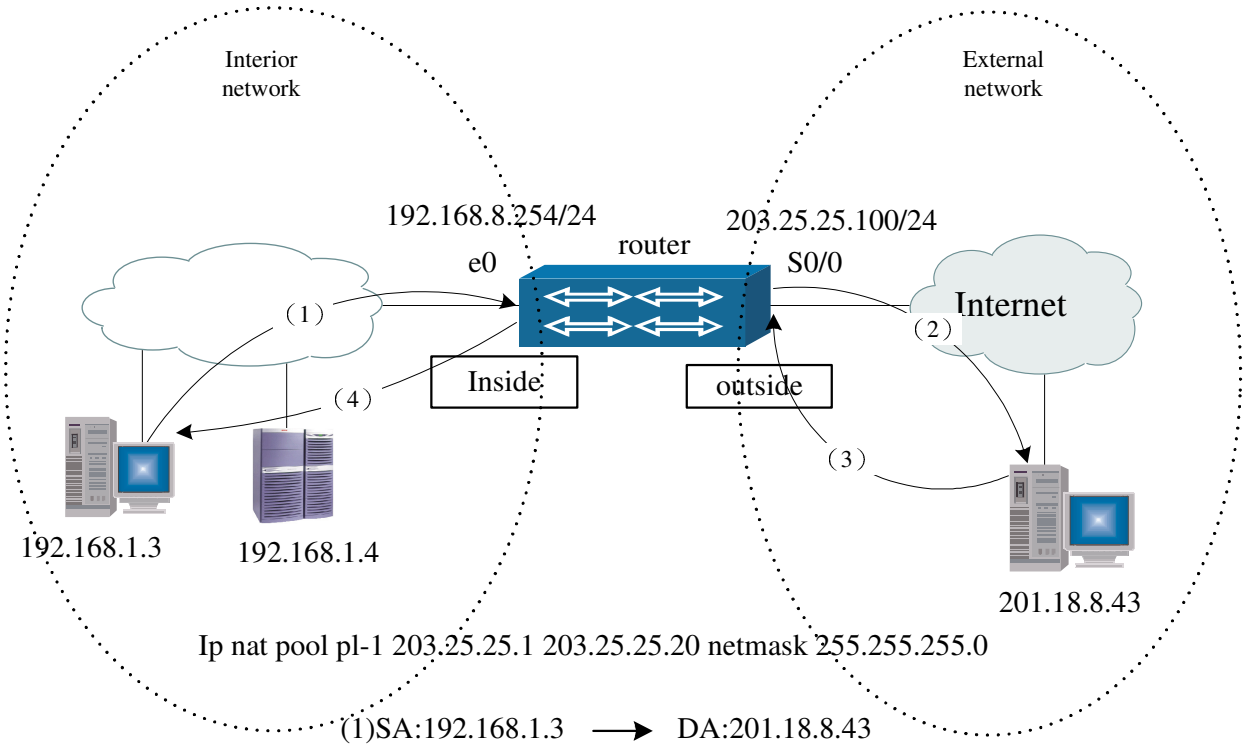
Static Translation Configuration

First, construct a static translation from 192.168.8.1 to 203.25.25.1. Configure the Ethernet interface 0 to an interior interface. Configure the serial 0 to an exterior interface.



Command	Task
router(config)#ip nat inside source static 192.168.8.1 203.25.25.1	Constructs a static translation from 192.168.8.1 to 203.25.25.1.
router(config)#interface e0	Designates the interface e0.
router(config-if-ethernet0)#ip nat inside	Connects the marked interface to an interior network
router(config)#exit	
router(config)#interface s0	Designates the interface s0
router(config-if-serial0)#ip nat outside	Connects the marked interface to an exterior network

Configuring Dynamic Translation



In order to translate the interior source address on the router in the preceding example, it should be configured as follows:

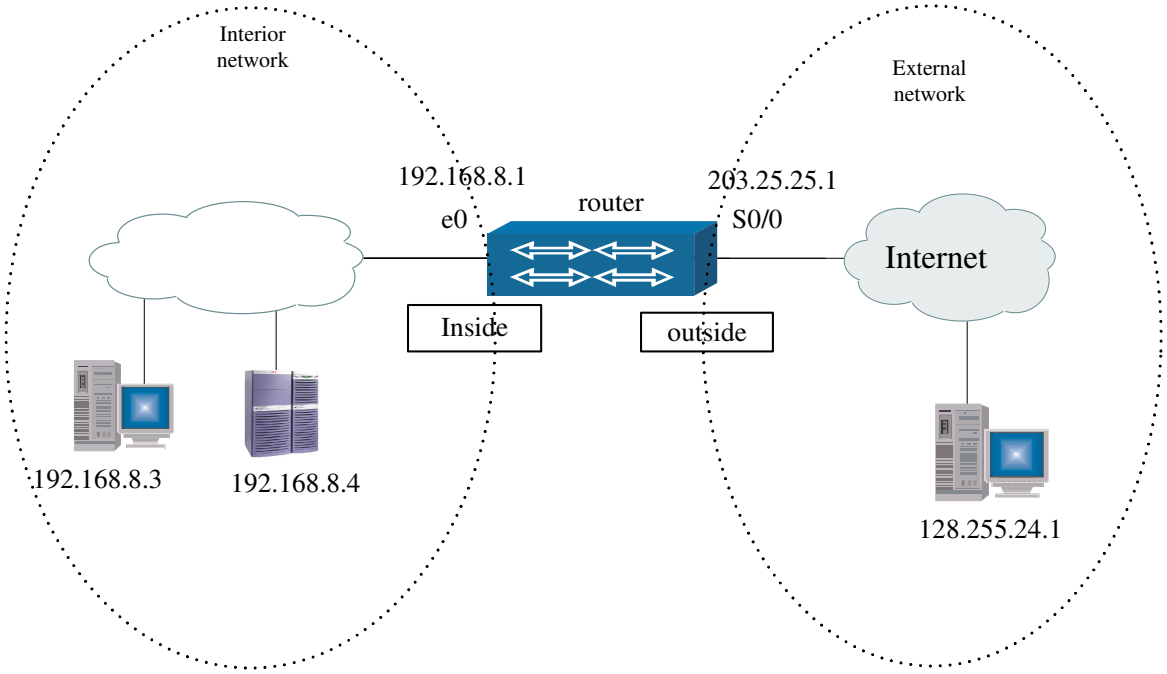
Command	Task
router(config)#ip nat pool pl-1 203.25.25.1 203.25.25.20 netmask 255.255.255.0	Constructs a global address pool with the name pl-l. The pool comprises 20 global addresses from 203.25.25.1 to 203.25.25.20.
router(config)#access-list 1 permit 192.168.8.0 0.0.0.255	Constructs an access list 1 and allows the network segment addresses 192.168.8.0 and 0.0.0.255 to be translated.
router(config)#ip nat inside source list 1 pool pl-1	Performs the address translation between list 1 and pool –1.
router(config)#interface e0	Designates the interface e0.
router(config-if-ethernet0)#ip nat inside	Connects the marked interface with the interior network
router(config-if-ethernet0)#exit	
router(config)#interface s0	Designates the interface s0.
router(config-if-serial0)#ip nat outside	Connects the marked interface with the exterior network
router(config-if-serial0)#exit	
router(config)#	

In the preceding case, a global address pool pi-1 is first constructed. The pool comprises 20 global addresses between 203.25.25.1 to 203.25.25.20. The access list 1 permits all hosts in the interior network to perform address translation. The Ethernet interface 0 is configured as an interior interface and the serial is configured as an exterior interface.

The access list should permit these addresses to be translated. An access list that permits too many addresses translations could allow a security breach or other type of malfunction.

Interior Global Address Overload

The router will be allowed to map many local addresses to a global address in order to save addresses in your interior global address pool. When an overload has been configured, the router will maintain original data from higher layers – for example: the TCP or UDP port numbers – to ensure that the global address will be translated into the right local addresses. When many local addresses are mapped into a global address, the TCP/UDP port numbers of each interior host will be used to differentiate between all of these different local addresses.



Internal local address: port	internal global address: port	external global address: port
192.168.8.3:2345	203.25.25.1:10027	201.255.24.1:80
192.168.8.4:1718	203.25.25.1:10028	201.255.24.1:80

In order to overload global addresses on the router, as shown in the preceding figure, the router should be configured as follows:

Command	Task
router(config)# ip nat pool pl-2 203.25.25.1 203.25.25.5 netmask 255.255.255.0	Builds a global address pool called pl-2. The pool comprises five global addresses between 203.25.25.1 and 203.25.25.5.
router(config)# access-list 1 permit 192.168.8.0 0.0.0.255	Permits access list 1 to perform the address translation to all hosts in the interior network.
router(config)# ip nat inside source list 1 pool pl-2 overload	Allows the access list 1 and the address pool pl-2 to build a dynamic source translation.
router(config)# interface e0	Designates the interface e0
router(config-if-ethernet0)# ip nat inside	Marks the above interface as an interior one
router(config-if-ethernet0)# exit	
router(config)# interface s0	Designates the interface s0
router(config-if-serial0)# ip nat outside	Marks the above interface as exterior.
router(config-if-serial0)# exit	
router(config)#	

In this example, the global address pool pl-2 is built first. The pool comprises five global addresses between 203.25.25.1 and 203.25.25.5. The access list 1 permits all hosts in the interior network to perform an address translation. The Ethernet interface 0 is configured as an interior interface, while serial 0 becomes an exterior interface. The router then allows many local addresses to use a global address.

Interior Destination Address Translation
If many interior network hosts – for example, Web servers – provide the same access to many continuous interior IP addresses, then you can configure the NAT translation of the interior destination address to obtain simple TCP load sharing. That way, the router can process many outbound global addresses.

The steps to configuring an interior destination address translation in the global configuration mode are as follows:

Define a rotary type of IP address pool that can be assigned as needed. The addresses in the pool are interior host addresses, and will be used to share the TCP load.

```
router(config)#ip nat pool name start-ip end-ip
{netmask netmask | prefix-length prefix-length} type rotary
```

Syntax	Description
Name	Pool name
Start-ip	Start address
end-ip	End address
netmask	Network mask
prefix-length	The mask's bit number
type rotary	The true IP host

Define an access list and permit addresses in this list to be translated.

```
router (config)#access-list access-list-number permit source
source-wildcard access-list access-list-number permit
protocol source source-wildcard destination destination-
wildcard [precedence precedence] [tos tos] [log]
```

Please consult the preceding section again and the section on firewall configuration (Section One) for a list of definitions related to each command.

This access list can generally be defined as an extension access list to limit the number of destination addresses from received data packet. It will only be translated when the exterior interface receives the destination address of the data packet.

Construct an interior destination translation based on the access list and the address pool you configured in the above steps.

Command	Description
ip nat inside destination list access-list-number pool name	

Designate an interior interface.

Command	Description
interface type number	

Mark the interface to connect with the interior.

Command	Description
ip nat inside	

Designate an exterior interface.

Command	Description
interface type number	

Mark the interface to connect with the exterior.

Command	Description
ip nat outside	

If there is only one interior host being used, it isn't necessary to perform dynamic NAT configuration. If you want to use NAT to hide the host IP address, then configure your router using static NAT. Because dynamic NAT only works for TCP data packets, you'd be better off using static NAT configuration – especially if your host provides other protocol services.

Change NAT Translation Parameter

Use ip nat translation command to change NAT translation parameter. Use no to reuse the default value.

```
ip nat translation {dns-timeout | finrst-timeout | icmp-error | icmp-max-entries | icmp-timeout | max-hash-size | max-proxy-entries | port-timeout| syn-timeout | tcp-timeout| timeout| udp-timeout}
```

Syntax	Description
dns-timeout	DNS translation timeout is 300 seconds by default.
finrst-timeout	Complete and reset TCP translation Timeout, 60 seconds.
icmp-error	ICMP protocal error type translation timeout is 60seconds by default.
Icmp-max-entries	ICMP translation max number is with memory below 64M:50—500,100 by default below 64M—128M:50- 2500,500 by default above 128M: 50- 5000,1000 by default
icmp-timeout	ICMP translation, 300 seconds by default.
max-entries	NAT translation max number is with memory below 64M: 5000—23000,10000 by default below 64M—128M: 5000-53000,23000 by default above 128M: 5000-150000,53000 by default
max-hash-size	NAT translation hash size is with memory. below 64M: 997 by default below 64M—128M: 1999 by default above 128M: 2999 by default
max-proxy-entries	When NAT reaching max_entryes, the added NAT proxy translation number is with memory. below 64M: 1000 by default below 64M—128M: 2000 by default above 128M: 4000 by default
port-timeout {tcp/udp} port value	Configure timeout for designated port translation record.

syn-timeout	TCP SYN status translation timeout. 90 seconds by default.
tcp-timeout	TCP translation timeout. 1800 seconds (30 minutes)
timeout	*simple dynamic translation timeout. 1800 seconds (30 minutes)
udp-timeout	UDP port translation timeout, 600 seconds by default(10 minutes)

`ip nat translation timeout`

Syntax	Description
<1_2147483647>	Timeout
never	Never timeout

For example:

Command	Description
router(config)#ip nat translation timeout 120	Configure timeout 120 seconds

(command mode)privileged user mode

NAT Monitoring, Maintenance & Debugging

Mornitoring and Maintenance Commands:
The dynamic address translation item can be removed with the privileged user command clear ip nat translation before you set a timeout.

Command	Task
router(config)#clear ip nat translation all	Clears all dynamic transmissions.
router(config)#clear ip nat translation inside global-ip local-ip	global-ip: Global address local-ip: Local address Clears the simple dynamic translation item.
router(config)#clear ip nat translation {tcp | udp} inside global-ip global-port local-ip local-port	global-ip: Global address global-port: Global port local-ip: Local IP address local-port: Local port Clears the extended dynamic translation item.

You can display the active translation list item with the privileged user

command show ip nat translations.

Command	Task
router#show ip nat translations	

The following are output examples of the preceding command:
You can use the global addresses 128.255.251.84 and 128.255.251.85 to communicate with some exterior hosts without overloading.

```
router# show ip nat translations

Dir  Pro  Hv0  Hv1    Inside global       Inside local           Outside global
Age

out  ---   426  982    128.255.251.85        192.168.0.2          128.255.251.90
1783

out  ---   425  981    128.255.251.84        192.168.0.2          128.255.251.89
1761

Dir   Pro     Inside global:Port       Inside local:Port     Outside global:Port
Flags

in    ----     201.10.10.1               10 .0 .0 .90         228.255.255.99

in    ----     201.10.10.2               10 .0 .0 .97         129.55.9.3
```

You can use one global address to perform an address translation by overloading.

```
router# show ip nat translations
Dir Pro   Hv0 Hv1   Inside global         Inside local          Outside global
Age
out ICMP 850 16   128.255.251.86:1027  192.168.0.2:44080
128.255.251.90:44080   295
out ICMP 849 15   128.255.251.86:1026  192.168.0.2:44080
128.255.251.89:44080   288
```

Translate 192.168.0.2 into 128.255.251.86 to access the exterior address 128.255.251.90/89.

```
Dir    Pro       Inside global:Port          Inside local:Port
Outside global:Port  Flags

in     ----       201.10.10.1:1026          10  .0  .0  .90:2347
228.255.255.99:23

in     ----       201.10.10.1:1027          10  .0  .0  .97:3455
129.55.9.3:21
```

The preceeding fields are defined as follows:

Field	Description
Dir	Creates the translation's packet direction.
Pro	Recognizes the overload translation protocol.
Hv0 Hv1	The NAT record location.
Inside global	The interior global IP and its port
Inside local	The interior local IP and its port
Outside global	The exterior global IP and its port
Age	The remaining lifetime of the NAT record, told in seconds.

You can display the NAT statistics with the privileged user command show ip nat statistics. Clear them by typing clear ip nat statistics.
router# **show ip nat statistics**

Information	Description
NAT version: 5.6	
Total translations: 0 static, 2 dynamic	
No memory: 0, Execcess drop: 0, Age1: 0, Age2: 0, Age3: 0	
Translation mode: NATNAPT	
NAT redirect enable	
Outside interfaces: fastethernet0	Exterior interface f0
Inside interfaces: serial2	Interior interface s2
Hits: 73 Misses: 7	
Expired translations: 3	
Dynamic mappings:	
-- Inside Source	
access-list 1 pool p1 refcount 2	
pool p1: netmask 255.255.255.248 start 128.255.251.83 end 128.255.251.86	The address pool uses the defined rules from access list 1.
type GENERIC, total addresses 4, allocated 1 misses 0	
flags: ipN_MAP ipN_OVERLOAD	
Fragment statistics: Totals: 0 Had-existeds: 0 No-memorys: 0	
Hits: 0 Expireds: 0 News: 0	
Ftp proxy session: Totals: 0 Hits: 0 No-memorys: 0	

The above displayed fields are described as follows:

Field	Description
Total translations	Shows the amount of active static translations and dynamic translations in the system.
Outside interface	Refers to the list marked as an outside interface.
Inside interface	Refers to the list marked as an inside interface.
Hits	Indicates the number of times the translation list had been examined and had its destination items found.
Misses	Indicates the number of times the translation list had been examined and didn't have its destination items found.
Expired translation	The expired translation that have happened since system startup.
Dynamic mappings	Indicates dynamic mapping information.
Inside Source	Indicates interior source address translation information.
access-list	Indicates the amount of times the access lists were used in translation.

pool	Indicates the address pool name used in translation.
Refcount	Pool reference times.
Netmask	The address pool's first IP address.
End	The address pool's final IP address.
Type	The type of address pool used: generic or rotary.
total addresses	The address pool's total address number.
allocated	The amount of allocated addresses in the pool.
misses	The number of times the missed packet didn't have an IP address.

You can display all NAT address pools with the privileged user command show ip nat pool.

router# show ip nat pool

Address pool : p1	
start : 128.255.251.83	
end : 128.255.251.86	
netmask : 255.255.255.248	
type : GENERIC	

To turn off the NAT redirect switch:

Command	Description
router(config)# no ip nat redirect	

The redirect switch is specially set by the NAT for OICQ applications, and users between the interior and exterior network won't be able to communicate with each other directly. The router's NAT provides the special switch function to establish direct communication between users, based on its application. The problem can be overcome, though, by transferring the OICQ server.

The default switch configuration will be set to ON. If you don't need this function, you can turn the switch off. You can open the switch again with the following command:

Command	Description
router(config)# ip nat redirect	

Command	Description
router#debug ip nat	To see all information of NAT
router#no debug ip nat	Close debug ip nat command

router#debug ip nat packets	Display information in detail of IP packets before and after translation
router#no debug ip nat packets	Close debug ip nat packet command

Considerations of Configuring NAT

The global addresses and the local addresses cannot be overlapped. The following three classes of local addresses are recommended:

Class	Description
Class A:10.0.0.0 / 8	One class A address.
Class B:172.16.0.0 / 12	16 class B addresses.
Class C:192.168.0.0 / 16	256 class C addresses.

The static addresses and the addresses in the dynamic address pool cannot be overlapped.

As a solution to connection, only when a small amount of hosts communicate with the external of the area, can NAT be practical. In this case, only a small sub-set of IP addresses in the area should be translated into unique IP addresses. And when these addresses are not applied any more, these addresses can be reused again.

When an IP address or a port is embedded into an application, NAT becomes non-transparent for end users. So, NAT can neither be applied to the case.

The router that has realize the technology cannot support IPsec because the end-to-end security cannot be ensured.

The route information can be broadcasted to the internal instead of the external

It is necessary to configure the static route between NAT and ISP routers.

IP OPTION cannot be supported normally.

When there exists multiple interfaces, the same NAT table should be adopted

Easy IP Configuration

Easy IP feature is to combine NAT and PPP/IPCP, and the router auto negotiates its WAN interface IP address from core server, to make all the remote hosts use this IP address, to visit global Internet.

The advantage of using Easy IP:

- reduce Internet access cost via dynamic distributing IP address;
- simplify router configuration and IP address management;
- distribute dynamic IP address to remote working station;
- remote LAN IP address encryption.

To make Easy IP work normally, configure static routing from LAN to WAN.

Easy IP Configuration

Task List

- Configure LAN interface
- Define NAT to LAN interface
- Configure WAN interface
- Define WAN interface to NAT

Easy IP Configuration Case

The following configuration command can make a number of interior network hosts use just one negotiated IP address to access the Internet.

Command	Task
router(config)# access-list 1 permit 192.168.12.0 0.0.0.255	Defines access list 1 and enables it to permit the addresses in the network segment to be translated.
router(config)# ip nat inside source list 1 interface serial0 overload	Builds the dynamic source address translation between list 1 and port s0.
router(config)# interface e0	Designated a LAN interface e0.
router(config-if-ethernet0)# ip address 192.168.12.1 255.255.255.0	
router(config-if-ethernet0)# ip nat inside	Defines the NAT for a LAN interface.
router(config-if-ethernet)# exit	
router(config)# interface s0	Designates the WAN interface s0.
router(config-if-serial0)# physical-layer async	
router(config-if-serial0)# speed 38400	
router(config-if-serial0)# flow-control hardware	
router(config-if-serial0)# encapsulation ppp	Encapsulates PPP.
router(config-if-serial0)# ip address negotiated	Starts PPP/IPCP address negotiation.
router(config-if-serial0)# ppp pap sent-username xxx password xxx	Starts PAP authentication.
router(config-if-serial0)# no keepalive	
router(config-if-serial0)# ip nat outside	Defines NAT for WAN interface.
router(config-if-serial0)# exit	
router(config)#	

NIA Configuration

Overview

Signamax NIA technology is a security control technology based on resource management.

Network Isolation Authorization Function

Signamax router network isolation authorization function divides a physical network into different service areas.

NIA Theory

The different access areas cannot communicate with each other, and each access area is a logical network.

Access area is based on interface. Network isolation realizes the filtering based on interface via distributing different accesses, to prevent pseudo source address attack.

Distribute the communicated interfaces as a same access area, to realize the isolation of different services.

NIA Commands

Command	Description	Config mode
nia ifgroup group-number interface interface-name1 interface-name2……	* network logical isolation command (distribute access area)	config
nia username user-name ifgroup group-number	* NIA user limitation	config
nia usergroup number user user-name1 user-name2…	* user and user group configuration	config
nia usergroup ug-number ifgroup ig-number	* NIA user group limitation	config

NIA Configuration Example

Network Logical Isolation

Command	Description
router(config)#nia ifgroup group-number interface interface-name1 interface-name2 interface-name3……	Group-number <1－8> interface-name interface name

group-number access area mark;

int-name1 int-name2… interface string, more than one

If the access area exists, add the interface to this access area; or, set up a new access area, and this area is consisted of subnet. Delete some connected subnets from designated access area:

```
no nia ifgroup group-num [ interface int1 int2…]
```

If the access area doesn't include the interface after this operation, delete the access area.

Once the router configures NIA, any interface (sub-interface) should belong to some access area, or the interface will become a logical network; the same interface may belongs to the different access areas.

Example one: (service isolation via sub-interface technology)

Seeing as the picture, MP2600 connects the other two routers via X.25 network, and S1/0.1 connects Router A,S1/0.2 connects Router B; requirement: this network is divided into two logical areas, and they will be isolated because of different services.

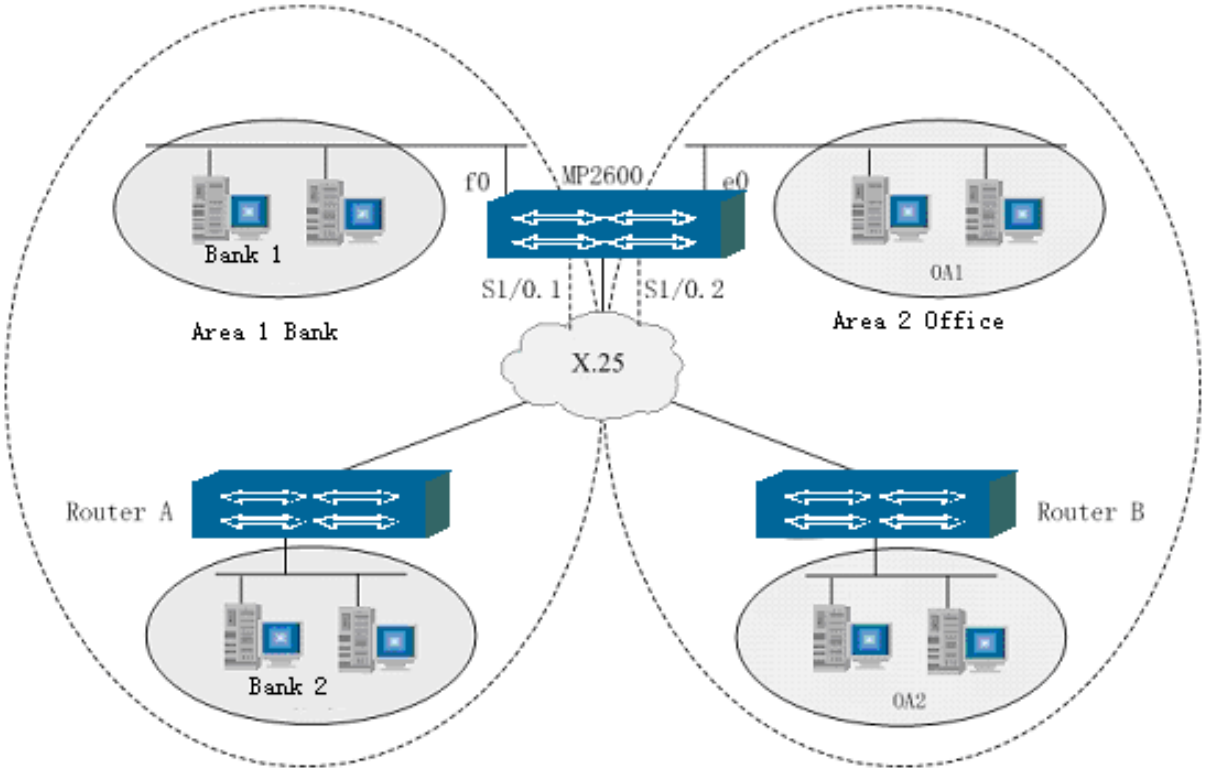


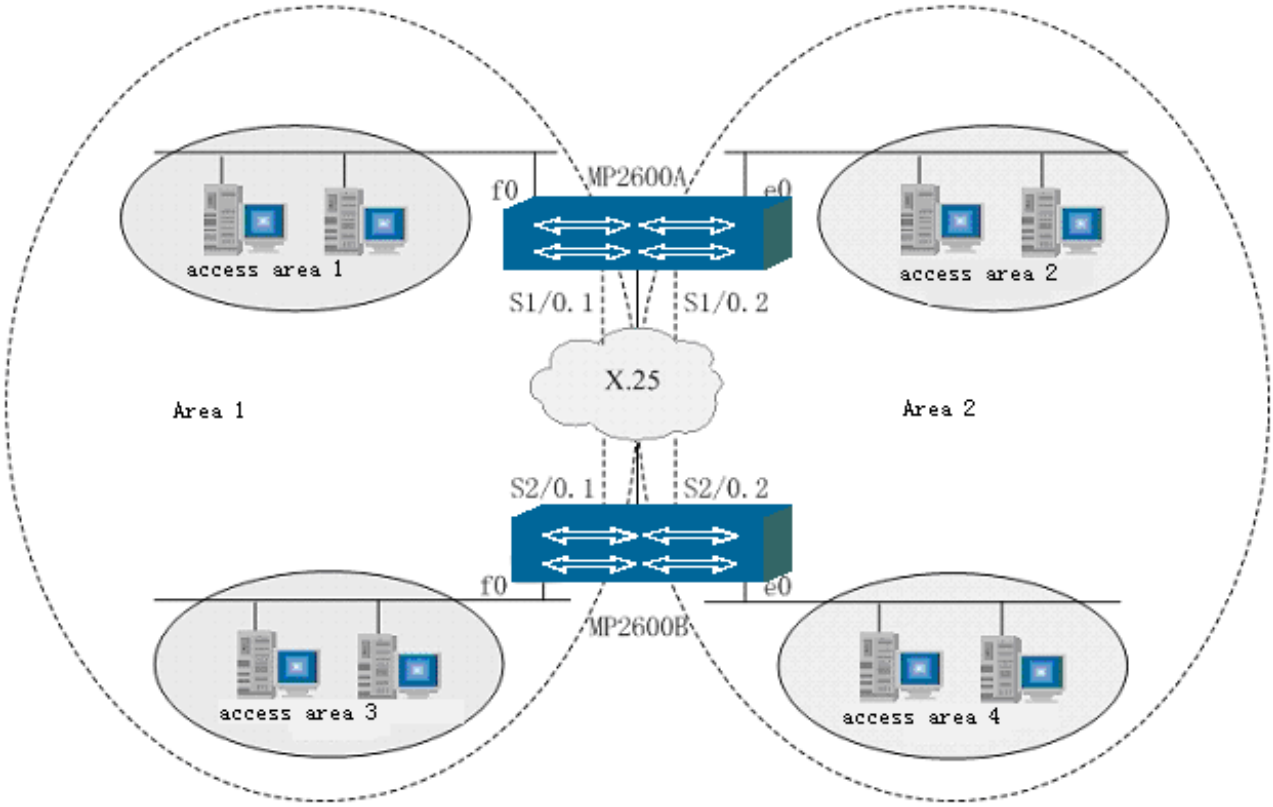
Figure 19-10

After configuring X.25, the subnet isolation function on MP2600 can satisfy:

```
mp2600(config)# nia ifgroup 1 interface fastethernet0 serial1/0.1
mp2600(config)# nia ifgroup 2 interface ethernet0 serial1/0.2
```

In this example, although the two different access areas use the physical interface s1/0, but because of the different service range of connected peer, please configure sub-interface on s1/0, to achieve the security.

Example two: (the service area will be isolated via remoter routers).
Seeing as the picture, the routers in two different areas are connected via x.25, and isolate it to two different access areas, and the two areas cannot be accessed to each other.



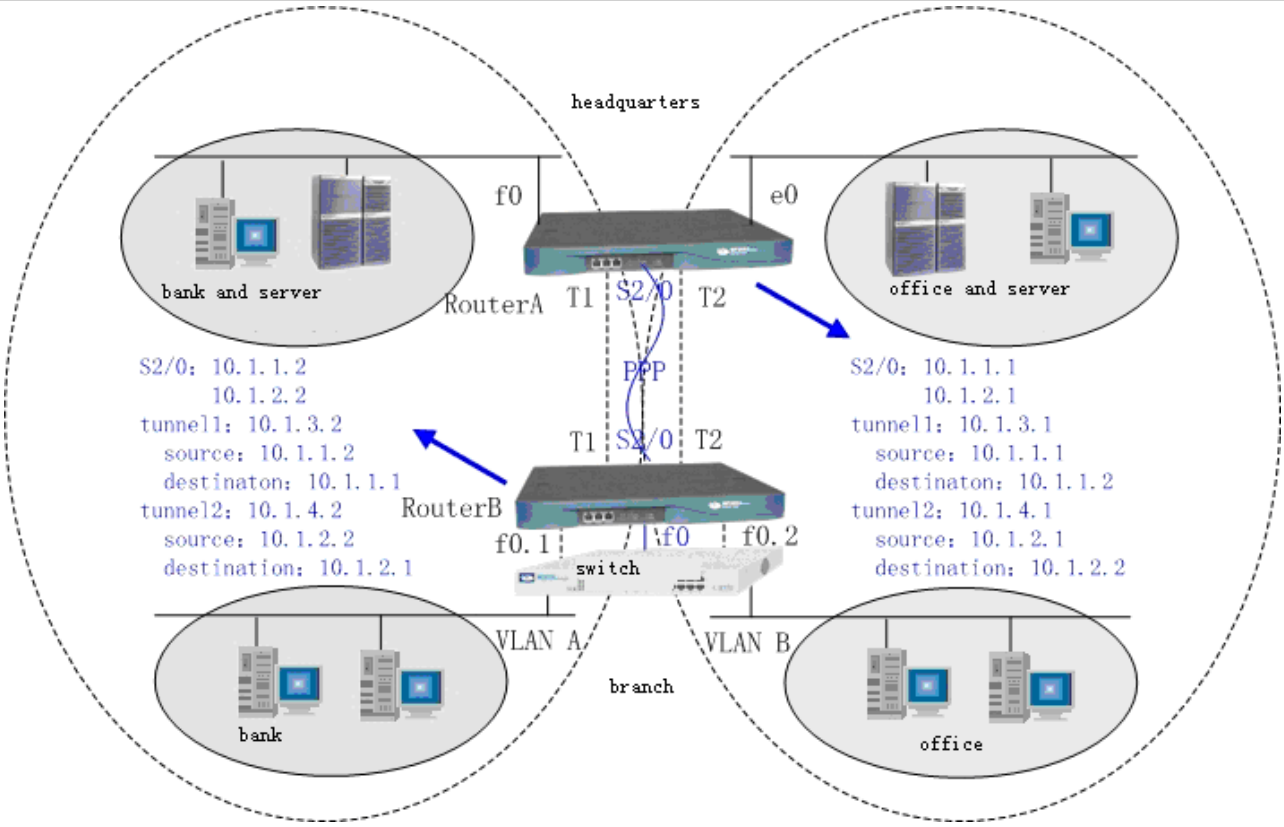
Step one: encapsulate and configure X.25 on the interfaces of the two routers;

On MP2600A:

```
mp2600A(config)#int s2/0
mp2600A(config-if-serial2/0)#enc x25
mp2600A(config-if-serial2/0)#x25 dce
mp2600A(config-if-serial2/0)#x25 addr 1110
mp2600A(config-if-serial2/0)#ip address 192.168.0.1
255.255.255.0
mp2600A(config-if-serial2/0)#exit
        /* encapsulate X.25 on S2, and designate X.25 address
and IP address*/
mp2600A(config)#int s2/0.1
mp2600A(config-if-serial2/0.1)#ip address 192.168.1.1
255.255.255.0
mp2600A(config-if-serial2/0.1)#x25 map ip 192.168.1.2 2220
mp2600A(config-if-serial2/0.1)#exit
        /* on sub-interface S2/0.1, designate IP address and
configure X25 MAP, and designate peer address */
mp2600A(config)#int s2/0.2
mp2600A(config-if-serial2/0.2)#ip address 192.168.2.1
255.255.255.0
```

```
mp2600A(config-if-serial2/0.2)#x25 map ip 192.168.2.2 2220

mp2600A(config-if-serial2/0.2)#exit

       /* on sub-interface S2/0.2, set IP address and
configure X25 MAP designated peer address */

On MP2600B:

mp2600B(config)#int s2/0

mp2600B(config-if-serial2/0)#enc x25

mp2600B(config-if-serial2/0)#x25 dte

mp2600B(config-if-serial2/0)#x25 addr 2220

mp2600B(config-if-serial2/0)#ip address 192.168.0.2
255.255.255.0

mp2600B(config-if-serial2/0)#exit

       /* encapsulate X.25 on S2/0, and set X.25 and IP
address */

mp2600B(config)#int s2/0.1

mp2600B(config-if-serial2/0.1)#ip address 192.168.1.2
255.255.255.0

mp2600B(config-if-serial2/0.1)#x25 map ip 192.168.1.1 1110

mp2600B(config-if-serial2/0.1)#exit

       /* on sub-interface S2/0.1, set IP address and
configure X25 MAP designated peer address */

mp2600B(config)#int s2/0.2

mp2600B(config-if-serial2/0.2)#ip address 192.168.2.2
255.255.255.0

mp2600B(config-if-serial2/0.2)#x25 map ip 192.168.2.1 1110

mp2600B(config-if-serial2/0.2)#exit

       /* on sub-interface S2/0.2, set IP address and
configure X.25 MAP, and designate peer address */

Step two: access area configuration.

mp2600A(config)# nia ifgroup 1 interface fastethernet0
serial2/0.1

mp2600A(config)# nia ifgroup 2 interface ethernet0
serial2/0.2

mp2600B(config)# nia ifgroup 3 interface fastethernet0
serial2/0.1

mp2600B(config)# nia ifgroup 4 interface ethernet0
serial2/0.2
```

Example three: (realize two networks service isolation via GRE technology)



Step one: configure GRE channel;

```
Router A:
        interface s2/0
        enc PPP
        clock rate 128000
        ip addr 10.1.1.1 255.255.255.252
        ip addr 10.1.2.1 255.255.255.252 sec

        interface tunnel1
        ip addr 10.1.3.1 255.255.255.252
        tunnel source 10.1.1.1
        tunnel destination 10.1.1.2

        interface tunnel2
        ip addr 10.1.4.1 255.255.255.252
        tunnel source 10.1.2.1
        tunnel destination 10.1.2.2
Router B:
        interface s2/0
        encapsulation PPP
```

```
      ip addr 10.1.1.2 255.255.255.252
      ip addr 10.1.2.2 255.255.255.252 sec

      interface tunnel1
      ip addr 10.1.3.2 255.255.255.252
      tunnel source 10.1.1.2
      tunnel destination 10.1.1.1

      interface tunnel2
      ip addr 10.1.4.2 255.255.255.252
      tunnel source 10.1.2.2
      tunnel destination 10.1.2.1
```

Step two:

```
Configure VLAN sub-interface on Router B:
interface fastethernet0.1
ip address 10.1.5.1 255.255.255.0
encapsulation dot1q 1
exit

interface fastethernet0.2
ip address 10.1.6.1 255.255.255.0
encapsulation dot1q 2
exit
Configure other interfaces on Router A:
      interface f0
      ip addr 10.1.7.1 255.255.255.0

      interface e0
      ip addr 10.1.8.1 255.255.255.0
Step three: Configure isolated access area on routers:
Router A:
      nia ifgroup 1 interface f0 tunnel1
      nia ifgroup 2 interface e0 tunnel2
Router B:
      nia ifgroup 1 interface tunnel1 f0.1
      nia ifgroup 2 interface tunnel2 f0.2
```

```
Step four: configure routing on routers (such as static routing).

Router A:

      ip route 10.1.5.0 255.255.255.0 10.1.3.2

      ip route 10.1.6.0 255.255.255.0 10.1.4.2

Router B:

      ip route 10.1.7.0 255.255.255.0 10.1.3.1

      ip route 10.1.8.0 255.255.255.0 10.1.4.1
```

In this way, the two logical areas have been isolated, and there is no need to use access list; but the user
right has not been limited, which means: if there is no authorization about NIA, all the users only need to log in a router to examine the configuration of the it; if it needs to add the limitation of the logical area for user authorization, add the binding between access area and user. The command is as following:

```
Router A:

      nia username user1 ifgroup 1

      nia username user2 ifgroup 2

Router B:

      nia username user1 ifgroup 1

      nia username user2 ifgroup 2
```

After above binding configuration, user1 only examines and operates the interface information and routing information with access area1; but user2 only examines and operates access area2; and so one router seems two logical routers.

NIA user limitation
Access area configuration controls the packet. Configure the binding between the user and access area to control the users.

Command	Description
router (config)# nia username user-name ifgroup group-number	Group-number <1—8> access area number user-name, configuring user access area.

When the user has binding relation with access area, the user is limited:

The user only can log in the router via the binding access area interface;

The user logged in this router only can access to other resource (other host, ping other address, or telnet to other machines) via binding access sub-interface;

The user logged in the router should have binding relation if it wants to use the resource to interface (displaying interface information, routing information and configuring interface).

The binding between user and access area only apply to router but not packet!

Example four:
There are three users: mary, stevens and eric; mary belongs to bank, stevens belongs to OA, and eric belongs to OA, but it is administrator, who can examine all the configuration information on router. And the binding configuration is as following:

```
mp2600(config)# nia username mary ifgroup 1
mp2600(config)# nia username stevens ifgroup 2
mp2600(config)# nia username eric ifgroup 1
mp2600(config)# nia username eric ifgroup 2
User and user group
```

The user with same attribute will be put into the same user group; and access area is distributed to user
group;

In order to manage, the same user cannot belong to different user group, but it can have other resource.

Add user in user group:

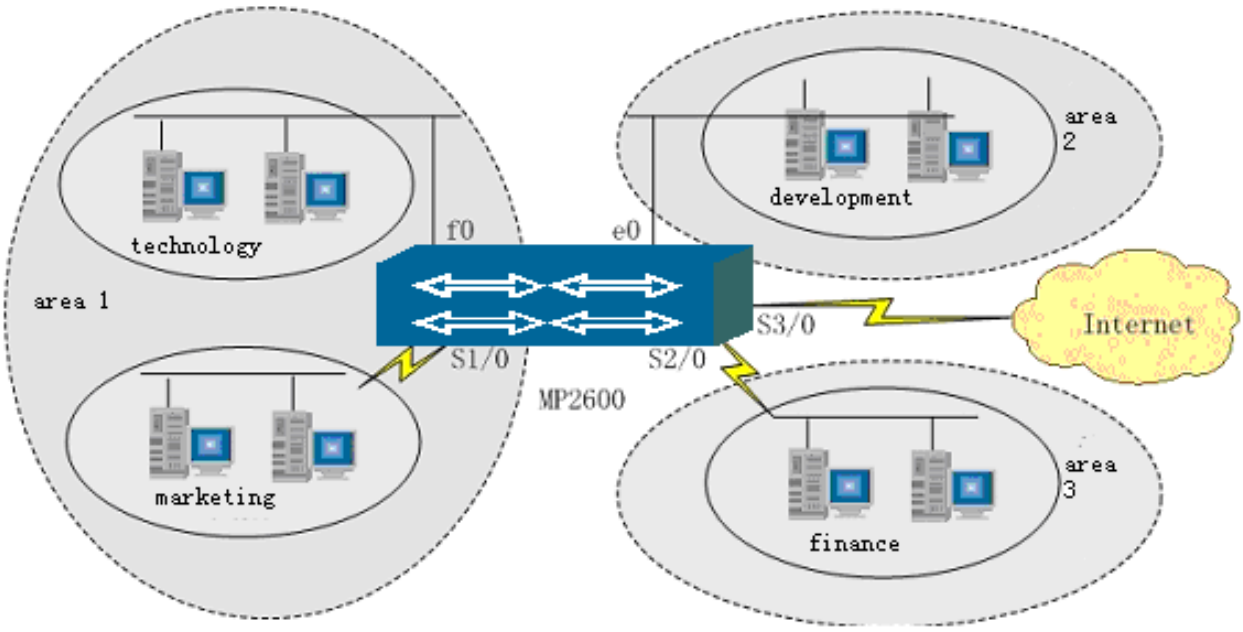
Command	Description
router (config)# nia usergroup number user user-name1 user-name2 user-name3…….	Number <1-8> user group number User-name user name

Binding between user group and access area:

Command	Description
router (config)# nia usergroup ug-number ifgroup ig-number	ug-number <1-100> user group number ug-number <1-100> access area number

Example five:
The network divides into four independent areas, and each department has:

```
Marketing department user: sc1 sc2
Development division user: kf1 kf2 mary
Technology supported department user: js1 js2 eric
Finance department user: cw1 cw2
Privileged user: eric mary
```



Requirement 1:
Each department isolates each other except marketing and technology departments; privileged user eric belongs to technology department, mary belongs to development division, but they have the configuration on router.

Configuration:

```
Step one: access area configuration
mp2600(config)#  nia  ifgroup  1  interface  fastethernet0
serial1/0
mp2600(config)# nia ifgroup 2 interface ethernet0
mp2600(config)# nia ifgroup 3 interface serial2/0
Step two: user group configuration and user adding
mp2600(config)# nia usergroup 1 user sc1 sc2
mp2600(config)# nia usergroup 2 user js1 js2 eric
mp2600(config)# nia usergroup 3 user kf1 kf2 mary
mp2600(config)# nia usergroup 4 user cw1 cw2
Step three: resource distribution
mp2600(config)# nia usergroup 1 ifgroup 1
mp2600(config)# nia usergroup 2 ifgroup 1
mp2600(config)# nia usergroup 3 ifgroup 2
mp2600(config)# nia usergroup 4 ifgroup 3
mp2600(config)# nia username eric ifgroup 2
mp2600(config)# nia username eric ifgroup 3
mp2600(config)# nia username mary ifgroup 1
```

```
mp2600(config)# nia username mary ifgroup 3
```

Requirement 2:
Other departments can examine internet information except finance department.
Configuration:

```
serial3/0 connecting to Internet adds to the  access area.
mp2600(config)# nia ifgroup 1 interface serial3/0
mp2600(config)# nia ifgroup 2 interface serial3/0
```

In this way, area 1 and area 2 users can connect Internet, but the packet from area 3 will be refused because serial2/0 and serial3/0 are not in the access area; and the packet on Internet will not reach area 3 via serial3/0; this kind of technology guarantees information security of some important departments.

NIA Displaying & Debug Details

NIA information displaying command:

Syntax	Description
router# show nia	**Display NIA configuration information;**

DEBUG information has three commands:

Command	Description
router# debug nia	**Display NIA packet information;**
router# no debug nia	**Close DEBUG switch;**
router# undebug nia	**Close DEBUG switch;**

Configure Virtual Private Dial-up Network (VPDN)

This section explains all commands that are necessary to configure virtual private dial-up network (VPDN). Virtual private dial-up network provides connection via ISP.

Global VPDN Configuration

```
Enable/Disable VPDN
```

To configure any VPDN, we should enable it . Only after VPDN is enabled, can some commands, which are used to configure LAC/LNS for L2TP dialin, be employed by users.

```
vpdn enable
```

It is very simple to enable VPDN. To enable VPDN, use the following global configuration command:

```
vpdn enable
```

(Configuration mode) Global configuration

```
no vpdn enable
```

Stop using VPDN. To disable VPDN, use the following global configuration command:
no vpdn enable
(Configuration mode) Global configuration

Create/ Delete a VPDN Group
The VPDN group is a mechanism, permitting us to organize all VPDN commands relative with devices (such as VPDN etc.) into an independent group. This mechanism can specify whether Signamax router is one of four L2TP (Layer 2 Tunneling Protocol, L2TP) devices (LAC (L2TP Access Concentrator, LAC) dialin, LAC dial-out, LNS (L2TP Network Server, LNS) accept-dialin and LNS accept-dial-out).

Once the VPDN group is configured as a L2TP device (LAC or LNS), then it can't be changed any longer. By means of utilizing multiple VPDN groups, we can make a router become a LAC or LNS.

vpdn-group
Employ the following configuration commands to create a VPDN group:

```
vpdn-group vpdn-group-number
```

Syntax	Description
vpdn-group-number	It is the name of the VPDN group, and its type is NUMBER.

(Configuration mode) Global configuration

```
no vpdn-group
```

Employ the following configuration commands to delete a specified VPDN group:

no vpdn-group vpdn-group-number

Syntax	Description
vpdn-group-number	It is the name of the VPDN group, and its type is NUMBER.

(Configuration mode) Global configuration

VPDN Configuration Keywords
The purpose of each keyword is to describe the activities executed by L2TP devices. When a user is performing the LAC dialin, LAC should request the dialin service from LNS and LNS need accept the dialin service. And when a user is performing the LNS dialout, LNS should

request the dialout service from LAC and LAC need accept the dialin service.
Multiple VPDN groups can be used to configure Signamax router so that it can serve as one of four devices (LAC dialin, LAC dialout, LNS accept-dialin and LNS accept-dial-out).

The following commands can be employed to specify which keyword each L2TP can use and enter related device configuration.

Syntax	Description
request-dialin	Configure VPDN request-dialin.
request-dialout	Configure VPDN request-dialout.
accept-dialin	Configure VPDN request-dialin group.
accept-dialout	Configure VPDN request-dialout group.

(Configuration mode) the VPDN group configuration mode

LAC request-dialin and LNS request-dialout have been realized.
l2tp tunnel authentication

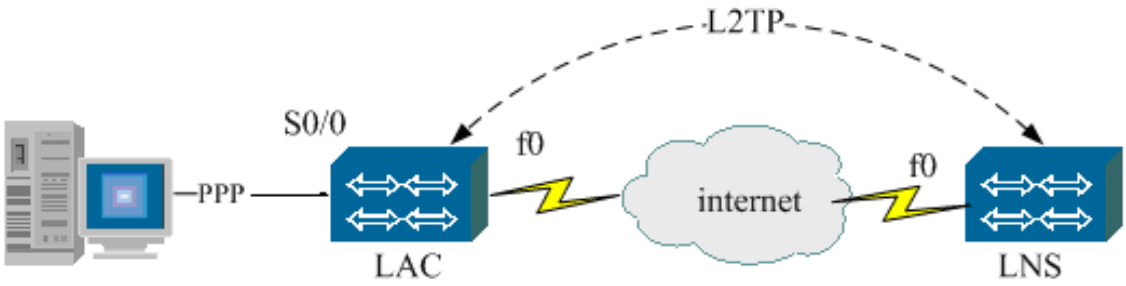
Enable this command to identify VPDN channel; and use no no l2tp tunnel authentication to cancel the authentication.

l2tp tunnel authentication
no l2tp tunnel authentication
(Default status) define
l2tp tunnel hello
Use this command to check VPDN channel connectivity; and use command no l2tp tunnel hello to cancel the command.
l2tp tunnel hello seconds
no l2tp tunnel hello seconds

Syntax	Description
seconds	VPDN channel keepalive sending time interval

(Default status) 60s

VPDN Configuration Example



Shown as the figure above, the PC dials in LAC via the remote dial-up, and the middle network is between LAC and LNS.

LAC is configured as follows:

Command	Description
Router(config)# vpdn enable	Enable VPDN.
router(config)# vpdn-group 1	Create a VPDN group
router(config-vpdn)#request-dialin	Permit the request-dialin of the VPDN group.
router(config-vpdn-req-in)# protocol l2tp	Specify the L2TP protocol for the VPDN group.
router(config-vpdn-req-in)#domain mp-2.com	Specify the domain name to relate a user with a VPDN group.
router(config-vpdn)#initiate-to ip 192.168.10.2	Specify the IP address of LNS.
router(config-vpdn)# local name r3	Specify the name for LAC to identify itself on LNS.
router(config-vpdn)# l2tp tunnel password 7 a	Specify the share password for identification.
router(config-if-serial0/0)#physical-layer sync	Configure the serial-port as the synchronous mode.
router(config-if-serial0/0)#encapsulation ppp	Encapsulate the protocol.
router(config-if-serial0/0)#ppp authentication pap	Configure the interface to employ the PAP authentication.
router(config-if-serial1/0)#physical-layer async	Configure the serial-port as the asynchronous mode.
router(config-if-serial1/0)#encapsulation ppp	Encapsulate the protocol.
router(config-if-serial1/0)#ip address 129.255.14.66 255.255.255.0	Configure the IP address and subnet mask of the interface s1/0.
router(config-if-serial1/0)#dialer in-band	Enable DDR on the interface.
router(config-if-serial1/0)#dialer-group 1	Configure the interface to be subject to some dialer-group.
router(config-if-serial1/0)# modem outer	Use the outer modem.

Configure on LNS as follows:

Command	Description
router(config)# vpdn enable	Enable VPDN.
router(config)# vpdn-group 2	Create a VPDN group.
router(config-vpdn)# accept-dialin	Permit the accept-dialin of the VPDN group.
router(config-vpdn-acc-in)# protocol l2tp	Specify the L2TP protocol in the VPDN group.
router(config-vpdn-acc-in)#virtual-template 1	Specify the virtual template interface.
router(config-vpdn)#terminate-from hostname r3	LAC provides the name of LNS.
router(config-vpdn)# local name r2	LNS provides its name to LAC.
router(config-vpdn)# l2tp tunnel password 7 a	Specify the share password for authentication.
router(config)#int virtual-template1	Create a virtual template interface.
router(config-if-virtual-template1)# encapsulation ppp	Encapsulate the protocol.
router(config-if-virtual-template1)# ppp authentication pap	Adopt the PAP as authentication protocol.
router(config-if-virtual-template1)#ip unnumber loopback1	Enable the IP un-number on the interface.
router(config-if-virtual-template1)# peer default ip address pool vpdn-pool	Specify the opposite-end IP address of the interface.
router(config)# user mp-5@mp-2.com password 0 a	Configure the username and password for the dialin user.
router(config)# ip local pool vpdn-pool 172.16.20.10 172.16.20.100	Configure the address pool.
router(config-if-loopback1)# ip address 172.16.20.1 255.255.255.0	Configure the IP address of L1.
router(config-if-serial2/0)#physical-layer sync	Configure the serial interface as synchronous mode.
router(config-if-serial2/0)#clock rate 9600	Configure the clock.
router(config-if-serial2/0)# encapsulation ppp	Encapsulate the protocol.
router(config-if-serial2/0)# ip address 192.168.10.2 255.255.255.0	Configure the IP address.

VPDN Monitoring & Debugging

```
show vpdn
```

Display the configuration of Tunnel.
(Command mode)the privilege user mode.

```
debug l2tp data
```

Trace information related with messages.

```
no debug l2tp data
```

(Command mode)the privilege user mode.

```
debug l2tp event
```

Trace the sending and receiving of messages.

```
no debug l2tp event
```

(Command mode)the privilege user mode.

```
debug l2tp detail
```

Trace the relative detail.

```
no debug l2tp detail
```

(Command mode)the privilege user mode.

Configure GRE

GRE(short for Generic Routing Encapsulation) can encapsulate the datagram of some network layer protocols (for example, IP) so that the encapsulated datagram can be transported over other network layer protocols (for example, IP). GRE adopts a tunnel technology between protocol layers. Tunnel is a virtual point-point interface that provides one channel over which the encapsulated datagram can be transported and encapsulates/decapsulates the datagram on both sides of the Tunnel interface.

Commands to Configure GRE

interface tunnel
Use the Description following command to create a virtual Tunnel interface and enter the tunnel configuration mode. The form no of the command is used to delete a specified tunnel.
interface tunnel tunnel-number
no interface tunnel tunnel-number

Syntax	Description
tunnel-number	Specify the tunnel-number, and its range is 0-65535.

(Default)No Tunnel interface is created.
(Command Mode)the Global configuration mode
tunnel checksum
Configure two sides of the tunnel to perform the checksum verification so as to check the correctness of messages. The form no of the command is used to disable the checksum checking of the Tunnel interface.
tunnel checksum
no tunnel checksum
(Default)Perform no checksum verification.
(Command)the Tunnel interface configuration mode.

Different verification can be configured on two sides of the Tunnel interface, which has no effect on its connectivity.

tunnel destination
Configure the IP address of the opposite end of the Tunnel interface. The form no of the command is used to delete the IP address of the opposite end of the Tunnel interface.

```
tunnel destination ip-address
```

```
no tunnel destination ip-address
```

Syntax	Description
ip-address	Specify that the opposite end employs the IP address of the factual physical port of the Tunnel interface.

(Default)Specify no IP address of the opposite end of the Tunnel interface.
(Command mode)the Tunnel interface configuration mode.

Ip-address should be consistent with the physical port of the opposite end and assure the port is reachable.

The destination address of local Tunnel interface should keep consistent with the source address of the opposite-end Tunnel interface.

tunnel key
Specify the identification key-number of the tunnel. And the form no of the command is used to cancel the identification key of the tunnel.

```
tunnel key key-number
```

```
no tunnel key key-number
```

Syntax	Description
key-number	Specify the identification key-number of the tunnel. And its value range is 0-4294967295.

(Default)Specify no identification key-number of the tunnel.
(Command mode)the Tunnel interface configuration mode.

Key-numbers of both sides of the tunnel should be consistent.
tunnel sequence-datagrams

Configure two sides of the tunnel to verify the sequence-number of datagrams. This configuration can be used to discard disordered datagrams. The form no of the command is employed to disable the verification of the sequence-number of datagrams.

tunnel sequence-datagrams
no tunnel sequence-datagrams
(Default)Don't verify the sequence-number of datagrams.
(Command Mode)the Tunnel interface configuration mode.

Different verification can be configured on the tunnel interface, without any effect on its connectivity.

tunnel source
Configure the local address of the tunnel interface. The form no of the command is used to delete the local port of the tunnel interface.。

```
tunnel source {ip-address|interface-name}
```

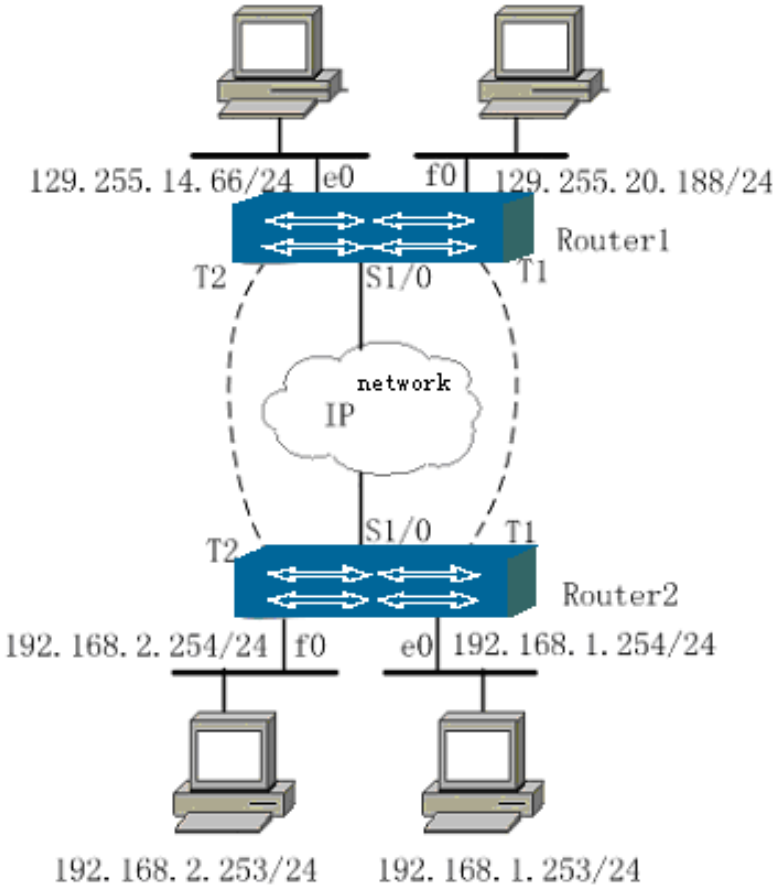
```
no tunnel source {ip-address|interface-name}
```

Syntax	Description
ip-address	Specify that the local end uses the IP address of the factual physical port of the tunnel interface.
interface-name	Specify that the local end uses the regular name of the factual physical port of the tunnel interface.

(Default)Specify no the local port of the tunnel interface.
(Command mode)the tunnel interface configuration mode.

GRE Configuration

The example is shown as the following figure:



Shown as the figure above, two tunnels are established between Router 1 and Router 2 via the IP network so that different services can use different logical channels.

Router1 is configured as follows:

Command	Description
router(config)# interface fastethernet0	Enter the configuration status of the port f0.
router(config-if-fastethernet0)#ip address 129.255.20.188 255.255.255.0	Configure the IP address of the subnet mask of the port f0.
router(config-if-ethernet0)#ip address 129.255.14.66 255.255.255.0	Configure the IP address of the subnet mask of the port e0.
router(config-if-serial1/0)#physical-layer sync	Configure the serial-port as the synchronous mode.
router(config-if-serial1/0)# clock rate 9600	
router(config-if-serial1/0)# encapsulation ppp	
router(config-if-serial1/0)# ip address 20.1.1.1 255.255.255.0	Configure the IP address of the subnet mask of the port s1/0.
router(config-if-serial1/0)# ip address 20.1.2.1	Distribute a secondary address

255.255.255.0 secondary	to the s1/0.
router(config-if-serial1/0)#intface tunnel1	
router(config-if-tunnel1)# ip address 1.1.1.1 255.255.255.0	Configure the IP address of the subnet mask of the tunnel1.
router(config-if-tunnel1)#tunnel source 20.1.1.1	The local end uses the IP address of the factual physical port of the tunnel interface.
router(config-if-tunnel1)#tunnel destination 30.1.1.2	The opposite end uses the IP address of the factual physical port of the tunnel interface.
router(config-if-tunnel1)#ip route peer-address 1.1.1.2	Specify the IP address of opposite end of the tunnel 1 in the dynamic route.
router(config-if-tunnel1)#intface tunnel2	
router(config-if-tunnel2)#ip address 2.1.1.1 255.255.255.0	Configure the IP address of the subnet mask of the port tunnel2.
router(config-if-tunnel2)# tunnel source 20.1.2.1	The local end uses the IP address of the factual physical port of the tunnel interface.
router(config-if-tunnel2)#tunnel destination 30.1.2.2	The opposite end uses the IP address of the factual physical port of the tunnel interface.
router(config-if-tunnel2)#ip route peer-address 2.1.1.2	Specify the IP address of opposite end of the tunnel 2 in the dynamic route.
router(config-ospf)#network 129.255.20.0 0.0.0.255 area 0	Configure the relative dynamic routing protocol.
router(config-ospf)#network 1.1.1.0 0.0.0.255 area 0	
router(config-ospf)#network 2.1.1.0 0.0.0.255 area 1	
router(config-ospf)#network 129.255.14.0 0.0.0.255 area 1	
router(config)# ip route 30.1.1.0 255.255.255.0 20.1.1.2	Configure the relative static routing protocol for the middle channel.
router(config)# ip route.30.1.2.0 255.255.255.0 20.1.2.2	

Route2 is configured as follows:

Command and Description	
router(config)# interface fastethernet0	Enter the configuration status of the port f0.
router(config-if-fastethernet0)#ip address 192.168.2.254 255.255.255.0	Configure the IP address of the subnet mask of the port f0.
router(config-if-ethernet0)#ip address 192.168.1.254 255.255.255.0	Configure the IP address of the subnet mask of the port e0.
router(config-if-serial1/0)# physical-layer sync	Configure the serial-port as the synchronous mode.
router(config-if-serial1/0)# clock rate 9600	Configure the clock
router(config-if-serial1/0)# encapsulation ppp	Encapsulate the protocol
router(config-if-serial1/0)# ip address 30.1.1.2 255.255.255.0	Configure the IP address of the subnet mask of the port s1/0.
router(config-if-serial1/0)# ip address 30.1.2.2 255.255.255.0 secondary	Distribute a secondary address to the s1/0.
router(config-if-serial1/0)#intface tunnel1	
router(config-if-tunnel1)# ip address 1.1.1.2 255.255.255.0	Configure the IP address of the subnet mask of the tunnel1.
router(config-if-tunnel1)#tunnel source 30.1.1.2	The local end uses the IP address of the factual physical port of the tunnel interface.
router(config-if-tunnel1)#tunnel destination 20.1.1.1	The opposite end uses the IP address of the factual physical port of the tunnel interface.
router(config-if-tunnel1)#ip route peer-address 1.1.1.1	Specify the IP address of opposite end of the tunnel 1 in the dynamic route.
router(config-if-tunnel1)#intface tunnel2	
router(config-if-tunnel2)#ip address 2.1.1.2 255.255.255.0	Configure the IP address of the subnet mask of the port tunnel2.
router(config-if-tunnel2)#tunnel source 30.1.2.2	The local end uses the IP address of the factual physical port of the tunnel interface.
router(config-if-tunnel2)#tunnel destination 20.1.2.1	The opposite-end uses the IP address of the factual physical port of the tunnel interface.
router(config-if-tunnel2)#ip route peer-address 2.1.1.1	Specify the IP address of opposite end of the tunnel 2 in the dynamic route.
router(config-ospf)#network 192.168.1.0 0.0.0.255 area 0	Configure the relative dynamic routing protocol.
router(config-ospf)#network 1.1.1.0 0.0.0.255 area 0	
router(config-ospf)# network 2.1.1.0 0.0.0.255 area 1	
router(config-ospf)# network 192.168.2.0 0.0.0.255 area 1	
router(config)#ip route 20.1.1.0 255.255.255.0 30.1.1.1 .	Configure the relative staticroute of the middle physical line
router(config)# ip route 20.1.2.0 255.255.255.0 30.1.2.1	

This is an application of the network isolation. And usually, it can work in with NIA/URA to realize the isolation of user authentication.

GRE Checking & Debugging

`show gre config`

display all GRE Tunnel interfaces condition.

`show gre config`

(command mode)privileged user mode

`show gre statistics`

display gre statistics data.

`show gre statistics`

(command mode)privileged user mode

`debug gre`

Enable gre debugging information switch. And the command no is used to disable gre debugging function.

`debug gre`

`no debug gre`

(command mode) privileged user mode

AAA Configuration

This chapter explains how to configure AAA (Authentication, Authorization and Accounting) on the router. AAA is the abbreviation of Authentication, Authorization and Accounting. As a client program that runs on the network access server (NAS), it provides a consistent framework for you to configure the three security functions, Authentication, Authorization and Accounting.

AAA Configuration Commands

Command	Description	Config mode
aaa new-model	*enable AAA	config
aaa authentication banner	*configure AAA authentication banner	config
aaa authentication fail-message	*configure AAA authentication fail message	config
aaa authentication username-prompt	Configure AAA authenticaitn user name prompt	config
aaa authentication password-prompt	Configure AAA authentication password prompt	config
aaa authentication login	*configure AAA authentication login	config
aaa authentication enable default	*configure authentication enabling default	config
aaa authentication ppp	*configure PPP negotiation authentication	config
aaa authorization	*configure AAA authorization	config
aaa authorization commands	Configure AAA authorization commands	config
aaa accounting	*configure AAA accounting (statistics)	config
aaa accounting commands	Configure AAA accounting commands	config
aaa accounting suppress null-username	Configure AAA accounting user name as null or not	config
aaa accounting update	Configure AAA accounting update or not	config
tacacs-server host	*configure TACACS server address	config
tacacs-server key	Configure TACACS service key	config
tacacs-server timeout	Configure TACACS communication timeout	config
aaa group server tacacs	Configure TACACS server group	config

server	Configure TACACS server member	config-sg-tacacs
radius-server host	*configure RADIUS server address	config
radius-server dead-time	Configure RADIUS server dead time	config
radius-server key	*configure RADIUS server key	config
radius-server timeout	Configure RADIUS server timeout	config
radius-server retransmit	Configure RADIUS server retransmitting times	config
ip {tacacs|radius} source-interface	Configure TACACS and RADIUS NAS server source address	config

Command with AAA

`aaa new-mode`

This command is used to enable AAA on the router. The form no of the command is used to close AAA function.

aaa new-model
no aaa new-model
(Default)Disable AAA.
(Command mode)The global configuration mode.

`aaa authentication banner`

This command is used to modify the displayed welcome information when you login on a router. The form no of the command is used to reset the default welcome information.

`aaa authentication banner banner`

`no aaa authentication banner`

Syntax	Description
banner	This is the welcome information displayed on the screen when you log in the router.

(Default)The default welcome information is "User Access Verification".
(Command mode)The global configuration mode.

`aaa authentication fail-message`

This command is used to modify the caution information when you fail to login on the router. The form no of the command is used to reset the default caution information.

aaa authentication fail-message fail-message
no aaa authentication fail-message

Syntax	Description

fail-message	This is the caution information when you fail to login on the router.

(Default)The default caution information is "Access denied!".
(Command mode)The global configuration mode.

```
aaa authentication username-prompt
```

This command is used to modify the displayed text that is used to prompt you to input user name. The form no of this command is used to reset the default-displayed text.

aaa authentication username-prompt username-prompt

```
no aaa authentication username-prompt
```

Syntax	Description
username-prompt	The displayed text when you are cautioned to input your user name.

(Default)The default displayed text is "login:".
(Command mode)The global configuration mode.

```
aaa authentication password-prompt
```

This command is used to modify the displayed text when you are cautioned to input your passport. The form no of this command is used to reset the default-displayed text.

aaa authentication password-prompt password-prompt
no aaa authentication password-prompt

Syntax	Description
password-prompt	The displayed text when you are cautioned to input your passport.

(Default)The default displayed text is "passport:".
(Command mode)The global configuration mode.

```
aaa authentication login
```

This command is used to configure the login identity authentication method list. The form no of this command is used to delete the method list.

```
aaa authentication login {default|list-name} method1[method2…]
```

```
no aaa authentication login {default|list-name}
```

Syntax	Description
default	Define the default method list.
list-name	This is the method list name.
method	Authentication methods: None: Pass directly without authenticating the identity,. Enable: Use the valid passport to authenticate the identity (the global enable passport).

	Local: Use the local user database to authenticate the identity. Line: Use the line passport to authenticate the identity. Radius: Use RADIUS to authenticate the identity. Tacacs: Use TACACS to authenticate the identity.

(Default)No authentication method list is defined.
(Command mode)The global configuration mode.

Cooperating with the command login authentication in line mode, the method list can be used to authenticate the login identities for some lines. The default method list applies to all the interfaces and lines (except the interfaces or lines that are defined explicitly and referred to) automatically.

`aaa authentication enable`

This command is used to configure the identity authentication method list for you to enter the privilege user mode. The form no of this command is used to deletes the method list.

`aaa authentication enable default method1[method2…]`

`no aaa authentication enable default`

Syntax	Description
default	Define the default method list.
method	Authentication methods: None: Pass directly without authenticating the identity, Enable: Use the valid passport to authenticate the identity (the user enable passport or the global enable passport). Line: Use the line passport to authenticate the identity. Radius: Use RADIUS to authenticate the identity. Tacacs:Use TACACS to authenticate the identity.

(Default)No authentication method list is defined.
(Command mode)The global configuration mode.

When using the radius authentication method, you should use the passport of the user $enab15$ (need to be set on the radius server) as the authentication passport.

`aaa authentication ppp`

This command is used to configure a PPP identity authentication method list. The form no of this command is used to delete the method list.

`aaa authentication ppp list-name method1[method2…]`

`no aaa authentication ppp list-name`

Syntax	Description
list-name	This is the method list name.
method	Authentication methods: None: Pass directly without authenticating the identity. Local: Use the local user database to authenticate the identity. Radius: Use RADIUS to authenticate the identity. Tacacs: Use TACACS to authenticate the identity.

(Default)No authentication method list is defined.

(Command mode)The global configuration mode.
(Usage specification)This method needs to cooperate with the command ppp authentication to apply the method list to the PPP authentication of an interface.

aaa authorization

This command is used to limit the user access authorization. The form no of the command is used to allow the access authorization.

aaa authorization {exec|network} {default|list-name} method1[method2…]

no aaa authorization {exec|network} {default|list-name}

Syntax	Description
exec	Configure the EXEC authorization command method list.
network	Configure the authorization method list of the network service.
default	Define a default method list.
list-name	This is the method list name.
method	Authorization methods: if-authenticated： If a user passes the identity authentication, then he is authorized to access the request function. Local: Use the local database to authorize. None: Operate no authorization. Radius: Request the authorization information from RADIUS server. Tacacs: Request the authorization information from TACACS server.

(Default)No access authorization is limited (being equivalent to the keyword none).
(Command mode)The global configuration mode.

When the EXEC authorization method list has been configured and you execute EXEC, NAS can implement the authentication to you to determine whether you have the authorization to execute the EXEC shell program; if NAS fails to authorize, then you can't execute EXEC.

EXEC supports the authorization of Vendor-specific AV of ciscoSecureACS radius (Cisco), and AV is defined as follows:

Define autocmd—auto-command, value is the command string, and its format is:

autocmd=STRING

Define nohangup—whether the connection is broken after the system executes the auto-command, and its format is:

nohangup=FALSE/TRUE or 0/1

Define priv-lvl—the right level authorized to the login user, the range of value is from 0 to 15, and its format is:

priv-lvl=NUM

Define timeout—the entire connection time authorized to the login user, value is a number (by second), and its format is:

timeout=NUM

- **aaa authorization commands**

limit user operating command Shell. And command no is used not to limit the access authorization.

aaa authorization config-commands

no aaa authorization config-commands

aaa authorization commands cmd-lvl {default | list-name} method1[method2…]

no aaa authorization commands cmd-lvl {default | list-name}

Syntax	Description
config-commands	Configure AAA permitting authorization command.
cmd-lvl	Authorization command level, and the range is <0-15>
default	Define default method list
list-name	Method list name
method	Authorization method if-authenticated :if passed id authentication, the user can access. local: use local data base to authorize. none: not execute authorization operation. radius:ask for authorization information from RADIUS server. tacacs: ask for authorization information from TACACS server. WORD:use TACACS server group for authorization, WORD is server group name

(Default status)not limit access authorization (none)
(command mode)global configuration mode

aaa accounting

This command is used to configure the AAA accounting method list. The form no of this command is used to cancel the method list.

aaa accounting {connection|exec|network} {default|list-name} {none|start-stop| stop-only| wait-start} method1[method2]

no aaa accounting {connection|exec|network} list-name

Syntax	Description
connection	Configure the accounting command that the user uses when he logins to other routers via telnet or rlogin.
exec	Configure the accounting command of enabling the EXEC session.
network	Configure all accounting commands of the service requests that are with the network.
default	Define a default method list.
list-name	This is the method list name.
none	Don't process accounting.
start-stop	Send a start-accounting notice when a process starts, and send an end-accounting notice when the process ends. Whether or not the server receives the start-accounting notice, all requested user processes will start to execute.
stop-only	Send an end-accounting notice when the requested user process ends.
wait-start	Send a start-accounting notice and an end-accounting notice to the AAA accounting server. The requested user service isn't enabled until the notices above are acknowledged.
method	Accounting methods: Radius: send the accounting information to the RADIUS server. Tacacs: send the accounting information to the TACACS server.

(Default)No accounting method list is defined.
(Command mode)The global configuration mode.

To execute the accounting work as little as possible, you can use the keyword stop-only to send a stop-record-accounting notice when a requested user process ends.

To get more accounting information, you can use the keyword start-stop. In this way, RADIUS or TACACS can send a start-accounting notice when the requested process starts, and can send an end-accounting notice when the process ends.

To obtain more control right to the accounting you can use wait-start, which ensures that the process request of the user can't be authorized until the RADIUS or TACACS server receives the start-accounting notice.

- **aaa accounting commands**

configure AAA statistics method list. And command no is used to cancel the list.

```
aaa accounting commands cmd-lvl {default | list-name} {none | start-stop} [broadcast] method1[method2…]
```

```
no aaa accounting commands cmd-lvl {default | list-name}
```

Syntax	Description
commands	The statistics of executed commands.
cmd-lvl	Command level, and the range is <0-15>
broadcast	If broadcast has configured many statistics methods, send these information to the server.
default	Define default method list.
list-name	Method list name.
none	No statistics.
start-stop	Start statistics when receiving the stating message, and end the statistics when receiving the ending message.
stop-only	Send ending statistics message when the process is finished.
wait-start	Send starting and ending statistics information to statistics server.
Method	Statistic method. tacacs: send statistic information to TACACS server WORD:use TACACS server for authorization, WORD is server group name

(Default status)no definition of statistics method list
(command mode)global configuration mode

```
aaa accounting suppress null-username
```

This command is used to forbid creating a accounting record for the user whose user name is null. The form no of this command is used to allow creating a accounting record for the user whose user name is null.

```
aaa accounting suppress null-username
```

```
no aaa accounting suppress null-username
```

(Default)Allow to create a accounting record for the user whose user name is null.
(Command mode)The global configuration mode.

```
aaa accounting update
```

This command is used to send temporary accounting records to the server. The form no of this command is used to cancel to send temporary accounting record.

```
aaa accounting update {newinfo|periodic number}
```

```
no aaa accounting update
```

Syntax	Description
newinfo	Send temporary accounting records to the server every time there is new accounting information.
periodic	Send temporary accounting records periodically.
number	The interval period.

(Default)No temporary accounting record is sent.
(Command mode)The global configuration mode.

```
tacacs-server host
```

This command is used to configure the Tacacs server. The form no of this command is used to delete the Tacacs server.

```
tacacs-server host address [key key] [port port] [timeout timeout]
```

```
no tacacs-server host address
```

Syntax	Description
address	The address of the Tacacs server.
key	The key that is used for the communication between the router and the Tacacs server.
port	The TCP port number that is used to connect with the Tacacs background program.
timeout	Set the interval timer for waiting the response from the Tacacs server.

(Default)The port number is 49, and the timeout is 5 seconds.
(Command mode)The global configuration mode.

The key configured on the router should be consistent with that on the Tacacs server.

Multiple Tacacs servers can be configured, and the system can select one of them for system authentication according to the configuration sequence; when some server is unavailable, the system can select the next one automatically till the last one fails.

tacacs-server key

This command is used to configure the encryption key of the Tacacs. The form no of this command is used to delete the key.

```
tacacs-server key key
```

```
no tacacs-server key
```

(Default)There is no encryption key.
(Command mode)The global configuration mode.

```
tacacs-server timeout
```

The command is used to configure the interval timer for waiting the Tacacs server response. The form no of this command is used to reset the default value.

```
tacacs-server timeout timeout
```

```
no tacacs-server timeout
```

(Default)5 seconds.
(Command mode)The global configuration mode.

```
radius-server host
```

This command is used to configure the RADIUS server. The form no of this command is used to delete the RADIUS server.

```
radius-server host address [acc-port acc-port] [auth-port auth-port]
```

```
no radius-server host address
```

Syntax	Description
address	The address of the RADIUS server.
acc-port	The UDP destination port that is specified for the authentication request.
auth-port	The UDP destination port that is specified for the accounting request.

(Default) acc-port is 1645, and auth-port is 1646.
(Command mode)The global configuration mode.

The key configured on the router should be consonant with that on the RADIUS server.

Multiple RADIUS servers can be configured, and the system can select one of them for system authentication according to the configuration sequence; when some server is unavailable, the system can select the next one automatically till the last one fails.

`radius-server dead-time`

This command is used to configure dead-time. The form no of this command is used to set dead-time to be 0.

`radius-server dead-time dead-time`

`no radius-server dead-time`

Syntax	Description
dead-time	This is the time length. During the time, no request is sent to the RADIUS server

(Default) dead-time is set to be 0.
(Command mode)The global configuration mode.
(Usage guide)After the command is used, the system labels the RADIUS severs that don't respond to the authentication requests as unusable, and don't send requests to these servers during the dead-time period of time.

`radius-server key`

This command is used to configure the RADIUS encryption key. The form no of this command is used to delete the RADIUS encryption key.

`radius-server key key`

`no radius-server key`

(Default)There is no encryption key.
(Command mode)The global configuration mode.

`radius-server timeout`

This command is used to configure the interval timer for waiting the response from RADIUS server. The form no of this command is used to reset the default value.

```
radius-server timeout timeout

no radius-server timeout
```

(Default)5 seconds.
(Command mode)The global configuration mode.

- **aaa group server tacacs** *grp-name*

configure Tacacs server group. Command no is used to delete server group.

```
aaa group server tacacs grp-name

no aaa group server tacacs grp-name
```

Syntax	Description
grp-name	Tacacs server group name

(Default status)none.
(command mode)global configuration mode

- **server**

configure Tacacs server group member, command no is used to delete the command.

```
server ip-address

no server ip-address
```

Syntax	Description
ip-address	Tacacs server address. This address should be configured by tacacs-server.

(Default status)none
(command mode)server group configuration mode.

```
radius-server retransmit
```

This command is used to configure the maximum times of retransmitting a packet to the RADIUS server. The form no of this command is used to reset the default value.

```
radius-server retransmit retries

no radius-server timeout
```

Syntax	Description
retries	The maximum times of retransmitting a packet.

(Default)3 times.
(Command mode)The global configuration mode.

```
ip {tacacs|radius} source-interface
```

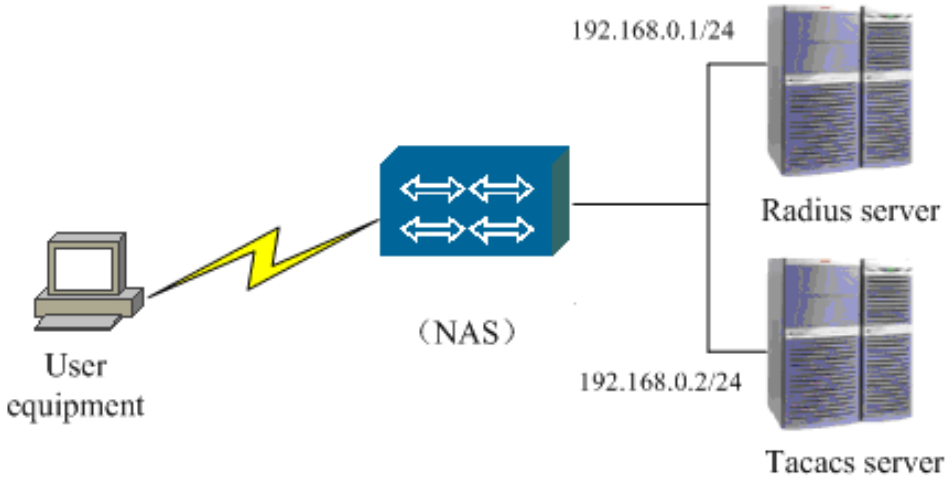
This command is used to configure the interface address, which is specified for the router to switch packets with the RADIUS or TACACS server. The form no of this command is used to reset the default value.

```
ip {tacacs|radius} source-interface interface-name
no ip {tacacs|radius} source-interface
```

Syntax	Description
interface-name	The interface name.

(Default) Use the address of the interface.
(Command mode)The global configuration mode.

AAA Configuration Example



In the configuration above, the PPP protocol is encapsulated between the user devices and the network access server (NAS), and login authentication uses the default method list.

The NAS configurations are as follows:

Command	Task
NAS#configure terminal	Enter the configuration mode.
NAS (config)# aaa new-model	Enable AAA authentication.
NAS (config)# aaa authentication banner ^ Welcome ^	Configure the welcome words for a use to login.
NAS (config)# aaa authentication fail-message ^ Sorry, Don't come in ^	Configure the prompt information for a user to fail to login.
NAS (config)# aaa authentication login default radius tacacs none	The authentication methods (radius, tacacs and none) are adopted for identification authentication of the telnet or rlogin user. (One or more authentication

	methods can be selected.)
NAS (config)# aaa authentication enable default radius enable	The authentication method radius enable is adopted for the telnet or rlogin user to enter the privilege use mode.
NAS (config)# aaa authentication ppp auth-name radius tacacs local	Configure the PPP authentication, and cooperate with the command ppp authentication on the interface s1/0.
NAS (config)# aaa authorization exec default radius	Configure that only users who are added into the RADIUS server can be authorized to execute the EXEC shell program; if the authorization fails, then the users cannot execute EXEC.
NAS (config)# aaa accounting exec default stop-only radius	Enable the accounting command of the exec session, and a stop-accounting notice is sent to the RADIUS server when the requested user process ends.
NAS (config)# aaa accounting connection default stop-only radius	Enable the accounting command connection, and implement the accounting when NAS logins on other router via telnet or rlogin.
NAS (config)# aaa accounting network list stop-only radius	Enable the accounting command (list) that the PPP service requests. (Because the PPP protocol is encapsulated between the user devices and the NAS.)
NAS (config)# radius-server host 192.168.0.1	Configure the address of the RADIUS server.
NAS (config)# radius-server key signamax	Configure the key of the RADIUS server, and the key should be the same as that of the NAS server on the RADIUS server.
NAS (config)# tacacs-server host 192.168.0.2 key mp	Configure the address and key of the TACACS server, and the key should be the same as that of the NAS server on the RADIUS server.
NAS (config)#interface s1/0	Enter the interface mode.
NAS(config-if-serial1/0)#ppp accounting list	Enable the PPP authentication accounting on the interface. Its name is list, which is the same as that following aaa accounting network.

Please implement the configuration strictly according to the Configuration Manual.

During the course of adopting the configured method list to authenticate a user, only when the previous method doesn't response can the router try the next method. If the identity authentication fails at any point of the period, namely, the security server or the local user name database response in the form of denying the user to access, then the identity authentication process will end and no other identity authentication method will be tried.

Checking & Debugging AAA

show aaa

Display AAA information

```
show aaa [configure | module | server | session | source-address]
```

Syntax	Description
configure	Display AAA configuration information
module	Display AAA functional module, and the result. These modules including: Shell:user interface module PPP:point to point module commands:command authorization, statistics module. system:system event module etc.
server	Display AAA using server information, including Tacacs and Radius
session	AAA accounting dialogue ID,recording AAA statistics dialog and information.
source-address	Display AAA using source address

(command mode)privileged user mode.

```
show accounting
```

This command is used to display the AAA accounting information.

show accounting

(Command mode)The privilege user mode.

```
debug aaa authentication
```

This command is used to open the switch of AAA authentication debugging information. The form no of this command is used to close the switch.

```
debug aaa authentication
```

```
no debug aaa authentication
```

(Command mode)The privilege user mode.

```
debug aaa authorization
```

This command is used to open the switch of AAA authorization debugging information. The form no of this command is used to close the switch.

```
debug aaa authorization
```

```
no debug aaa authorization
```

(Command mode)The privilege user mode.

```
debug aaa accounting
```

This command is used to open the switch of AAA accounting debugging information. The form no of this command is used to close the switch.

```
debug aaa accounting
```

```
no debug aaa accounting
```

(Command mode)The privilege user mode.

- **debug aaa all**

Enable AAA all debugging information switch. And command no is used to disable all the switches.

```
debug aaa all
```

```
no debug aaa all
```

(command mode)privileged user mode.

```
debug tacacs
```

This command is used to open the switch of TACACS debugging information. The form no of this command is used to close the switch.

```
debug tacacs
```

```
no debug tacacs
```

(Command mode)The privilege user mode.

```
debug radius
```

This command is used to open the switch for RADIUS debugging information. The form no of this command is used to close the switch of RADIUS debugging information.

```
debug radius [in-plain]
```

```
no debug radius
```

Syntax	Description
in-plain	Display the RADIUS packet information in the form of plaintext.

(Command mode)The privilege user mode.

DHCP Configuration

When a network is too large to manage directly by its builder, it is hard to manage the network. The frequent problem in the network where IP addresses are assigned manually is IP address conflict. The only method to resolve the problem is to assign IP addresses to clients dynamically.

Dynamic Host Configuration Protocol (DHCP) assigns an address from an address pool to the host that requests an address. DHCP also provides other information, such as gateway IP and DNS server. The purpose of designing DHCP is not to provide the diskless workstation with boot information, but to reduce burden of assigning IP addresses manually for a manager. DHCP can accomplish the work of assigning addresses.

DHCP Configuration Commands

Command	Description	Config mode
ip dhcp pool	*configure DHCP address pool	config
ip dhcp excluded-address	*exclude DHCP some addresses in address pool	config
ip dhcp-server	*configure DHCP relay address	config
ip dhcp ping	Configure DHCP ping detecting parameters	config
network	Configure DHCP address range network segment	config
range	*configure DHCP address range IP segment	dhcp-config
host	Configure DHCP address range host	dhcp-config
hardware-address	Configure DHCP host address pool Client hardware address	dhcp-config
client-identifier	Configure DHCP host address pool Client ID	dhcp-config
server-identifier	Configure DHCP server ID	dhcp-config
ip address dhcp	*Configure DHCP client end	config-if-××

Commands

The following table explains commands of DHCP server, relay and client.

Command	Description
In global configuration mode:	
router(config)#ip dhcp excluded-address	Remove addresses from the address pool.
router(config)#ip dhcp ping	Use the parameter ping.
router(config)#ip dhcp pool	Define an address pool for assigning addresses.
router(config)#ip dhcp-server A.B.C.D	Act as dhcp relay by appointing a dhcp server
Create an HDCP:	
router(config)#ip dhcp pool word	Define an address pool and enter DHCP configuration mode. The name of the address pool is the value of word.
In DHCP configuration mode:	
router(dhcp-config)# default-router	Configure the default gateway of the host.
router(dhcp-config)# dns-server	Configure DNS server address of the host.
router(dhcp-config)# domain-name	Configure the server name of the host.
router(dhcp-config)# netbios-name-server	Configure the address of the server netbios-name.
router(dhcp-config)# network	Define the address assigned in the address pool.
router(dhcp-config)#exit	Exit the interface mode.
In INTERFACE configuration mode:	
router(config-if-fastethernet0)#ip address dhcp	Act as dhcp client by requesting a address from some DHCP server

The first step: Define an address pool applied

The first step to star DHCP service is to define an address pool. The addresses in the address pool will be assigned dynamically to these hosts that use DHCP to request addresses. The following configuration commands should be used on the router:

Command	Description
router(config)#ip dhcp pool word	Define an address pool with the name of word.
router(dhcp-config)#network A.B.C.D netmask	Define an address pool for address assignment. And A.B.C.D are network ID and netmask is the network mask.
router(config)#ip dhcp excluded-address low ip address [high ip address]	Remove the low ip address and high ip address from the address pool. Low ip address is the starting address and high ip address is the ending address.

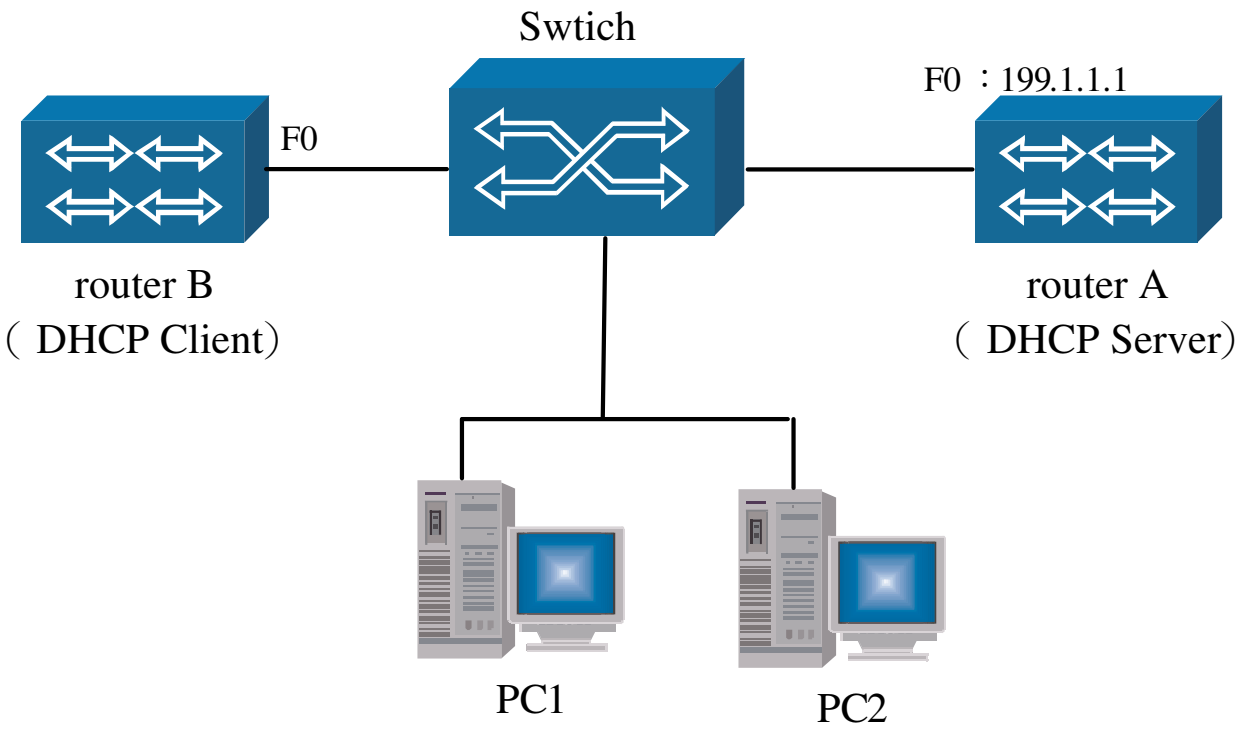
The second step: Configure the optional parameters passing to the host

DHCP can send more other information to the host in addition to assign addresses dynamically.

Configure DHCP address pool optional parameters

Command	Description
router(dhcp-config)#default-router A.B.C.D	Configure the default gateway of the host. A .B. C . D is the default gateways.
router(dhcp-config)#dns-server A.B.C.D	Configure DNS server addresses of the host. The addresses is A.B.C.D.
router(dhcp-config)#domain-name word	Configure DNS server name of the host
router(dhcp-config)#netbios-name-server A.B.C.D	Configure the addresses of server netbios-name. The addresses of the server netbios-name is A.B.C.D

DHCP Configuration Case



Signamax routerA f0 connects two PC and router B via L2 switch. Router A uses as DHCP server end, two
PC and router B use as client end. And routerA f0 ip address is 199.1.1.1. Configuration process is as following:

DHCP Commands of Router A in Global Mode

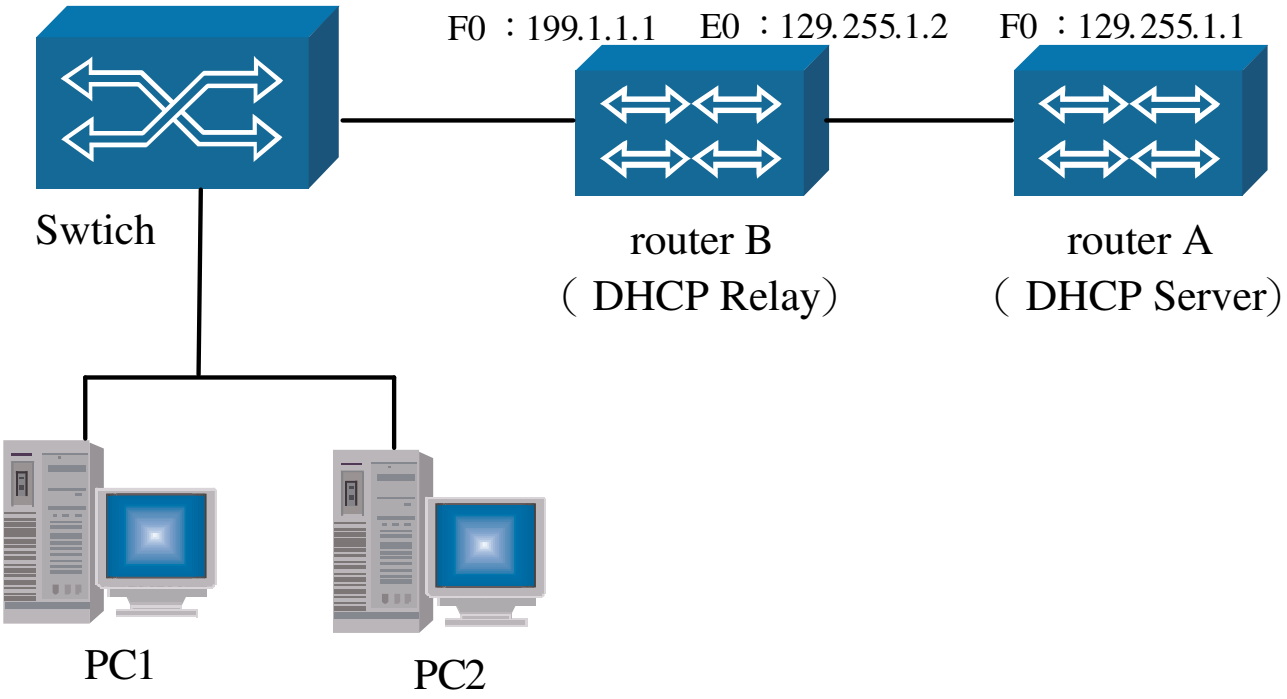
Command	Description
routerA#configure terminal	
routerA(config)#ip dhcp pool signamax	Define a DHCP address pool
routerA(config)# ip dhcp excluded-address 199.1.1.15	199.1.1.15 cannot be distributed.

DHCP Pool Command of Router A

Command	Description
routerA# configure terminal	
routerA(config)#ip dhcp pool signamax	Define an address pool
routerA(dhcp-config)#range 199.1.1.11 199.1.1.60 255.255.255.0	Define a range of ip address
routerA(dhcp-config)#dns-server 61.139.2.2	Designate router A dchp client dns address
routerA(dhcp-config)#default-router 199.1.1.1	Designate router A dchp client default gateway
routerA(dhcp-config)#lease 7 10 30	Distribute address lease time 7 10 30

On f0 of router B

Command	Description
routerB# configure terminal	
routerB(config-if-fastethernet0)#ip address dhcp	DHCP clinet get ip address from DHCP server.



dhcp configuration 2

Seeing figure 21-2, router A is dhcp server, router B is dhcp relay. F0 of router A address is 129.255.1.1,f0 of router B is 199.1.1.1 ,e0 ip address is 129.255.1.2,and the address pool of router A is the distributing address of pc1 and pc2.

Configuration process is as following:

Router A Configures DHCP Command in Global Mode

Command	Description
routerA#configure terminal	
routerA(config)#ip dhcp pool signamax	Define a DHCP address pool
routerA(config)# ip dhcp excluded-address 199.1.1.15	199.1.1.15 cannot be distributed.

Command of Router A in DHCP Pool

Command	Description
routerA# configure terminal	
routerA(config)#ip dhcp pool signamax	Define an address pool
routerA(dhcp-config)#range 199.1.1.11 199.1.1.60 255.255.255.0	Define a range of ip address
routerA(dhcp-config)#dns-server 61.139.2.2	Designate router A dchp client dns address
routerA(dhcp-config)#default-router 199.1.1.1	Designate router A dchp client default gateway
routerA(dhcp-config)#lease 7 10 30	Distribute address leased term 7 10 30

Router B Configuration

Command	Description
routerB# configure terminal	
routerB(config)# ip dhcp-server 129.255.1.1	Point to DHCP server

DHCP Checking and Debugging

- **show ip dhcp binding**

examine distributed IP address host list.

```
show ip dhcp binding
```

(command mode)privileged user mode

- **show ip dhcp pool-statistic**

examine DHCP address statistics information.

```
show ip dhcp pool-statistic
```

(command mode)privileged user mode

- **show ip dhcp arp-proxy-ipaddr**

This command is used for DHCP over IPsec,displaying gateway proxy remote client address information.

```
show ip dhcp arp-proxy-ipaddr
```

(command mode)privileged user mode

- **clear ip dhcp arp-proxy-ipaddr**

This command is used for DHCP over IPsec,to delete gateway proxy remote client address information.

```
clear ip dhcp arp-proxy-ipaddr [address | all]
```

Syntax	Description
address	Designate deleting special IP address proxy information
all	Delete all proxy information

(command mode)privileged user mode

- **debug ip dhcp**

Track debugging DHCP information.

```
debug ip dhcp {packet| lease| events|relay}
```

Syntax	Description
packet	Display DHCP switching packet.
lease	Display DHCP leased information
events	Display DHCP switching process
relay	Display DHCP proxy information.

(command mode)privileged user mode

SNA Configuration

IBM's SNA model is very similar to the OSI reference model. The traditional SNA physical entity adopts one of the four forms: host computer, communication controller, establishment controller and terminal.

An establishment controller is always called a cluster controller and it controls the input/output operation of peripherals (for example, a terminal). The SNA data link control layer supports multiform media including SDLC and X.25 etc.

DLSw Configuration

Data Link Switching (DLSw) explains peer connection establishment betwee routers, locating resources, transmitting data, flow control and SSP (Switch-to-switch Protocol) for error correction. Data-link peer connection between routers should be terminated according to RFC 1795, the data-link connection should be acknowledged locally.

DLSw terminates transmission of acknowledgement of the Data Link Layer and keepalive information over WAN by local acknowledgement of the local data-link connection. Timeout of the Data Link Layer cannot occur because of the local acknowledgement of data-link connection.

DLSw routers are to place multiple transmissions of data-link control to related pipelines of TCP and send them out reliably over IP networks. If two terminal systems want to establish connection via DLSw, the following tasks should first be completed:

Establish peer connection

Exchange capabilities

Establishing circuit

Configuring Commands to DLSw

Configuring the local parameters of DLSw:

Router(config)#dlsw local-peer ?

Commmand	Description
init-pacing-window	Configures the size of the initial window.
peer-id ip_address <promiscuous>	Sets the IP address of the local router. The parameter promiscuous is an optional command keyword, which is used to designate that the local router can accept the DLSw TCP connection request of the remote-end router without configuration.

Having configured the local parameters (for example, ip-address and promiscuous etc.) of the router, if you need to alter them, you should configure them afresh only after having canceled the latest parameters via related no command. At the same time, this no command should be executed before the other parameters of DLSw are configured, or else other commands will be ignored.

Configuring the remote parameters of DLSw:

The indispensable parameters are as follows:

Router(config)#

Command	Description
dlsw remote-peer list-number	The group number of token-ring. The default value of the group number is 0 (It represents that it can establish a chain with any ring group of the opposite terminal and can establish the peer relation).
dlsw remote-peer list-number tcp ip_address	ip-address is the local-peer address of the remote router. The local router uses the IP address and the local-peer address of itself to establish a kind of DLSw peer relation between two routers.

The optional parameters:

```
Router(config)#dlsw remote-peer list-number tcp  ip_address ?
```

Command	Description
backup-peer	Designates the remote-end router used as backup.
Cost	Designates the cost from the local router to the remote-end router specified by ip_address. Its valid value scope is from 1 to 5 and the default value is 3. The larger the value gets, the higher the cost of reaching the remote-end router is.
Keepalive	This is used for the remote-end router to configure the interval to keep alive. And the value scope of the interval whose unit is second is from 1 to 1200, the default value being 30. After the parameter keepalive

	has been configured, DLSw will transmit keepalive messages regularly on the TCP connection where no data is transmitted.
Lf	This command is used for the local router to inform the remote-end router designated by ip_address about its maximum frame length measured by byte so as to avoid segmenting the data frame. The valid size is 516, 1470, 1500, 2052, 4472, 8144,11407, 11454 and 17800 bytes and the default size is 1500 bytes.
Passive	This command is used to indicate that the remote-end router is passive because the local router will not send the DLSw connection request to the opposite router initiatively, but wait for the connection request sent by the opposite router.

```
router (config)#dlsw remote-peer list-number tcp  ip_address backup-peer ip_address1
```

Here, the remote-end router designated by ip_address is regarded as the backup entity of the remote-end router designated by ip_address1, namely that the router designated by ip_address1 is primary peer while the router designated by ip_address is backup peer.

In addition, before configuring backup peer, you should configure primary peer; while before deleting backup peer, you should delete backup peer. The same primary peer permits having one backup peer at most.

Configuring the DLSw bridge group

The DLSw bridge group command can be used to connect DLSw TCP link to the Ethernet bridge group or interrupt the connection between them.

The command is as follows:

Router (config)#

Command	Description
Dlsw bridge-group group-number	Connects the DLSw link to the Ethernet bridge group. The parameter group-number is used to designate the number of the transparent bridge group that will be connected with DLSw. The valid value ranges between 1 and 63.

The following command can be used to interrupt the link between the DLSw link and the designated Ethernet LAN bridge group:

router (config)#no dlsw bridge-group group-number

However, this command can interrupt the SNA link to the bridge group .

Configuring the prohibition/activation of running DLSw:

Router (config)#

Command	Description
dlsw disable	**Dlsw disable can be used to remove/ reconfigure DLSw, which does not change the configuration; while the command no dlsw disable can restart DLSw. In the default situation, DLSw is in the active status. In a peculiar situation, users may need to use the command dlsw disable to reconfigure the DLSw protocol module.**

dlsw icanreach and dlsw icannotreach

Above two commands are used for configuring DLSw switching content.

dlsw icanreach: designate local router reachable resource.

dlsw icannotreach: designate local router cannot reachable resource.

dlsw icanreach {mac-address mac-addr | mac-exclusive | saps sap}

dlsw icannotreach saps sap

Syntax	Description
mac-address	Configure local router **reachable** MAC address
mac-addr	Local router **reachable** MAC address
mac-exclusive	The local router only reaches user configured MAC address
saps	Configure local router supported or not supported service access site.
Sap	Local router supported or not supported service access site.

(command mode)global configuration mode

- **dlsw time range filtering command**

On router, DLSw Circuit local Mac address has realized control function.

dlsw mac-address mac-address time-range time-range

Syntax	Description
mac-address	Designate MAC address
mac-address	Designate filtering MAC address
time-range	Designate time-range.
time-range	Designate time filtering range name.

(command mode)global configuration mode
Note: 1, without configuring time-range, the default is deny.
2, In actual environment, the time is always gained via sntp protocol

from ntp srver. Mprouter configuration method is: sntp server <ip-address>, and ip address is ntp server address.

Debugging & Monitoring

- **show dlsw capabilities**

Display DLSw protocol performance information

```
show dlsw capabilities [{ local | ip-address ip-address }]
```

Syntax	Description
local	Display local router DLSw protocol all performance information
ip-address	Display peer router DLSw performance information
ip-address	Peer router ip address

(command mode)privileged user mode

- **show dlsw peers**

display router DLSw TCP connection status.

```
show dlsw peers
```

(command mode)privileged user mode

- **show dlsw circuits**

display router circuits status.

```
show dlsw circuits [detail]
```

Syntax	Description
detail	Detailed display

(command mode)privileged user mode

- **show dlsw reachability**

display DLSw reachable information
show dlsw reachability
(command mode)privileged user mode

- **debug dlsw**

```
enable dlsw sending and receiving message debugging switch.
debug dlsw [{core | peers ip-address ip-address}]
```

Syntax	Description
core	Enable DLSw core debugging information
peers ip-address	Enable remote designated router dlsw event message debugging switch

ip-address	Remote router ip address

(command mode)privileged user mode

SDLC Configuration

Overview

Synchronous Data Link Control (SDLC) was developed by IBM for System Network Architecture (SNA) environments, and it is the first bit-oriented synchronous protocol among all link-layer protocols. SDLC defines two types of network nodes: master node and secondary node. The master node controls other workstations (called secondary nodes) and polls the secondaries in a predetermined order. If a secondary node has data to send, it can transmit them only when it is polled by the master node. In working procedure, the master node will establish, terminate and manage links.

SDLC Configuring Commands

Set the serial port protocol as the SDLC encapsulation mode.

```
Router(config-if-xxx)# encapsulation sdlc
```

The commands on a serial port is as follows:

```
Router(config-if-xxx)#sdlc ?
```

Command	Description
address sdlc_address <xid-passthru | xid-poll>	This command can be used to designate the physical address of the equipment connected with related interface of router. The router can, via this address, establish a link layer connection with the lower-end equipment. The indispensable command parameters are as follows: The parameter sdlc-address represents the address assigned to the low-end physical equipment, and its valid value is a hexadecimal numeral within the range from 01 to FE. The optional command words are as follows: The command word xid-poll indicates that the type of the physical equipment designated by sdlc_address is PU2.1; It needs a given discovery frame to originate the link connection

	procedure. The command word xid-passthru indicates that router does not process any accepted XID frames in the data transmission procedure. This configuration is usually applied to minicomputer whose up-end host computer is of AS/400 class, while it is rarely applied to the down-end router.
vmac vmac_address	The parameter vmac_address designates the VMAC address of a given interface. It is a hexadecimal numeral character string separated by ".". Its format is like XXXX.XXXX.XXXX, of which X represents any a hexadecimal numeral within 0-F. Executes the command to designate a VMAC address for the interface. This address is used to identify each other when all equipment hanged by the interface establishes communication link with the up-end SNA equipment.
xid sdlc_address xid	Executes this command to configure XID values for the low-end equipment designated by sdlc_address. A XID value is used for the up-end SNA equipment to identify the low-end equipment. The indispensable parameters are as follows: The parameter sdlc_address represents the address of the low-end equipment whose XID value need be designated. The parameter xid represents the value that need be designated. Its format is like XXXXXXXX, of which X represents any a hexadecimal numeral within 0-F.
partner partners_mac_address sdlc_address	Execute this command to configure MAC address of the opposite terminal for the low-end equipment belonging to the SDLC interface. The indispensable parameters are as follows: The parameter partners_mac_addres represents the opposite terminal MAC address related to the low-end equipment. Its format is the same as that of the VMAC parameter. The parameter sdlc_address represents the physical address of the low-end equipment that needs to be configured.
dlsw local_sdlc_address	A series of low-end equipment configured on the interface can be associated with DLSw TCP connection via this command. Without this association, related equipment will not be used. The indispensable parameters are as follows: The parameter local_sdlc_addres designates a series of low-end equipment addresses, which are separated by blanks.
delay-response	Delays the response time.
poll-pause-timer	Sets the polling interval.
sdlc-largest-frame	Configures the length parameter of the maximum information frame permitted by the low-end equipment.

The command sdlc xid sdlc_address xid is useful only when the type of the low-end equipment is PU2.0. In the situation that the command words xid-passthru and xid-poll have be configured in the command sdlc address, configuring XID value will not take effect. In addition, before XID value is configured, the physical address of related low-end equipment should first be configured, or else related XID value cannot be configured. When configuring XID value, users should ensure it is consistent with the configuration of the up-end equipment, or else the SNA connection cannot be established.

When configuring the command sdlc partner partners_mac_address sdlc_address, users should configure the physical address of the low-end equipment. At the same time users should ensure the opposite terminal MAC address configured on the local router is consistent with the up-end VMAC address.

Specify that the data encode mode on the interface is NRZI (the default mode is NRZ)

```
router(config-if-serial1)#nrzi-encoding
```

Configuring Operations of SDLC on Interface

The SDLC address of the equipment (PU) connected with the interface is c2, the up-end host computer is a minicomputer of AS400 type. The virtual MAC address of the local interface serial1 is 4020.2654.0a00. The XID value of the connected equipment is c2 0a238e33, the opposite terminal MAC address is 5600.7507.34c2, and the SDLC address is c2. The following are designated: the size of the transmission window, whose data-coding mode on the interface is NRZI, is 5; the polling interval is 20 seconds, and the local station should be polled 5 times before the next polling; the latest frame should be held for 2 seconds.

Command	Description
router(config-if-serial1)# encapsulation sdlc	Encapsulating SDLC
router(config-if-serial1)#sdlc vmac 4020.2654.0a00	The virtual MAC address of the interface
router(config-if-serial1)#sdlc address c2 xid-passthru	The SDLC address up-end host of the equipment (PU), which is connected with the interface, is of AS400 type.
router(config-if-serial1)#sdlc xid c2 0a238e33	The connected equipment XID
router(config-if-serial1)#sdlc partner 5600.7507.34c2 c2	The MAC address and SDLC address of the port

router(config-if-serial1)#nrzi-encoding	Designates that the data coding mode of the interface is NRZI.
router(config-if-serial1)#sdlc k 5	The transmission window size is 5.
router(config-if-serial1)#sdlc poll-pause-time 20	The poll interval is 20 seconds.
router(config-if-serial1)#sdlc n2 5	The local station is polled 5 times before the polling.
router(config-if-serial1)#sdlc t1 2	Sets waiting time as 2 seconds for the latest frame.
router(config-if-serial1)#sdlc dlsw c2	The local equipment address running on the SDLC link

LLC2 Configuration

Overview

The router connects to the bridge group in LAN via the local Ethernet interface. The bridge group is related with the DLSw TCP connection, and the local LAN interface runs LLC2 protocol.

- **dlsw bridge-group**

Use the command **dlsw bridge-group** to relate the DLSw TCP connection with the Ethernet bridge group in the global configuration mode.

```
dlsw bridge-group  group-number
```

Syntax	Description
group-number	The bridge-group number that will be related with the DLSw TCP connection. its value range is from 1 to 10.

(Command mode)the global configuration mode.

- **bridge group**

Use the command bridge group to connect the local Ethernet interface to the bridge group in the local LAN.

```
bridge group group-number
```

Syntax	Description
group-number	The bridge-group number configured for the Ethernet interface. It should be consistent with group-number of the command dlsw bridge-group

(Command mode)the interface configuration mode.

When there is too much data in the LAN and LLC2 is bridged via Bridge, SAP access list can be configured on Bridge and nothing but SNA data is allowed to be bridged so that it can be avoided that the data broadcasted in the local LAN is bridged to LLC2 and transmitted to the upper-end router via DLSw. That is to say that the upper-end network congestion can be avoided.

- **access-list**

Use the command **access-list** to configure LSAP access list.

```
access-list list-number permit/deny lsap-addr [lsap-wildcard]
```

Syntax	Description
access-list list-number {permit | deny} {any | host macaddress/macaddress macmask}	Configure MAC access list
list-number	The access list number. Its value range is from 4001 to 5000.
permit/deny	Permit/Deny access.
lsap-addr	The permitted/denied <dsap,ssap>.
lsap-wildcard	The wildcard

(Command mode)the global configuration mode.

```
bridge-group group-number  input-lsap-list <list-number>
```

Use the command **bridge-group *group-number* input-lsap-list *<list-number>*** to filter the SAP frames received by the bridge group.

```
bridge-group group-number  output-lsap-list <list-number>
```

Use the command **bridge-group *group-number* output-lsap-list *<list-number>*** to filter the SAP frames sent by the bridge group.

```
bridge-group group-number  input-type-list <list-number>
```

Use the command **bridge-group *group-number input*-type-list *<list-number>*** to filter the Ethernet frames received by the bridge group.

```
bridge-group group-number  output-type-list <list-number>
```

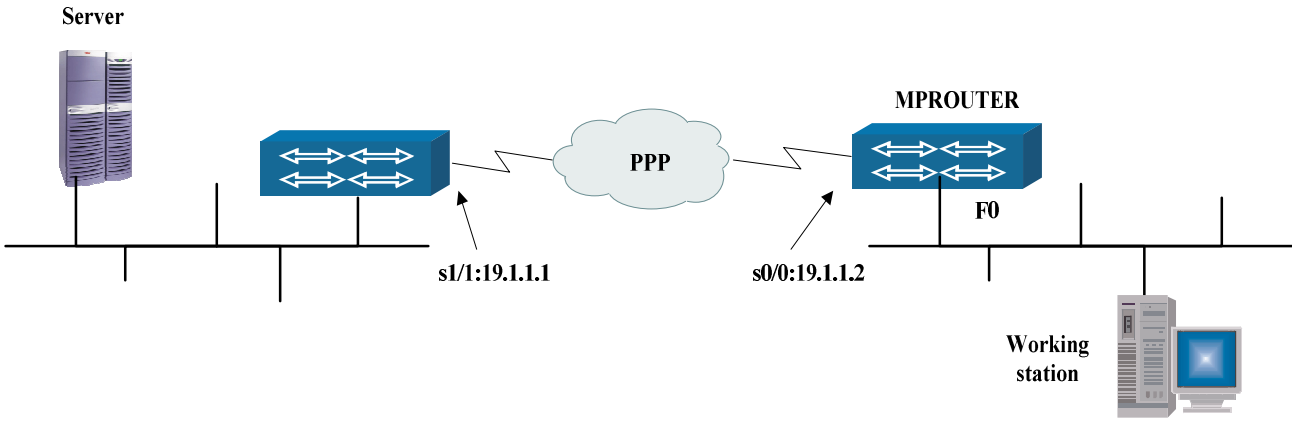
Use the command **bridge-group *group-number output*-type-list *<list-number>*** to filter the Ethernet frames sent by the bridge group.

🕮 Note:

```
Generally, The SAP list is configured as follows:
access-list 4001 permit  0x0404 0x0000  or
access-list 4001 permit  0x0d0d 0x0000
```

Thereby, lsap(0x04,0x04)SNA needs is permitted to pass and other types of packets can be filtered out.

An example of typical LLC2 configuration



Signamax router connects to the bridge group in LAN via the local Ethernet interface. And the bridge group is related with the DLSw TCP connection.

Configure related DLSw commands in the global configuration mode.

Syntax	Description
Dlsw local-peer peer-id 19.1.1.2	The DLSW address of the local end.
Dlsw remote-peer 0 tcp 19.1.1.1	The DLSW address of the remote end.
Dlsw bridge-group 1	The DLSw bridge-group number in the local LAN

The interface S0/0 adopt the PPP protocol to connect to the upper-end router.

Syntax	Description
encap ppp	Encapsulate the PPP protocol.
ip address 19.1.1.2 255.255.255.0	Specify an IP address for the interface S0/0.

The interface F0 connects to the bridge-group in the local LAN.

Syntax	Description
bridge-group 1	The bridge-group number.

Filter the SAP frames received by the bridge-group.

Syntax	Description
access-list 4001 permit 0x0404 0x0000	The SNA packets are permitted to pass.
bridge-group 1 input-lsap-list 4001	The SNA packets received by the bridge-group from the station are permitted to pass.

To relate the DLSw TCP connection with the bridge-group in the local LAN, configure the bridge-group number of DLSw in the global configuration mode, and the same bridge-group number should be configured on the Ethernet interface so that the Ethernet bridge-group can be related with the DLSw bridge-group.

QLLC Configuration

Qualified Link Layer Control (QLLC) is a data link protocol defined by IBM and which allows SNA data to be transmitted in the X.25 network. In the traditional SNA network, any equipment using the X.25 protocol on the SNA communication channel, no matter which on terminal or intermediate system it resides in, needs to make use of the QLLC protocol.

The QLLC transform feature avoids the requisition for the local IBM equipment to install X.25 software. And QLLC only demands that the low-end equipment can provide X.25 interface to connect with the lower-end equipment in the remote-end X.25 network with the IBM mainframe via the router with QLLC transform feature. The router connects with the upper-end equipment via DLSw TCP, so the intermediate equipment does not need the X.25 interface and the software.

QLLC Commands

Command	Description	Config mode
encapsulation x25	* encapsulate x.25 protocol on serial interface	config-if-××
• dlsw qllc local-window size	* configure local x25 window size for flow control between DLSw and x.25.	config
x.25 pvc pvc qllc vmac	*connect x.25 interface pvc and QLLC protocol	config-if-××
qllc dlsw pvc pvc partner partner_address	* connect QLLC protocol and DLSw TCP.	config-if-××
x25 map qllc vmac x121-addr	Router adopts x.25 svc communication with remote x.25 protocol PU equipment.	config-if-××
qllc dlsw vmac vmac1 partner vmac2	Connect QLLC protocol SVC and DLSw TCP	config-if-××
qllc dlsw partner vmac	Execute the command if the interface x.25 equipment are the same.	config-if-××

Basic Commands

`encapsulation x25`

Encapsulate x.25 protocol on serial interface in interface mode.

(command mode)interface configuration mode

`dlsw qllc local-window size`

Configure local x25 window size to control DLSw and x.25. when X.25 speed is so slow, change window value, and reduce sending rate of DLSw, to avoid x.25 data sending queue flooding.

```
dlsw qllc local-window size
```

Syntax	Description
local- window	Connected DLSw TCP bridge number, and the range is 1—63
size	Window size, and the range is 10 – 100,default is 50

(command mode)global configuration mode

- **show qllc**

Examine QLLC connecting status

```
show qllc {interface interfcae | partner | connection}
```

Syntax	Description
interface	Display qllc interface information
interface	Interface name
partner	Display qllc partner configuration information
connection	Display qllc connection information

(command mode)global configuration mode

- **debug qllc**

Display qllc connecting and disconnecting information
(command mode)global configuration mode
QLLC DLSw has two modes, which is: pvc(permanent virtual circuit) mode, svc(switching virtual circuit) mode.

PVC Mode

```
x.25 pvc pvc qllc vmac
```

relate x.25 pvc and QLLC protocol.

```
x.25 pvc pvc qllc vmac
```

Syntax	Description
pvc	Pvc number, and the range is 1—4095(should be small than ltc)
vmac	Low site vmac address connecting remote x.25 network.

(command mode)interface configuration mode

- **qllc dlsw pvc pvc partner partner_address**

Relate QLLC protocol and DLSw TCP.

```
qllc dlsw pvc pvc partner partner_address
```

Syntax	Description
pvc	Pvc number, with the last command designated PVC number
partner_address	Peer equipment vmac address to low site equipment.

(command mode)interface configuration mode

SVC mode

- **x25 map qllc**

```
Router adopts x.25 svc mode to communicate with PU equipment.
x25 map qllc vmac x121-addr
```

Syntax	Description
vmac	Vmac address connecting remote x.25 network.
x121-addr	x.121 address connecting to remote x.25 network. (vmac designated equipment)

(command mode)interface configuration mode

- **qllc dlsw vmac vmac1 partner vmac2**

Relate QLLC protocol and DLSw TCP.

```
qllc dlsw vmac vmac1 partner vmac2
```

Syntax	Description
vmac1	Low site vmac address connecting remote x.25 network.
vmac2	Upper site vmac address communicating with vmac1

(command mode)interface configuration mode

- **qllc dlsw partner vmac**

This command can be executed if this interface all x.25 equipment host is the same.

```
qllc dlsw partner vmac
```

Syntax	Description
vmac	Vmac address connecting x.25 equipment.

(command mode)interface configuration mode

Typical QLLC Configuration

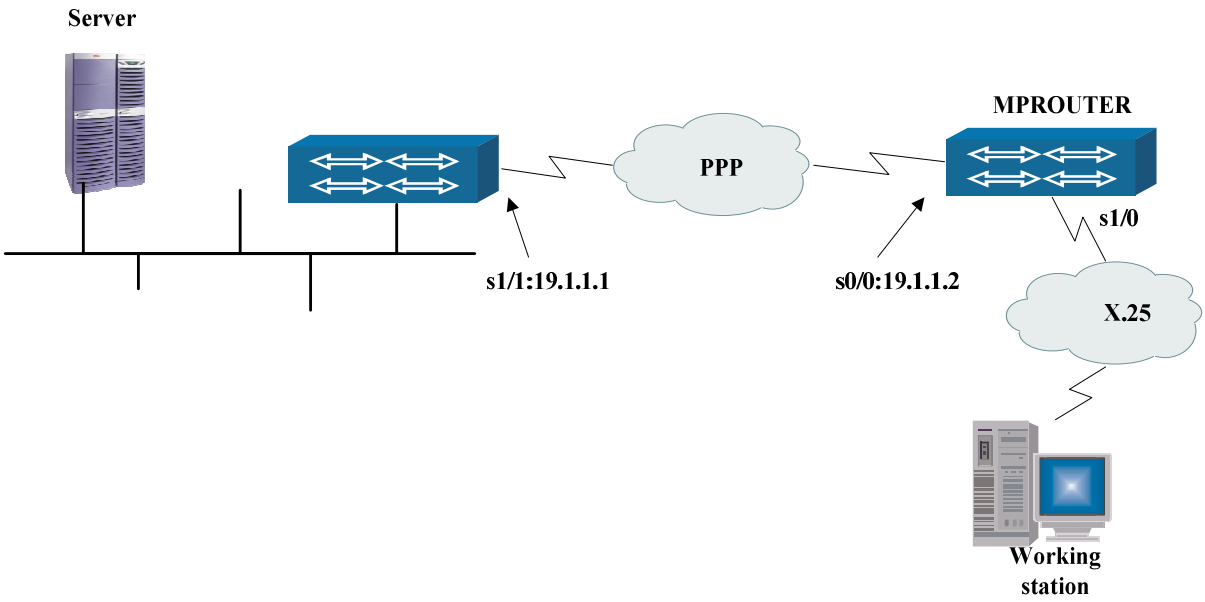


Figure 22-2

Illustration:

Here the Signamax router connects with a X.25 network via a serial port, runs QLLC protocol, connects with the low-end SNA equipment, and associates the DLSw TCP with the QLLC protocol. The configuration of the down-end Signamax router is as follows:

Configuring the commands of DLSw in the global configuration mode:

Command	Task
router(config)#dlsw local-peer peer-id 19.1.1.2 router(config)#dlsw remote-peer 0 tcp 19.1.1.1	Configures DLSw.

The interface S0 connects with the upper-end router via PPP protocol:

Command	Task
router(config)#int s0	Configures the PPP protocol for the interface to connect with the up-end router.
router(config-if-serial0)#encap ppp	
router(config-if-serial0)#ip address 19.1.1.2 255.255.255.0	
router(config-if-serial0)#exit	

The interface S1 connects with X.25 network, runs QLLC protocol, and connects with the low-end SNA equipment:

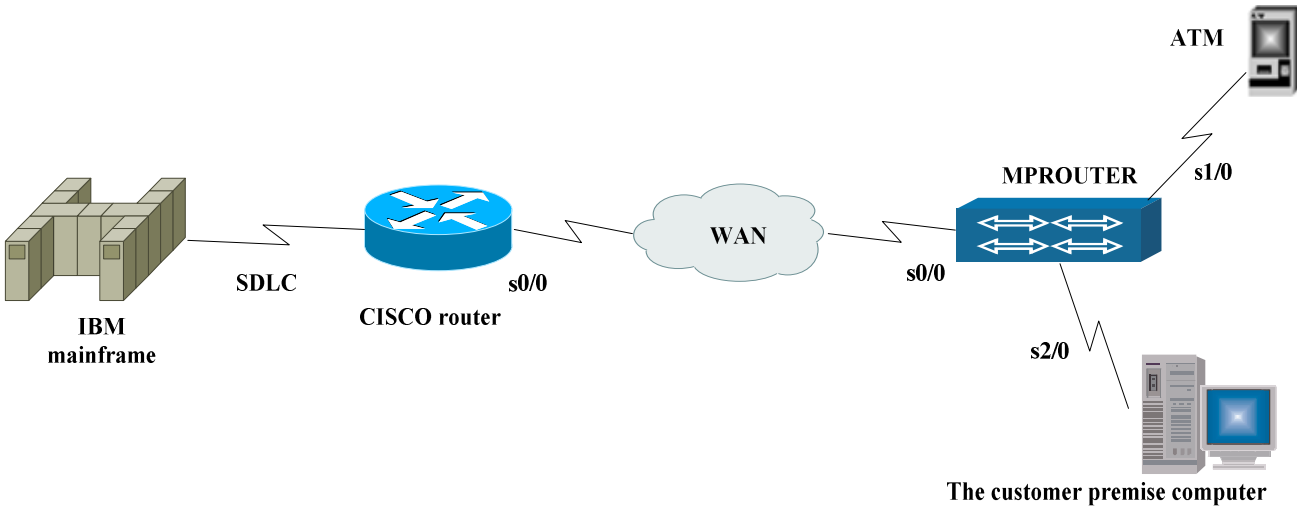
Command	Task
router(config)#int s1	
router(config-if-serial1)#encap x25	Encapsulates the X.25 protocol.
router(config-if-serial1)#x25 dce	Configures it as the DCE mode.
router(config-if-serial1)#x25 ltc 10	
router(config-if-serial1)#x25 pvc 1 qllc 1111.2222.3344	Associates VC of the X.25 interface with the QLLC protocol; 1111.2222.3344 is the VMAC address of the low-end equipment.
router(config-if-serial1)#qllc dlsw pvc 1 partner 2233.4455.6677	Associates the QLLC protocol with the DLSw TCP connection.
router(config-if-serial1)#end	

The QLLC protocol associates the low-end equipment with X.25 VC, and exclusively determines a low-end equipment via related VMAC address and the partner address.

SNA Network Mode & Configuration

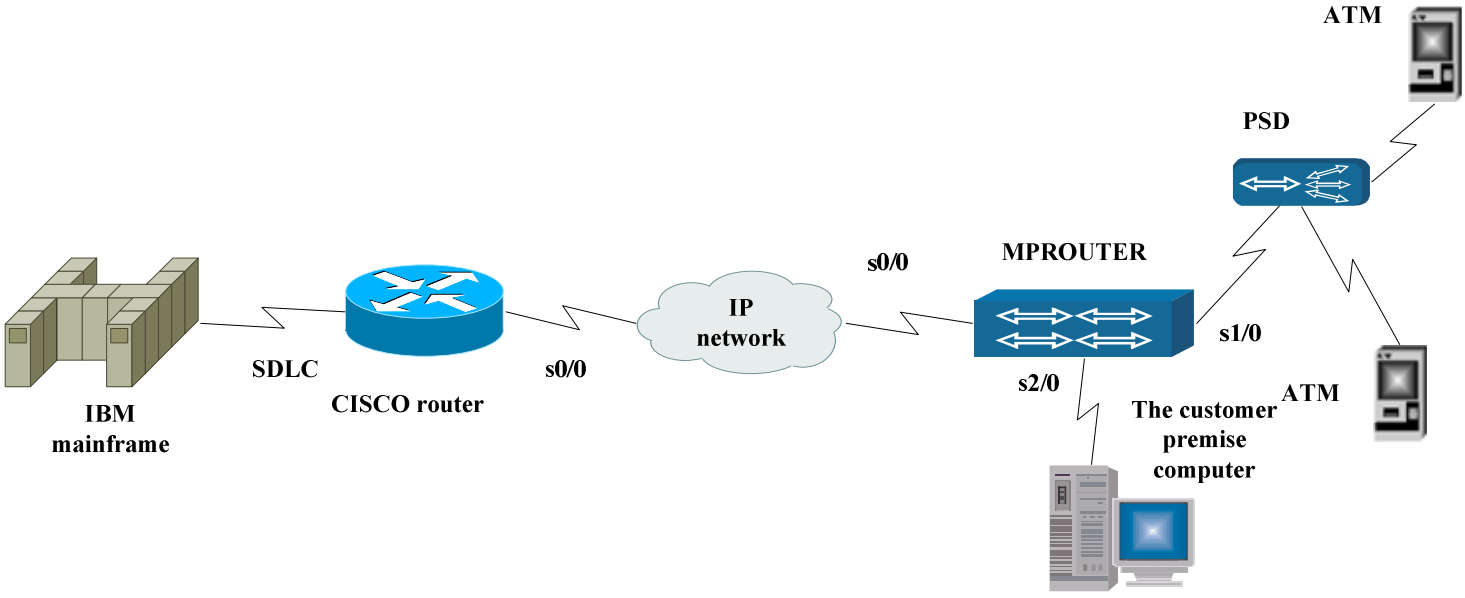
Network Construction Mode of SNA Application

A. Connect the ATM with the customer FEP directly via synchronous/asynchronous serial port. The network structure is showed in the following figure:



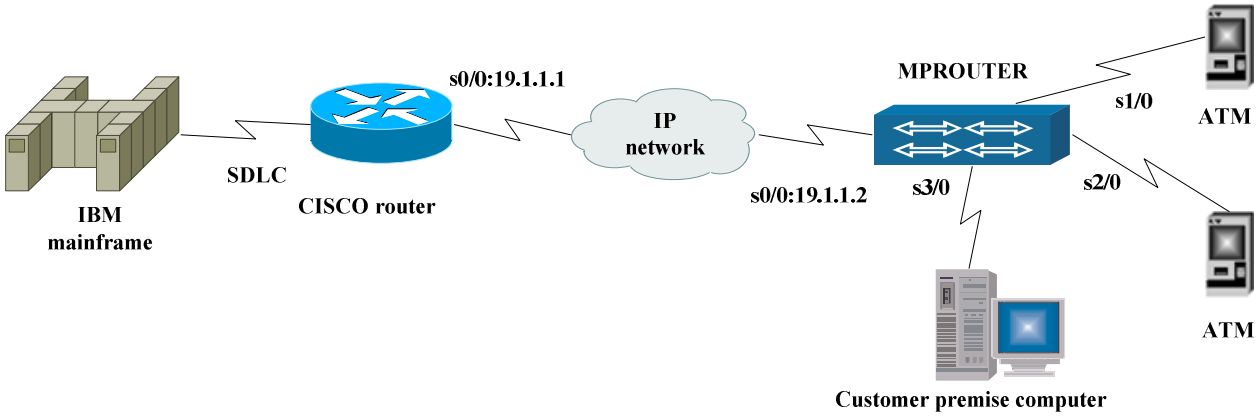
A Cisco router and a Signamax router can communicate via the serial interface by means of some link protocols, such as PPP, HDLC, FR and X.25, or can communicate directly via the local Ethernet.

The synchronous/asynchronous serial port connects with ATM and the customer FEP via PSD, or connects with IBM mainframe via Cisco router. It can be shown as follows:



Network Mode Configuration

Example



ATM and front end processor connect to the serial interface of Signamax router directly, and Signamax router connects to Cisco router by means of running the PPP protocol on the serial interface.

The DLSw configuration commands in the global configuration mode are listed as follows:

Syntax	Description
dlsw local-peer peer-id 19.1.1.2	DLSW local-peer address
dlsw remote-peer 0 tcp 19.1.1.1	DLSW remote-peer address

The PPP is configured for the interface S0/0 to connect to the upper-end router:

Syntax	Description
encap ppp	Encapsulate the PPP protocol.
ip address 19.1.1.2 255.255.255.0	Specify an IP address for the interface S0/0.

Configure the ATM (the SDLC address is C1) on the interface S1/0:

Syntax	Description
encap sdlc	Encapsulate SDLC.
sdlc vmac 1111.1111.1100	The interface vmac address
sdlc address c1	The SDLC address of the connected equipment
sdlc xid c1 05df0301	The xid of the connected equipment.
sdlc partner 1111.2222.33c1 c1	The vmac address of the opposite end.
sdlc dlsw c1	Relate SDLC to DLSW.
clock rate 9600	Clock rate.

Configure the ATM (the SDLC address is C2) on the interface S2/0:

Syntax	Description
encap sdlc	Encapsulate SDLC
sdlc vmac 2222.2222.2200	The interface vmac address
sdlc address c2	The SDLC address of the connected equipment
sdlc xid c2 05df0302	The xid of the connected equipment
sdlc partner 1111.2222.33c2 c2	The vmac address of the opposite end
sdlc dlsw c2	Relate SDLC to DLSW
clock rate 9600	Clock rate

Configure the front end processor (the SDLC address is C3 and the type is PU2.1) on the interface S3/0:

Syntax	Description
encap sdlc	Encapsulate SDLC.
sdlc vmac 3333.3333.3300	The interface vmac address
sdlc address c3 xid-poll	The downstream equipment of the SDLC interface is the PU2.1 front end processor.
sdlc partner 1111.2222.33c3 c3	The vmac address of the opposite end.
sdlc dlsw c3	Relate SDLC to DLSW.
clock rate 9600	Clock rate

For the downstream equipment of the SDLC interface, there exists some difference between PU2.1 and PU2.0.

Typical configuration two

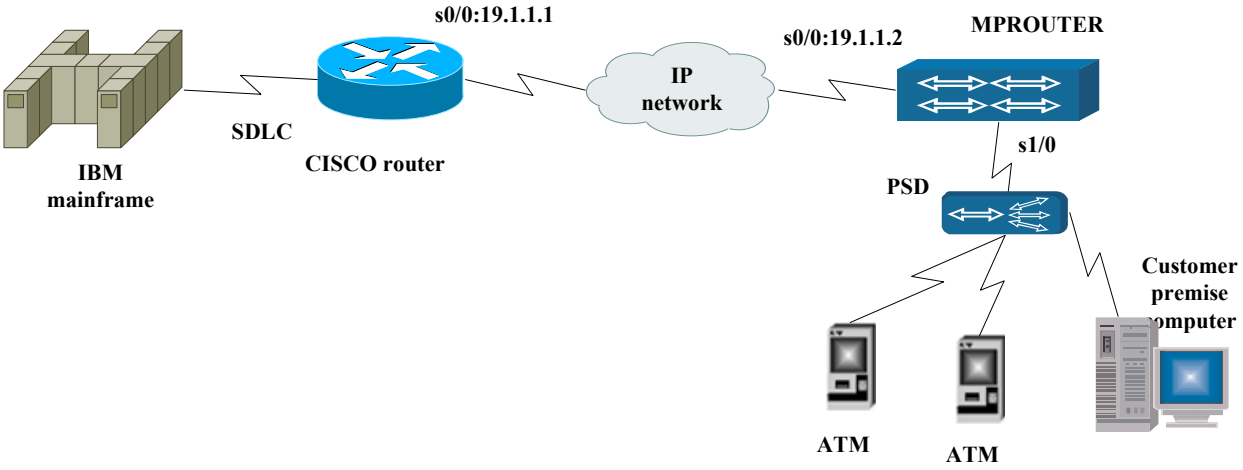


Figure 22-6

By means of PSD, one serial interface of Signamax router connects with multiple downstream equipments, and connects to the upper-end Cisco router via WAN.

The DLSw configuration commands in the global configuration mode are listed as follows:

Syntax	Description
dlsw local-peer peer-id 19.1.1.2	DLSW local-peer address.
dlsw remote-peer 0 tcp 19.1.1.1	DLSW remote-peer address.

The configuration interface S0/0 connects to the upper-end router by means of PPP protocol.

Syntax	Description
encap ppp	Encapsulate the PPP protocol.
ip address 19.1.1.2 255.255.255.0	Specify an IP address for the interface s0/0.

The configuration interface S1/0 connects with two ATMs (whose SDLC addresses are respectively C1 and C2) and the front end processor (the address: C3, type: PU2.1) via PSD.

Syntax	Description
encap sdlc	Encapsulate SDLC.
sdlc vmac 1111.1111.1100	The interface vmac address
sdlc address c1	The SDLC address of the connected equipment
sdlc xid c1 05df0301	The xid of the connected equipment.
sdlc partner 1111.2222.33c1 c1	The vmac address of the opposite end.
sdlc address c2	The SDLC address of the connected equipment
sdlc xid c2 05df0302	The xid of the connected equipment.
sdlc address c3 xid-poll	
sdlc partner 1111.2222.33c3 c3	
sdlc partner 1111.2222.33c2 c2	The vmac address of the opposite end.
sdlc dlsw c1 c2 c3	Relate SDLC to DLSW.
clock rate 9600	Clock rate

If multidrop is enabled on the same interface, multiple VMAC addresses can be adopted.

Syntax	Description
encap sdlc	Encapsulate SDLC.
sdlc address c1	The SDLC address of the connected equipment
sdlc vmac 1111.1111.1111 c1	The interface vmac address(the sdlc partner address of the opposite router is 1111.1111.1111). There exists no relation between the interface address and sdlc c1 address.
sdlc xid c1 05df0301	The xid of the connected equipment.
sdlc partner 1111.2222.33c1 c1	The vmac address of the opposite end.
sdlc address c2	The SDLC address of the connected equipment

sdlc vmac 2222.2222.2222 c2	The interface vmac address(the sdlc partner address of the opposite router is 2222.2222.2222) There exists no relation between the interface address and sdlc c2 address.
sdlc xid c2 05df0302	The xid of the connected equipment.
sdlc address c3 xid-poll	
sdlc vmac 3333.3333.3333 c3	
sdlc partner 1111.2222.33c3 c3	
sdlc partner 1111.2222.33c2 c2	The vmac address of the opposite end.
sdlc dlsw c1 c2 c3	Relate SDLC to DLSW.
clock rate 9600	Clock rate

The configuration above indicates that: different types of downstream equipments can connect to one serial interface via PSD. At the same time, when PSD is adopted, the line clock is provided by PSD, and the interface of the router operates in the external clock mode.

The following points should be noticed in the SNA applications:

- Whether Signamax router and Cisco router are consistent on DLSw/SDLC configuration.

- The status of the interface connecting with ATM, front end processor or PSD is UP.(by means of the command show int <interface name>)

- Determine whether the static route is configured on Signamax router according to the factual requirements.

- Determine whether the configuration of DLSw remote-peer is added on Cisco router according to the factual requirements.

- Check whether the IP address specified by Cisco local-peer can be reachable via Signamax router(by means of Ping)；

- Check whether the XID frame need be configured.

- Check whether some special options need be configured.

- Check whether cables are in order and physical signals are adequate.

MPLS Configuration

MPLS (Multiprotocol Label Switching) is a label-based packet forwarding technology, with advantages of both the packet forwarding technology of layer-2 switch and the routing technology of layer-3, simplifying segment-by-segment data forwarding and enhancing the packet forwarding capacity. The main contents of this chapter are as follows:

Brief introduction to MPLS

Description of commands to configure MPLS

An example of MPLS configuration

MPLS Overview

For the traditional IP packet forwarding, the router in each relay segment of the network analyses the destination IP address independently and executes the network routing algorithm so as to make the independent forwarding decision and determine the next hop for the packet.

However, MPLS divides all packets that enter the network into different FECs (Forwarding Equivalence Class) and assigns a label to each FEC, so each packet carries a short label with fixed length. The routers in the network determine how to forward a packet according to its label.

In the whole MPLS area, the packet forwarding is operated according to the label, without operating anything to the IP header.

MPLS consists of two sections. One is the label packet forwarding, implementing the forwarding of the received IP packets or label packets. Its main operations include:

If the received packet is an IP packet, then search the label forwarding list according to its destination address; if there exists the output label (namely, the next hop supports the label forwarding) of the destination address, then insert this output label into the IP header, subsequently, forward this packet to the next hop.

If the received packet is a label packet, then search the label forwarding list according to the input label on the label stack top; if it succeeds in finding out related output label, then replace the input label with the output label, subsequently, forward this packet; if it fails in finding out

related output label, then pop the input label, subsequently, forward this packet in the form of IP packet.

The other section is LDP (Label Distribution Protocol), used to switch the label binding information with the neighbor routers. Via sending Hello packets periodically, LDP finds and maintains a LDP peer. When finding out a new LDP neighbor, LDP creates a TCP connection with it. Then, via this TCP connection, it uses information switch label that LDP defines to bind information, create and maintain a label-forwarding list.

Commands to Configure MPLS

mpls ip

To enable mpls on the router, you can do nothing but configure the command under the global configuration mode and the interface configuration mode. The form no of this command is used to disable mpls.

mpls ip

no mpls ip

(Command mode)The global configuration mode and the interface configuration mode.

🕮 **Note:**

To use mpls, you should configure the command mpls ip under both the global configuration mode and the interface configuration mode. Configuring the command mpls ip under the global configuration mode is used to enable mpls, while configuring the command under the interface configuration mode is used to specify which interface to use mpls packet forwarding. You can configure the command mpls ip on multiple interfaces.

If the link layer protocol is PPP, then it needs to configure the command ppp mpls on the interface.

mpls ip propagate-ttl

This command is used to configure encapsulating MPLS packet TTL. In default status, MPLS top TTL segment uses IP top TTL value, and after configuring this command, MPLS top TTL value is 255, and the command no is used to renew the default value.

```
mpls ip propagate-ttl [forwarded | local]
```

```
no mpls ip propagate-ttl [forwarded | local]
```

Syntax	Description
forwarded	Effective for forwarded packet.
local	Effective for local packet.

(Default status)MPLS top TTL segment uses IP top TTL value.
(command mode)global configuration mode

🕮 **Note:**

This command is only valid for encapsulating MPLS packet. And via this command, MPLS network label switching can be hidden to users.

mpls ldp router-id

When mpls is enabled, you need select a router-id (namely, an IP address) to serve as the ldp ID, which is used to identify a specific LSR label space. The form no of this command is used to reset the default value of route id.

```
mpls ldp router-id A.B.C.D
```

```
no mpls ldp router-id
```

Syntax	Description
A.B.C.D	This is an IP address serving as the ldp ID

(Default)When mpls starts, it automatically selects an interface address to serve as router-id.

(Command mode)The global configuration mode.

🕮 **Note:**

By default, mpls automatically selects an interface address to serve as router-id when starting. And it can select the address of a loopback interface. Under the situation that no router-id is configured, if the selected interface address that serves as the router-id is changed, all ldp connections are deleted, and the ldp can update the router-id, subsequently, a new connection is rebuilt.

mpls ldp loop-detection

ldp check loopback via leap and routing vector. You may not install this LSP if there is loopback. The command no is used to disable this function.

```
mpls ldp loop-detection
```

```
no mpls ldp loop-detection
```

(Default status)ldp disables loopback check function by default.
(command mode)global configuration mode

mpls ldp label-distribution

This command is used to set the ldp label distribution mode. The form no of this command is used to reset the default setting of the label distribution mode.

```
mpls ldp label-distribution <dod/du>
```

```
no mpls ldp label-distribution
```

Synt ax	Description
dod/du	Label distribution is on demand or unsolicited for downstream.

(Default)The DU (downstream unsolicited) label distribution mode.

(Command mode)The interface configuration mode.

🕮 **Note:**

When using the downstream-unsolicited label distribution mode, for a specific FEC, an LSR (label switched router) can assign and distribute a label immediately without getting a label request message from the upstream; however, when using the downstream-on-demand label distribution mode, for a specific FEC, only after receiving the upstream label request message from the upstream can an LSR (label switched router) assign and distribute a label.

This command is configured under the interface mode, and different label distribution modes can be configured for different interfaces.

mpls ldp label-control

This command is used to configure the ldp label control mode. The form no of this command is used to reset the default setting of the ldp label control mode.

```
mpls ldp label-control  <independent/ordered>
```

```
no mpls ldp label-control
```

Syntax	Description
independent/ordered	The independent control mode or the ordered control mode.

(Default)The independent control mode.

(Command mode)The global configuration mode.

🕮 **Note:**

When using the independent label control mode, each LSR can announce the label mapping to the LSR (label switch router) that connects with it at any time; however, when using the ordered control mode, only after the LSR receives the FEC label mapping message of the specific FEC net hop or when the LSR is the LSP out-bound node, can the LSR send label mapping messages to the upstream.

mpls ldp label-retention

This command is used to set the ldp label retention mode. The form no of this command is used to reset the default setting of the ldp label hold mode.

```
mpls ldp label-retention  <conservative/liberal>
```

```
no mpls ldp label-control
```

Syntax	Description
conservative/liberal	The conservative hold mode or the liberal retention mode.

(Default)The liberal retention mode.

(Command mode)The global configuration mode.

🕮 **Note:**

For a specific FEC, suppose that the upstream has received the label binding that comes from the downstream, then, when the downstream router is no longer the next hop of this FEC, if the upstream still preserves this binding, the mode used by the upstream is called the liberal label retention mode; if the upstream discards this binding, then the mode used by the upstream is called the conservative label retention mode.

There are various combinations between three label assignment parameters (label distribution mode, label control mode and label retention mode). However, the default parameters are downstream-unsolicited distribution, independent control and liberal retention.

mpls ldp hello-interval

This command is used to set the interval (by second) for LSR to send a Hello message periodically. The form no of this command is used to reset the default setting of interval of the Hello message.

```
mpls ldp hello-interval  <1-60>
```

```
no mpls hello-interval
```

Syntax	Description
1-60	The interval to send a Hello message.

(Default)5 seconds.

(Command mode)The interface configuration mode.

🕮 **Note:**

Via sending the Hello packet periodically, LSR finds or maintains a Hello neighbor.

mpls ldp hello-hold-interval

This command is used to set the hold time of ldp hello. The hold time specifies the maximum hold time (by second) for the LSR to keep the previous Hello message before sending the next Hello message to its

peer. LSRs can, via respectively putting forward its own Hello hold time , negotiate the Hello hold time with each other and then adopt the minimum value of them. The form no of this command is used to reset the default value of the Hello hold time.

`mpls ldp hello-hold-interval <1-60>`

no mpls ldp hello-hold-interval

Syntax	Description
1-60	Hello hold time.

(Default)15 seconds.

(Command mode)The interface configuration mode.

🕮 **Note:**

LSR maintains a Hello hold timer for each Hello neighbor peer. When an LSR receives a Hello message from a specific Hello neighbor, related Hello hold timer will be restarted. If the LSR hasn't still received the next Hello message from the specific Hello neighbor when the Hello hold timer expires, then LSR deletes this Hello neighbor, and sends related announcement message; subsequently, closes the TCP connection and ends the LDP session.

Hello hold time being 0 indicates the default value. For a link Hello message (connecting with the neighbor directly), the default value is 15s; while for a destination Hello message (not connecting with the neighbor directly), the default value is 45s.

mpls ldp keepalive-interval

This command is used to set the interval (by second) for LSR to send a Keepalive message periodically. The form no of this command is used to reset the default setting of the Keepalive message.

`mpls ldp keepalive-interval  <1-60>`

`no mpls keepalive-interval`

Syntax	Description
1-60	The interval for LSR to send a Keepalive message periodically.

(Default)15 seconds.

(Command mode)The interface configuration mode.

🕮 **Note:**

An LSR should ensure that the LDP peer can receive at least one LDP message (any LDP message is effective) in the keepalive-interval. But if there is no other LDP message for LSR to send, then LSR should send a session hold message.

mpls ldp keepalive-hold-interval

This command is used to set the ldp session hold interval. LSRs can, via putting forward its own session hold interval respectively, negotiate the session hold interval with each other, and then adopts the minimum value of them. The form no of this command is used to reset the default value of the session hold interval.

```
mpls ldp keepalive-hold-interval
```

```
no mpls ldp keepalive-hold-interval
```

Syntax	Description
1-60	The ldp session hold interval.

(Default)45 seconds.

(Command mode)The interface configuration mode.

🕮 **Note:**

Via the LDP PDU received from the session transmission connection, an LDP checks the integrality of the LDP session. The LSR maintains a session hold timer for each LDP session connection, and related session hold timer can be restarted when the LSR receives the LDP PDU from a specific session connection. If the LSR hasn't still received LDP PDU from the LDP peer when the session hold timer expires, then LSR sends an announcement message, closes the TCP connection and ends the LDP session.

mpls route-cache

The MPLS fast switching is realized via route cache mechanism. The purpose of the route cache is to reduce the repeated searching of a routing table and to accelerate the packets sending speed via using previous cache searching results. But under certain circumstances, users can choose to enable/disable the following two places to process route cache.

```
mpls route-cache
```

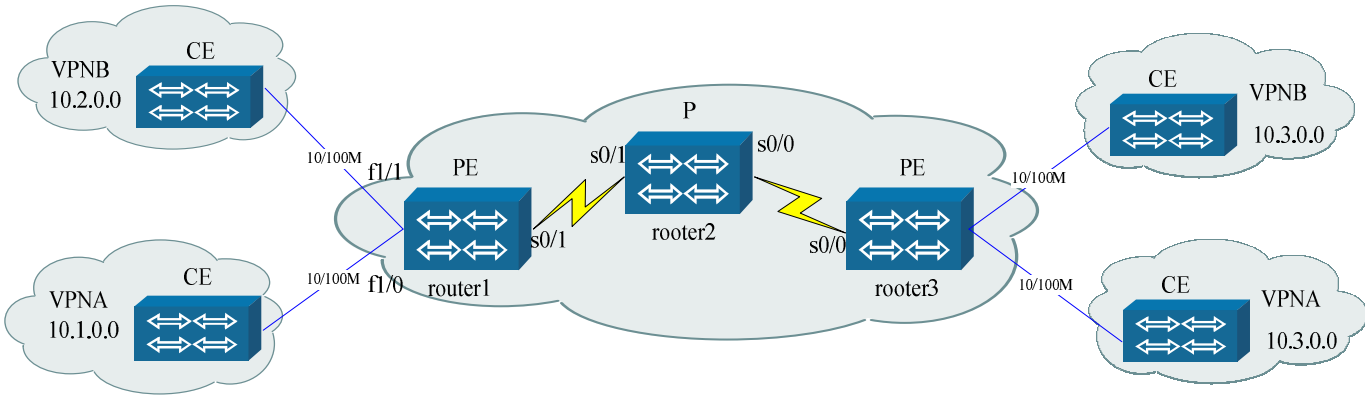
```
no mpls route-cache
```

(Command mode)The interface configuration mode.

🕮 **Note:**

The mpls fast switching is turned on by default, The form no of this command is used to disable this function.

MPLS\VPN Configuration Example



🕮 **Illustration:**

In the configuration figure above, router1 and router3 are PE devices, and router2 is a P device. P\PE devices construct the MPLS backbone network, in which the IGP routing protocol OSFP is running.

IBGP is running between two PE devices that respectively connect with two different networks----VPNA\VPNB. Via BGP announcing the VRF table, the network vrf_a in router1 interconnects with the network vrf_a in router3, and the network vrf_b in router1 interconnects with the network vrf_b in router3. VPNs are realized via MPLS\BGP.

The concrete configuration of Router1 is as follows:

Command	Task
Router1(config)# mpls ip	Run MPLS.
Router1(config)# ip vrf vrf_a	Create a vrfa
Router1(config -vrf)# rd 1:1	Configure the route descriptor.
Router1(config -vrf)# route-target export 1:1	Set properties of the destination VPN.
Router1(config -vrf)# route-target import 1:1	Set properties of the destination VPN.
Router1(config -vrf)#exit	
Router1(config)# ip vrf vrf_b	Create a vrfb.
Router1(config -vrf)# rd 2:2	Configure the route descriptor.
Router1(config -vrf)# route-target export 2:2	Set properties of the destination VPN.
Router1(config -vrf)# route-target import 2:2	Set properties of the destination VPN.
Router1(config -vrf)#exit	
Router1(config)# interface loopback0	Configure the loopback address with 12.12.12.12.

Router1 (config-if-loopback0)# ip address 12.12.12.12 255.255.255.255	
Router1 (config-if-loopback0)# interface fastethernet 1/0	
Router1 (config-if-fastethernet1/0)# ip vrf forwarding vrf_a	Add the interface into the vrfa.
Router1 (config-if-fastethernet1/0)# ip address 10.1.1.1 255.255.0.0	Configure the IP address.
Router1 (config-if- fastethernet1/0)# interface fastethernet 1/1	
Router1 (config-if-fastethernet1/1)# ip vrf forwarding vrf_b	Add the interface into the vrfb.
Router1 (config-if-fastethernet1/1)# ip address 10.2.1.1 255.255.0.0	Configure the IP address.
Router1 (config-if-fastethernet1/1)#interface serial0/1	
Router1 (config -if-serial0/1)# encapsulation ppp	Encapsulate PPP.
Router1 (config -if-serial0/1)# ppp mpls	Use MPLS on the interface (when the link layer protocol is PPP).
Router1 (config -if-serial0/1)# ip address 21.2.1.1 255.255.0.0	
Router1 (config -if-serial0/1)# mpls ip	Use MPLS on the interface.
Router1 (config -if-serial0/1)# exit	
Router1 (config)# router ospf 1	Configure IGP (OSPF).
Router1 (config-ospf)# network 12.12.12.12 0.0.0.0 area 0	
Router1 (config-ospf)# network 21.2.0.0 0.0.255.255 area 0	
Router1 (config-ospf)#exit	
Router1 (config)#router bgp 100	Configure BGP, and the AS number is 100.
Router1 (config -bgp)# no synchronization	Set the asynchronous mode between BGP and IGP.
Router1 (config -bgp)# neighbor 14.14.14.14 remote-as 100	Specify the AS number of the BGP peer.
Router1 (config -bgp)# neighbor 14.14.14.14 update-source loopback0	Specify TCP connection port.
Router1 (config-bgp)# address-family ipv4 vrf	Configure the vrf_a address family.

vrf_a	
Router1(config-bgp-af)# no synchronization	Set the asynchronous mode between BGP and IGP
Router1 (config-bgp-af)# redistribute connected	Redistribute direct routes.
Router1 (config-bgp-af)exit	
Router1 (config –bgp)# address-family ipv4 vrf vrf_b	Configure the vrf_b address family.
Router1 (config-bgp-af)# no synchronization	Set the asynchronous mode between BGP and IGP.
Router1 (config-bgp-af)# redistribute connected	Redistribute direct routes.
Router1 (config-bgp-af)#exit	
Router1 (config-bgp)# address-family vpnv4	Configure the VPN address family.
Router1 (config-bgp-af)# neighbor 14.14.14.14 activate	
Router1 (config-bgp-af)# neighbor 14.14.14.14 next-hop-self	
Router1 (config-bgp-af)# neighbor 14.14.14.14 send-community extended	Send properties of the expanded community to the peer.
Router1 (config-bgp-af)#exit	
Router1 (config-bgp)#exit	

The concrete configuration of Router2 is as follows:

Command	Task
Router2 (config)#mpls ip	Run MPLS
Router2 (config)#interface loopback 0	Configure the loopback address with 13.13.13.13.
Router2 (config-if-loopback0)# ip address 13.13.13.13 255.255.255.255	
Router2 (config-if-loopback0)#exit	
Router2 (config)#interface serial0/0	
Router2 (config-if-serial0/0)#encapsulation ppp	Encapsulate PPP.
Router2 (config-if-serial0/0)# ppp mpls	Use MPLS on the interface (when the link layer protocol is PPP).
Router2 (config-if-serial0/0)# ip address 21.1.1.2 255.255.0.0	
Router2 (config-if-serial0/0)# mpls ip	Use MPLS on the interface
Router2 (config-if-serial0/0)# exit	
Router2 (config)#interface serial0/1	
Router2 (config-if-serial0/1)# encapsulation ppp	Encapsulate PPP.
Router2 (config-if-serial0/1)# ppp mpls	Use MPLS on the interface (when the link layer protocol is PPP).
Router2 (config-if-serial0/1)# ip address 21.2.1.2 255.255.0.0	
Router2 (config-if-serial0/1)# mpls ip	Use MPLS on the interface
Router2 (config-if-serial0/1)# exit	
Router2 (config)#router ospf 1	Configure IGP (OSPF)
Router2 (config-ospf)# network 21.2.0.0 0.0.255.255 area 0	
Router2 (config-ospf)# network 21.1.0.0 0.0.255.255 area 0	
Router2 (config-ospf)# network 13.13.13.13 0.0.0.0 area 0	
Router2 (config-ospf)# exit	

The concrete configuration of Router3 is as follows:

Command	Task
Router3 (config)#mpls ip	Run MPLS.
Router3 (config)#ip vrf vrf_a	Create a vrfa.
Router3 (config-vrf)# rd 1:1	Configure the route descriptor.
Router3 (config-vrf)# route-target export 1:1	Set properties of the destination VPN.
Router3 (config-vrf)# route-target import 1:1	Set properties of the destination VPN.
Router3 (config-vrf)# exit	
Router3 (config)#ip vrf vrf_b	Create a vrfb.
Router3 (config-vrf)# rd 2:2	Configure the route descriptor.
Router3 (config-vrf)# route-target export 2:2	Set properties of the destination VPN..
Router3 (config-vrf)# route-target import 2:2	Set properties of the destination VPN.
Router3 (config-vrf)# exit	
Router3 (config)#interface loopback0	Configure the loopback address with 14.14.14.14.
Router3 (config-if-loopback0)# ip address 14.14.14.14 255.255.255.255	
Router3 (config-if-loopback0)# exit	
Router3 (config)#interface fastethernet2/2	
Router3 (config-if-fastethernet2/2)# ip vrf forwarding vrf_a	Add the interface into the vrfa.
Router3 (config-if-fastethernet2/2)# ip address 10.3.1.1 255.255.0.0	Configure the IP address.
Router3 (config-if-fastethernet2/2)# exit	
Router3 (config)#interface fastethernet2/3	
Router3 (config-if-fastethernet2/3)# ip vrf forwarding vrf_b	Add the interface into the vrfb.
Router3 (config-if-fastethernet2/3)# ip address 10.3.1.1 255.255.0.0	Configure the IP address.
Router3 (config-if-fastethernet2/3)# exit	
Router3 (config)#interface serial1/0	
Router3 (config-if-serial1/0)# encapsulation ppp	Encapsulate PPP.
Router3 (config-if-serial1/0)# ppp mpls	Use MPLS on the interface (when the link layer protocol is PPP).
Router3 (config-if-serial1/0)# ip address 21.1.1.1 255.255.0.0	
Router3 (config-if-serial1/0)# mpls ip	Use MPLS on the interface.

Router3 (config-if-serial1/0)# exit	
Router3 (config)#router ospf 1	Configure IGP (OSPF).
Router3 (config-ospf)# network 21.1.0.0 0.0.255.255 area 0	
Router3 (config-ospf)# network 14.14.14.14 0.0.0.0 area 0	
Router3 (config-ospf)# exit	
Router3 (config)#router ospf 2 vrf vrf_a	Configure the dynamic routing protocol between PE (router3) devices and CE (VPNA) devices.
Router3 (config-ospf)# network 10.0.0.0 0.255.255.255 area 0	
Router3 (config-ospf)# redistribute bgp 100	Redistribute the BGP_100 route.
Router3 (config-ospf)# exit	
Router3 (config)#router bgp 100	Configure BGP, and the AS number is 100.
Router3 (config-bgp)# no synchronization	Set the asynchronous mode between BGP and IGP.
Router3 (config-bgp)# neighbor 12.12.12.12 remote-as 100	Specify the AS number of the BGP peer.
Router3 (config-bgp)# neighbor 12.12.12.12 update-source loopback0	Specify aTCP connection port.
Router3 (config-bgp)# address-family ipv4 vrf vrf_a	Configure the vrf_a address family.
Router3 (config-bgp-af)# no synchronization	Set the asynchronous mode between BGP and IGP.
Router3 (config-bgp-af)# redistribute ospf 2 vrf vrf_a	Redistribute the OSPF (vrf_a) route.
Router3 (config-bgp-af)# redistribute connected	Redistribute direct routes.
Router3 (config-bgp-af)# exit	
Router3 (config-bgp)# address-family ipv4 vrf vrf_b	Configure the vrf_b address family.
Router3 (config-bgp-af)# no synchronization	Set the asynchronous mode between BGP and IGP.
Router3 (config-bgp-af)# redistribute connected	Redistribute direct routes.
Router3 (config-bgp-af)# exit	
Router3 (config-bgp)# address-family vpnv4	Configure the vpn address family.
Router3 (config-bgp-af)# neighbor 12.12.12.12 activate	
Router3 (config-bgp-af)# neighbor 12.12.12.12 next-hop-self	
Router3 (config-bgp-af)# neighbor 12.12.12.12 send-community extended	Send the properties of the expanded community to the peer.

Router3 (config-bgp-af)# exit	
Router3 (config-bgp)# exit	

MPLS Monitoring & Testing

- show mpls cache

Display mpls high speed forwarding list.

```
show mpls cache
```

(command mode)privileged user configuration mode

- show mpls forwarding-table

Display mpls forwarding list information.

```
show mpls forwarding-table [address mask-len [detail] | detail]
```

Syntax	Description
Address	Display forwarding list ip address label information
mask-len	Mask length
Detail	Detailed information

(command mode)privileged user configuration mode.

- show mpls forwarding-table interface

Display mpls forwarding information according to exit interface.

```
show mpls forwarding-table interface interface number [detail]
```

Syntax	Description
interface number	Interface name
detail	Detailed information

(command mode)privileged user configuration mode

- show mpls forwarding-table lables

Display mpls forwarding information according to designated label range.

```
show mpls forwarding-table labels low-label [high-label] [detail]
```

Syntax	Description

low-label	Label range minimum value
high-label	Label range maximum value
detail	Detailed information

(command mode)privileged user configuration mode

- show mpls forwarding-table next-hop

Display mpls forwarding information according to next hop address.

```
show mpls forwarding-table next-hop address [detail]
```

Syntax	Description
address	Next hop address
detail	Detailed information

(command mode)privileged user configuration mode

- show mpls forwarding-table vrf

Display designated vrf mpls forwarding list information.

```
show mpls forwarding-table vrf vrf-name [address mask-len
[detail] | detail]
```

Syntax	Description
vrf-name	Designate vrf name
address	Display forwarding list designated ip address label information.
mask-len	Mask length
detail	Detailed information

(command mode)privileged user configuration mode

- show mpls interface

Display interface mpls information.

```
show mpls interface
```

(command mode)privileged user configuration mode

- show mpls ldp

Display ldp information

```
show mpls LDP [database | discovery | interface | neighbor |
parameters]
```

Syntax	Description
database	Display ldp label information data base

discovery	Display ldp neighbor information
interface	Display interface ldp status
neighbor	Display ldp neighbor information
parameters	Display ldp configured parameter information

(command mode)privileged user configuration mode

- show mpls statistics

Display mpls statistics information.

```
show mpls statistics
```

(command mode)privileged user configuration mode

- debug mpls

Enable mpls debugging information.

```
debug mpls {event | fastswitch | mfib | packet }
```

Syntax	Description
event	Enable mpls event debugging information switch.
fastswitch	Enable mpls high forwarding debugging information switch.
mfib	Enable mpsl forwarding information list debugging information switch.
packet	Enable mpals forwarding packet debugging information switch.

(command mode)privileged user configuration mode

- debug mpls ldp

Enable mpls ldp debugging information switch.

```
debug mpls  ldp {all | binding | errors | events | packet |
policy | route | state | task | timer}
```

Syntax	Description
all	Enable mpls ldp all debugging information switch.
binding	Enable mpls ldp label binding debugging information switch.
errors	Enable mpls ldp error debugging information switch.
events	Enable mpls ldp event debugging information switch.
packet	Enable mpls ldp packet debugging information switch.
policy	Enable mpls ldp policy debugging information switch.
route	Enable mpls ldp routing changing debugging information switch.
state	Enable mpls ldp state debugging information switch.
task	Enable mpls ldp task debugging information switch.
timer	Enable mpls ldp timer debugging information switch.

(command mode)privileged user configuration mode

SNMP Configuration

This chapter explains the configuration of router SNMP agent server and RMON(remote network monitoring) .

SNMP agent server configuration

SNMP (Simple Network Management Protocol) is a standard protocol to manage the Internet. Its purpose is to assure that the management information can be transmitted between the Network Management Station and the managed equipment——agent. It is convenient for the system manager to manage the network system.

SNMP adopts the tree labeling method to number each managed element and insures the number is exclusive. About the detailed information on SNMP protocol, refer to the TCP/IP data.

Command	Description
snmp-server start	Activate SNMP network management.
snmp-server community	Set the SNMP community name.
snmp-server contact	Set the contact mode of the device manager.
snmp-server context	Set V3 context
snmp-server enable	Enable snmp parameter configuration
snmp-server host	Set the host name or IP address of the network management station receiving SNMP trap.
snmp-server location	Set the location of the device.
snmp-server view	Set the network management view.
snmp-server enable traps	Enable to send specified type of traps
snmp-server AddressParam	Set the address parameter.
snmp-server TargetAddress	Set related destination address parameter aaa.
snmp-server engineID	Set the engine.
snmp-server engineGroup	*Set engine group
snmp-server trap-source	Set sending trap source address
snmp-server send	*Test sending a notify for network management
snmp-server group	Set the group.
snmp-server notify	Set notify-message.
snmp-server proxy	Set the proxy for transmitting packet.
snmp-server user	Set the user.
snmp-server keepalive	Set the keepalive packet.

SNMP agent Server Configuration

- **SNMP proxy start**

```
router(config)#snmp-server start
```

After starting the equipment, SNMP agent server is disable by default, and so we should use this command to start SNMP agent server. When SNMP agent server is starting, a default and public will be configured automatically.

```
Delete SNMP on router: (disable network management proxy process)
```

The configuration of disabling SNMP on router is as following:
Router(config)#no snmp-server start

After executing this command, the SNMP agent server on router is disabled, and the network management software cannot manage the router via SNMP.

- **Configure administrator contact mode and the location of the equipment**

```
Router(config)#snmp-server contact <LINE> configure the contact mode.
Router(config)#snmp-server location <LINE> configure location of the equipment
```

The network working station can get the contact and location for the management of the router. And the default configuration is router company name and address.

- **View configuration**

```
router(config)#snmp-server view view-name oid-string {include|exclude}
```

Command	Description
view view-name	Configure view name
oid-string	Designate the vie OID
{include|exclude}	Designate view attribute

SNMP enables a view: default, the OID is: 1.3.6.1, include: including all the objects in the sub-tree 1.3.6.1 of MIB, exclude: remove all the objects.

- **Configuring Community Name:**

router(config)#snmp-server community community-name [view view-name [{rolrw}] [access-list]]

Command	Description
community community-name	Set the community name.
view view-name	Specify the view related to the community name.
{ro|rw}	Specify the operation right of the community name.
access-list	Specify the access control list or name of the community name.

🕮 Note:
The parameter community-name is used to specify the community name that is added to the router. Usually, the community name should be the same as that configured on the network management station, or else the network management station has no way to perform any operation to the

router.
The parameter { ro | rw} is used to set the network management station's rights to operate the router. The parameter ro means read-only and rw means reading/writing.
The parameter view is used to specify the view scope for the community. Signamax router can do without the configuration of the parameter view (it can do with the default).
The parameter access-list is the access control list that is used to perform the access control of hosts in the community. So, nothing but those hosts that are in the same community with the router and permitted by the router's access control list can access the router. (About the detailed information, refer to Signamax router access control module)

For example:
Add the community public to the router, and then set the reading/writing right to operate the router for the network management station whose community name is public:
router(config) #snmp-server community public rw
🕮 Note:
After starting up the router, you should configure the community for it, or else, the network management station has no way to manage the router by means of snmpv1/v2c;
If you want to perform writing operations on the router, such as upgrading a program, backing up the configuration file, the parameter < ro/rw/view > should be set as rw(reading/writing).

- **Configuring the router to send traps message:**

The configuration of sending traps message on the router is described as follows:

```
Router (config)#snmp-server host ip/name [traps] [community community-name] [version {1|2}]
```

Command	Description
host ip/name	Specify the IP address and name of the network management station.
traps	Specify the sending type as traps.
community community-name	Specify the community name.
version {1|2}	Specify the version number of the trap message.

🕮 Note:
The parameter < ip/name > represents the destination name or IP address to which the traps message will be sent. Usually, it is the IP address or name of the host on which the network management application has been installed. It is noticeable that the trap message is the message the router forwardly sends to the host on which the network management application has been installed.
If parameters following host, such as traps, community-name and version, are not configured, the system will adopt the default configuration: type—traps, community-name—public and version—2.

- **Configure sending traps information interface:**

The configuration is as following:

```
Router(config)#snmp-server trap-source ip-address
```

Command	Description
ip-addres	Designate sending trap information interface ip address.

- **Configure sending traps information content:**

The configuration is as following:

```
Router(config)# snmp-server enable traps [bgp] [dlsw] [frame-relay] [isdn] [ospf] [pim] [rsvp] [snmp] [x.25]
```

🕮 **Note:**

Configure the sending trap content, the SNMP agent provides the trap information of bgp/dlsw/ frame-relay / isdn / ospf / pim / rsvp / snmp / x.25 protocols. Execute the command to receive the trap. If parameters of enable traps are not configured, the default is to send all trap information.
For example,
The sending coldstart type trap information configuration command is:

```
Router(config)#snmp-server enable traps snmp coldstart
```

- **Configuring SNMPv3 engine ID:**

```
router(config)#snmp-server engineID ?
```

Command	Description
remote	Configuring the remote engine ID.
local	Configuring the local engine ID.

Note:

Each SNMPv3 entity comprises an engine (also called local engine), and snmpEngineID is used to exclusively identify an SNMPv3 entity in a management domain. Moreover, when sending an advertisement or forward a message, the SNMPv3 need know the engineID of the remote destination SNMP entity. So, the remote engineID need be configured, and the destination IP address and UDP port number need be specified for the engineID.

```
router(config)#snmp-server engineID local engineID
```

Command	Description
engineID	The value of the local engineID.

For example:

Use the following command to configure the local engineID as 12345678:

```
router(config)#snmp-server engineID local 12345678
```

```
router(config)#snmp-server engineID remote ip-address port-num engineID [engineGroup]
```

Command	Description
ip-address	The IP address of the destination entity.
port-num	The UDP port-number of the destination entity.
engineID	The value of the remote engineID.
[engineGroup]	The engine group name.

Note:

When configuring automatic proxy forwarding, you many know no IP address of the surrogated equipment. Here, you do nothing but input 0.0.0.0 at the location of ip-address. Moreover, the automatic proxy forwarding cannot work without the keepalive mechanism.

For example:

```
Use the following command to configure the destination entity: IP address—1.1.1.1, port-number—162,engineID—abcdef1234:
router(config)#snmp-server engineID remote 1.1.1.1 162 abcdef1234
```

```
router(config)#snmp-server engineGroup groupname usrname {noauth |auth |priv}
```

Command	Description

groupname	The name the engine group.
usrname	The user name.
{noauth |auth |priv}	The security level of the username :no-authentication, authentication but encryption, authentication and encryption.

🕮 Note:

The foregoing command is used to configure the automatic proxy forwarding. Before the command is configured, related username need be configured in advance. The function of the command is to relate several engines (SNMPv3 entities) to an engine group. One user can be specified for each engine group. In this way, the username can be used to access any engine of the engine group. The parameter {noauth |auth |priv} is used to describe the security level of the username, and should be consistent with the username.

For example:

Use the following command to configure an engine group: group-name—group1, username—user1, security level—auth:

router(config)#snmp-server engineGroup group1 user1

- **Configuring an SNMPv3 group:**

Router(config)#snmp-server group *group-name* v3 {noauth|authnopriv|authpriv}

[notify notify-view] [read read-view] [write write-view]

Command	Description
group-name	The group name.
v3	The security mode of the group is v3.
noauth	The security level of the group is no-authentication no-encryption.
authnopriv	The security level of the group is authentication no-encryption.
authpriv	The security level of the group is authentication encryption.
notify notify-view	Configure the notify-view of the group.
read read-view	Configure the read-view of the group.
write write-view	Configure the write-view of the group.

🕮 Note:

In the SNMPv3 group, map a group-name, security information and message type (read, write or notify) into a MIB view. A given MIB view can determine whether a managed object does not permit of being accessed. At the same time, several SNMPv3 users can be related to the group. The configuration of the group can strengthen the SNMPv3 access control.

For example:

Use the following command to configure a group: group name—group1, security level—authentication encryption, notify-view—view3, read-view—view1, and write-view—view2.

```
Router(config)#snmp-server group group1 v3 authpriv read view1 write view2 notify view2
```

- **Configuring SNMPv3 user:**

```
Router(config)#snmp-server user user-name group-name [remote ip-address portnum] v3 [auth {md5|sha} password [encrypt des password]]
```

Syntax	Description
user-name	The username.
group-name	The name of the group the user belongs to.
remote ip-address portnum	The IP address of and port-number of the remote user.
v3	The user security mode is v3.
auth {md5|sha} password	Configure the user authentication protocol as MD5 or SHA, and specify the password.
encrypt des password	Configure the user encryption protocol as DES, and specify the password.

📖 Note:

Configure an USM-based (User security mode) SNMPv3 user, and save the authentication and encryption information of each user. Notice that the encryption protocol cannot be configured until the authentication protocol is configured. For a remote user ("Remote" is relative to the local SNMPv3 entity. If the local SNMPv3 entity wants to communicate with the other entity, then the other entity is called "remote" SNMPv3 entity. This will be involved in Notify and Proxy.), the IP address and UDP port-number are still specified. When configuring the remote user, you should configure the engineID of the remote SNMP entity related to the user. Moreover, each user should be related to a group. Only in this way can a security model and security name be mapped into a group name by means of the view-based control access 。

For example:

Use the following command to configure a user: the user name—user1, related group name-group1, security level—authentication encryption, authentication protocol—MD5, password—123456, encryption protocol—DES, password—234567.

Router (config)# snmp-server user user1 group1 v3 auth md5 123456 encrypt des 234567

Use the following command to configure a remote user: the user name—user2, IP address—1.1.1.1, port-number—162, security level—authentication encryption, authentication protocol—SHA, password—123456, encryption protocol—DES, password—123456.

router(config)#snmp-server user user2 group1 remote 1.1.1.1 162 v3 auth sha 123456 encrypt des 123456

- **Configure SNMPv3 context:**

```
Router(config)#snmp-server context context—name
```

📖 **Note:**

The context configuration is one of parameters of snmp V3, but it doesn't

affect the use of snmp V3.

- **Configuring SNMPv3 Address Parameter:**

```
router(config)#snmp-server AddressParam address-name v3 user-name {noauth | authnopriv | authpriv}
```

Syntax	Description
address-name	The address name.
paramIn	Configure dynamic proxy forwarding
v3	The message processing model v3 used for the generation of SNMP messages.
user-name	The user name related to the address parameter.
noauth	The security level is no-authentication no-encryption.
authnopriv	The security level is authentication no-encryption.
authpriv	The security level is authentication encryption.

Note:

Some MIB tables have been defined in SNMPv3 so as to configure the destination to which the notify-message is sent. The address parameter table defines the SNMP parameters that should be used when a message (notification) is generated.
For example:

```
Use the following command to configure the address parameter: parameter name—addparam1, message processing model—v3, related user name (also called security name)—user1, security level—authpriv.

router(config)#snmp-server AddressParam addparam1 v3 user1 authpriv
```

- **Configuring the destination address table:**

```
router(config)#snmp-server TargetAddress target-name ip-address port-num address-param taglist time-out retry-num
```

Syntax	Description
target-name	The address name.
ip-address	The destination address.
port-num	The UDP port-number.
address-param	The address parameter name.
taglist	The tag list.
time-out	The timeout.
retry-time	The times of retransmission.

Note:

The destination address table is used to specify the destination that is used when the SNMP message is generated. (Notice that TargetAddress and AddrssParam cannot be configured until the local SNMPv3 entity accesses the other (remote) SNMPv3 entity). What you need know is: address-param is the address parameter name that has been configured in the address parameter table; taglist, which can be configured with

multiple values spaced by commas, is used to identify the notify-message and forward messages to the other destination address.
For example:

```
Use the following command to configure the destination address table: the addressname—target1, IP address—1.1.1.1, UDP port-number—162, related address parameter name—addparam1, the tag-table—tag1 and tag2, timeout—2 seconds, try-time—2.

router(config)#snmp-server TargetAddress target1 1.1.1.1 162 addparam1 tag1,tag2 2 2
```

- **Configuring notification:**

Use the following command to perform the configuration of SNMPv3: configure the notification parameter table, notification filtering table and notification configuration table.

```
router(config)#snmp-server notify ?
```

Command	Description
filter	Configure the filtering table of the notification.
notify	Configure the notification parameter table.
profile	Configure the notification configuration table.

Thereinto:
The notification parameter table is used to specify the destination address to which the notification message is sent. Whether the notification message is sent to a destination address depends on whether the created filter comprises the destination address.
The notification filtering table has defined a filter that is used to determine whether the notification message is sent to the destination address.
The notification configuration table is used to relate the foregoing address parameters to the notification parameter table.
About the detailed information about SNMPv3's fundamentals and functions, refer to related data about the SNMP protocol.

```
router(config)#snmp-server notify notify notify-name taglist inform
```

Command	Description
notify-name	The notification name, used to index the unique identification of the notification table.
taglist	The tag value, related to the tag list configured in the address table.
inform	Specify the type of the notification message as inform.

🕮 **Note:**

In SNMPv3, the destination address need be specified when a notification is sent. Whether the notification message can be sent to a destination address depends on whether the created filter comprises the destination address. About the detailed information about SNMPv3 notification, refer to related technical manuals.

For example:

```
Use the following command to configure a notification message: the name—notify1, the tag-value—tag1.

router(config)#snmp-server notify notify notify1 tag1 inform

router(config)#snmp-server notify notify filter-name oid-subtree {exclude|include}
```

Command	Description
filter-name	The name of the notification filter
oid-subtree	MIB sub-tree.
exclude	The object under the MIB sub-tree cannot send notification message.
include	The object under the MIB sub-tree can send notification message.

🕮 **Notice:**

The notification filtering table has defined a filter that can determine whether a message can be sent to the destination address.

For example:

```
Use the following command to configure a notification filter: the name—filter1, the MIB sub-tree—1.3.6.1, the type—include.

router(config)#snmp-server notify filter filter1 1.3.6.1 include


router(config)#snmp-server notify profile filter-name address-param
```

Command	Description

filter-name	The name of the notification filter
address-param	The address parameter name.

🕮 **notice:**

The notification configuration table is used to relate the address parameter table to the notification filtering table. If both a notification filtering table and a notification configuration table are defined the SNMP proxy can detect the object OID when sending a notification message. If the object OID is contained in the defined MIB sub-tree, the notification message will be sent, or else, the message cannot be sent.

For example:

```
Use the following command to configure the notification configuration table: the name—filter1, the address parameter name—addparam1.

router(config)#snmp-server notify profile filter1 addparam1

router(config)#snmp-server proxy proxyname {inform | trap |read | write} engineId address-param target-addr
```

Command	Description
proxyname	The forwarding configuration name.
{inform | trap |read | write}	The message property that need be matched.
engineId	The engine ID that need be matched.
address-param	The address parameter name that need be matched.
target-addr	The destination address name for forwarding.

🕮 **Note:**

The goal of SNMP proxy forwarding is to forward the SNMP request to other SNMP entity. To do it, it may be necessary to convert one version to another version or convert one transmission domain to another transmission domain. The SNMP on Signamax equipment can realize nothing but the v3-to-v3 forwarding, is applied to the conversion from one transmission domain to another transmission domain. Additionally, two message properties trap and inform in the table above cannot be supported.

For example:

```
Use the following command to configure a proxy forwarding item: the name—proxy1, the address parameter name—param1, the destination address name—addr1, the engine—1111, message property—read.

router(config)#snmp-server proxy proxy1 read 1111 param1 addr1


router(config)#snmp-server keepalive destination ip-addr
```

Command	Description
ip-addr	Configure the destination address of the sent keepalive message.

For example:

Use the following command to configure the destination addresses of two keepalive messages: 202.1.25.1 and 179.68.0.4:

```
router(config)#snmp-server keepalive destination 202.1.25.1
router(config)#snmp-server keepalive destination 179.68.0.4

router(config)#snmp-server keepalive interface if-name
```

Command	Description
if-name	Configure the interface address carried by the sent keepalive message.

A keepalive message can carry only one interface address. If the interface address has not been configured, the address of the interface fastethernet0 is carried by default. The keepalive message is used to maintain the SNMP proxy forwarding table. For a configured proxy forwarding item, if no related keepalive message is received in a period of time, the proxy forwarding item will be discarded.

For example:

Use the following command to configure a keepalive message: carry the address of the interface ethernet0:

```
router(config)#snmp-server interface ethernet0
```

```
router(config)#snmp-server keepalive interval { interval-time | default }
```

Command	Description
interval-time	Configuring the interval of sending a keepalive message.
Default	Adopt the default interval of sending a keepalive message: 10 seconds.

For example:

Use the following command to configure the interval of sending a keepalive message as 6 minutes.

```
router(config)#snmp-server keepalive interval 360
```

```
router(config)#snmp-server notify interface interface-name [with {hostname | saId | engineId}]
```

Command	Description
interface-name	Configure the interface address that is carried by the sent keepalive message.
{hostname | said | engineId}	Configure whether the host name, channel ID and engineID are carried by the keepalive message.

Note:

The command is used to be compatible with the old version of keepalive messages that adopt the notify format. The snmp-server keepalive series commands can be used to configure the new version of keepalive messages.
The command snmp-server host is used to determine the destination address of the keepalive message adopting the notify format.
SaId is the identification of the security alliance. About the detailed

information about security alliance, refer to related IPsec technical documents.
For example:
Use the following command to configure a keepalive message: to carry the address of the interface ethernet0, engineID and host name information.

```
router(config)#snmp-server notify interface ethernet0 with engineId hostname
```

```
router(config)#snmp-server notify interval { interval-time | default }
```

Command	Description
interval-time	Configure the interval of sending a keepalive message.
Default	Adopt the default interval of sending a keepalive message: 10 seconds.

🕮 **Note:**

The command is used to be compatible with the old version of keepalive messages. The snmp-server keepalive series commands can be used to configure the new version of keepalive messages.
The interval is independent of the value of the command snmp-server keepalive interval, and there exist no mutual influence between them.
For example:
Use the following command to configure the sending interval of a keepalive message as 3 minutes:

```
router(config)#snmp-server notify interval 180
```

```
router#show snmp-server engineID
```

🕮 **Note:**

The command is used to display the engineID (including both remote engineID and local engineID) that has been configured on the router:
router#show snmp-server engineID
Local engine ID: 12345678
IPAddress: 1.1.1.1.0.162 remote engine ID: abcdef1234
Information above indicates that two engineIDs have been configured on the router: one is the local engineID and another is the remote engineID.

router#**show snmp-server group**

🕮 **Note:**

The command is used to display the SNMP user group that has been configured on the router:

```
router#show snmp-server group
```

GroupName: group1 SecModel:v3,SecLevel:authpriv

```
    Read      View: readview
```

```
    Write     View: writeview

    Notify    View: notifyview
```

A SNMP user group has been configured on the router, the group name—group1, the security model—v3, the security level—authentication encryption, the read-view—readview, the write-view—writeview, and the notification view—notifyview.

```
router#show snmp-server user
```

🕮 **Note:**

The command is used to display the users that have been configured on the router:

router#show snmp-server user

SNMP User List:

```
     User Name    SecLevel      Status        EngineID

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

         user1      AuthPriv    active        12345678

         user2      AuthPriv    active        abcdef1234
```

Two users have been configured on the router: the security level—authentication encryption, related engine ID—12345678/ abcdef1234, which can indicate that the user1 is the local user and the user2 is the remote user.

```
router#show snmp-server AddressParams
```

🕮 **Note:**

The command is used to display the address parameter table that has been configured on the router:

```
router#show snmp-server AddressParams

SNMP TargetAddressParam List:

     ParamName        User Name            MP_model     SecurityModel
SecurityLevel

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

    addparam1            user2                  v3               USM
authpriv
```

Configure the address parameter on the router; the name—addparam1, related user—useer2, the message processing mode—v3, the security model—USM, the security level—authentication encryption.

```
router#show snmp-server TargetAddress
```

🕮 **Note:**

The command is used to display the destination address table that has been configured on the router:

```
router#show snmp-server TargetAddress
TargetAddressList:
================================================
Name:       target1
Address:    1.1.1.1.0.162
ParamName:  addparam1
TagList:    tag1 tag2
TimeOut(sec) :2
RetryCount    :2
================================================
A destination address item has been configured on the router: the
name—target1, the destination address—1.1.1.1, UDP port-number—162,
the taglists—tag1 and tag2, the timeout—2 seconds, try-time—twice.
```

```
router#show snmp-server notify notify
```

🕮 **Note:**

The command is used to display the notification table configured on the router.

```
router#show snmp-server notify notify
SNMP Notify List:
      Name              Tag           Type
=========================================================
   notify1              tag1          inform
A notification table has been configured on the router: the name—
notify1, related tag—tag1, the message type—inform
router#show snmp-server notify filter
🕮 Note:
The command is used to display the notification filtering table
configured on the router.

router#show snmp-server notify filter
SNMP Notify Filter List:
          Name         FilterSubtree       Type
=============================================================
          filter1        1.3.6.1           include
A notification filter table filter1 has been configured on the
router, including all nodes under the MIB sub-tree 1.3.6.1.
router#show snmp-server notify profile
```

🕮 **Note:**

The command is used to display the notification configuration table configured on the router.

router#show snmp-server notify profile

```
SNMP Notify Profile List:
          Name           ParamName           Status
============================================================
       filter1          addparam1            Active
```

From the configuration above, you can know: the notification filter filter1 is related to the address parameter name addparam1.

router#show snmp-server engineGroup

Note:

The command is used to display the engine group configured on the router.

Snmp Debugging command :

Command	Description
Debug snmp-server all	Debug all snmp, excluding response
Debug snmp-server groupget	Debug SCALAR variables GET
Debug snmp-server groupset	Debug SCALAR variables SET
debug snmp-server response	The response of last operation
Debug snmp-server tblgetnext	Debug TABULAR variables GETNEXT
Debug snmp-server tblset	Debug TABULAR variables SET
Debug snmp-server trap	Debug TRAP

Remote Network Monitoring (RMON)

Main contents of this section:

- Brief introduction of RMON
- RMON basic command description
- RMON configuration example

Brief introduction of RMON

RMON defines a set of MIB: standard network monitoring function and interface, to make the communication between SNMP management terminal and remote monitor.

RMON MIB has 10 groups:

·statistics:maintenance of use and error statistics.

·history:recording the sample of statistics information from statistics group.

·alarm:configure administration control user sampling time interval and the over threshold of RMON

proxy.

·host:the flow of each host to this subnet.

·hostTopN:host statistics information.

·matrix:show the error and usage information in the form of matrix.

·filter:permit the monitor to observe the filtering data packet.

·capture:how to send management data to administration control platform.

·event:the event list of RMON proxy.

·tokenRing:maintain the subnet statistics and configuration information.

🕮 **Note:**

The router ly supports alarm group and event group.

RMON basic command description

Command	Description
router(config)#rmon	Activate the RMON task.
router(config)#no rmon	Cancel the RMON task.
router(config)#rmon alarm <1-65536> <OID> <1-65536> absolute/delta risingthreshold <0-2147483647> <1-65536> fallingthreshold <0-2147483647> <1-65536>	Configure the RMON alarm.
router(config)#rmon event <1-65536> description word log <1-65536> owner <word> trap <word>	Configure the RMON event.

The procedure to configure the remote monitoring RMON on the MP router is described as follows:

Step 1: Start the remote monitoring RMON.

router (config)#**rmon < CR >**

Step 2: Configure relative alarms and objects that are remotely monitored.

router(config)#rmon alarm <1-65536> <OID> <1-65536> absolute/delta risingthreshold <0-2147483647> <1-65536> fallingthreshold <0-2147483647> <1-65536>

🕮 Note:

The parameter <1-65536> behind rmon alarm is the serial number of the alarm;

The parameter <OID> is the object that is remotely monitored (an index need be added behind the object oid). The object can be represented with an oid sequence or an oid alias, and the following parameter <1-65536> is the time interval to sample the value of the parameter <OID> ;

The parameter absolute/delta indicates that the type of sampling is of

the absolute/relative value ;

The parameter <0-2147483647> behind the parameter risingthreshold is the rising threshold value, and the parameter <1-65536> indicates the serial number of the event that arises when the rising threshold value is triggered (the default value is 1) ;

The parameter <0-2147483647> behind the parameter fallingthreshold is the falling threshold value, and the parameter <1-65536> indicates the serial number of the event that arises when the falling threshold value is triggered (the default value is 1);

At present, the rmon has only realized monitoring the 10th –21st objects in the interface table (ifTable) of the standard MIB. The object alias ifEntry of the interface table has been generated automatically in the OID table when the system starts up. About some information about supporting OID variable, refer to the command router# show rmon alarm supportVariable.

Step 3: Configure the action that will be implemented proportionally when the remote monitoring RMON is triggered.

router(config)#rmon event <1-65536> description word log <1-65536> owner <word> trap <word>

📖 Note:

The parameter <1-65536> behind rmon event is the serial number of the event ;

The parameter word behind description is the description of the event. The parameter log <1-65536> and trap <word> represents the event action. The parameter log indicates that the recording is implemented in the log; the parameter <1-65536> represents the maximal number of records ; The parameter trap denotes the remote destination to which the trap information is sent, and the parameter <word> denotes the community name.

The parameter owner <word> denotes the owner of the event.

An example of RMON Configuration

Remotely monitoring the OID object ifEntry.10 on the interface fastethernet0 of the router demands that the ifEntry.10 should be sampled one time every other 5 seconds (Suppose that the interface index of the interface f0 is 1, the object instance is ifEntry.10). The rising threshold value and the falling threshold value are 5000 respectively. If the sampling result triggers the threshold, then the trap message will be sent to the community public. At the same time, it will be recorded in the log on the router (At most 100 records can be recorded.). The detailed configuration is described as follows:

```
 router (config)#rmon
 router (config)#rmon alarm 1 ifEntry.10.1 5 absolute
risingthreshold 5000 1 fallingthreshold 5000 1
 router (config)#rmon event 1 description Monitoring the
number of bytes received on the interface f0
 log 100 trap public
```

RMON debugging commands

The RMON command show is used to display the basic information:

Command	Description
router# show rmon event	Display information about the rmon event that has been configured.
router# show rmon alarm	Display information about the rmon alarm that has been configured.
router# show rmon alarm supportVariable	Examine the monitored objects that rmon supports.

```
show rmon event—to display information about the rmon event that has been set:
router# show rmon event
Output:
Event 1 is active, owned by config
Description : signamax
Event firing causes: log and trap, last fired at 00:25:17
 log entries:
           logIndex           logTime              Description
   ---------------------------------------------------------------
               4              00:12:27        Rising threshold crossing
               5              00:23:26        Rising threshold crossing
               6              00:23:36        Rising threshold crossing
               7              00:23:46        Rising threshold crossing
               8              00:23:56        Rising threshold crossing
               9              00:24:07        Rising threshold crossing
              10              00:24:27        Rising threshold crossing
              11              00:24:47        Rising threshold crossing
              12              00:25:07        Rising threshold crossing
              13              00:25:17        Rising threshold crossing

   Event 2 is active, owned by config
   Description :
   Event firing causes: log, last fired at 00:00:00
   Event 5 is active, owned by config
   Description :
   Event firing causes: trap, last fired at 00:00:00
   Event 6 is active, owned by config
   Description :
```

Event firing causes: nothing, last fired at 00:00:00

After the command has been executed, the result output comprises:

· The example has 4 rmon events that are identified with 1, 2, 5 and 6 respectively.

· The event 1 triggers the event log and the snmp trap. The last event 1 happens after the system has been started for 25 minutes and 17 seconds. The relative log table can display the log index, the time the event happened and simple description of events.

· The event 2 and 5 trigger the event log and snmp trap respectively. At present, the two events haven't happened.

· The event 6 triggers nothing. At present, the event hasn't happened.

```
show rmon alarm——to display information about rmon alarm that
has been set:

router# show rmon alarm
```

- **Output:**
- **Alarm 1 is active, owned by config**
- **Monitoring variable: ifEntry.10.1 Sample interval: 10 second(s)**

- **Taking samples type: delta, last value was 6510**
- **Rising threshold : 50, assigned to event: 1**
- **Falling threshold : 40, assigned to event: 1**
-
- **Alarm 2 is active, owned by config**
- **Monitoring variable: ifEntry.15.1 Sample interval: 50 second(s)**
- **Taking samples type: delta, last value was 156**
- **Rising threshold : 1500, assigned to event: 2**
- **Falling threshold : 500, assigned to event: 5**
-
- **Alarm 4 is active, owned by config**
- **Monitoring variable: ifEntry.16.2 Sample interval: 30 second(s)**
- **Taking samples type: delta, last value was 0**
- **Rising threshold : 300, assigned to event: 6**
- **Falling threshold : 200, assigned to event: 1**

After the command has been executed, the result output comprises:
The example has configured 3 rmon alarms that are identified with 1, 2 and 4 respectively.
The alarm 1 monitors the object instance that is on the interface (whose the index is 1) and related to the 10th object of ifTable (The number of the total bytes received by the fast Ethernet interface, including the delimiter). The sampling interval is 10 seconds and sampling type is the delta. The last sample value of the monitored object is 6510. When the sample rises 50 or falls 40, the event 1 will be triggered (Setting it when configuring the rmon event).
The alarm 2 and alarm 4 respectively monitor the object instances that are on the interfaces (whose the indexes are 1 and 2) and related to the 10th and 16th objects of ifTable. And related sampling interval is 50 seconds and 30 seconds respectively. Related triggered events are: alarm 2---- the rising event is the event 2 and the falling event is the event 5, alarm 4----the rising event is the event 6 and the falling event is the event 1.

- show rmon alarm supportVariable——**To examine information about the OID alias of the monitored objects that are supported by rmon.**

- **Output:**

- **ly support MIB object: (NOTE:be sure to add the index after OID)**
- **ifEntry.[10-21] MIB-II interface table entry**

After the command has been executed, the result output comprises:
At present, rmon has only realized monitoring the 10th –21st objects in the interface table of the standard MIB. The object alias ifEntry of the interface table has been generated automatically in OID alias table when the system starts up.
Remote Network Monitoring (RMON)
RMON instruction set is listed as follows:

Command	Description
router(config)#rmon	Activate the RMON task.
router(config)#no rmon	Cancel the RMON task.
router(config)#rmon alarm <1-65536> <OID> <1-65536> absolute/delta risingthreshold <0-2147483647> <1-65536> fallingthreshold <0-2147483647> <1-65536>	Configure the RMON alarm.
router(config)#rmon event <1-65536> description word log <1-65536> owner <word> trap <word>	Configure the RMON event.

Remote Network Monitoring (RMON)
RMON Instruction Set

Command	Description
router(config)#rmon	Activates the RMON task.
router(config)#no rmon	Cancels the RMON task.
router(config)#rmon alarm <1-65536> <OID> <1-65536> absolute/delta risingthreshold <0-2147483647> <1-65536> fallingthreshold <0-2147483647> <1-65536>	Configures the RMON alarm information.
router(config)#rmon event <1-65536> description word log <1-65536> owner <word> trap <word>	Configures the RMON event information.

Debugging RMON Commands:
The RMON show command Displays basic information:

Command	Description
router# show rmon event	Displays configured rmon event data.
router# show rmon alarm	Displays configured rmon alarm data.
router# show rmon alarm supportVariable	Examines the OID alias data of RMON's monitored objects.

To display information about the RMON event, input router # show rmon event.

```
Output:
Event 1 is active, owned by config
Description: Signamax
Event firing causes: log and trap, last fired at 00:25:17
 log entries:

           logIndex           logTime              Description

   ------------------------------------------------------------------

               4              00:12:27        Rising threshold
   crossing

               5              00:23:26        Rising threshold
   crossing

               6              00:23:36        Rising threshold
   crossing

               7              00:23:46        Rising threshold
   crossing

               8              00:23:56        Rising threshold
   crossing

               9              00:24:07        Rising threshold
   crossing

              10              00:24:27        Rising threshold
   crossing

              11              00:24:47        Rising threshold
   crossing

              12              00:25:07        Rising threshold
   crossing

              13              00:25:17        Rising threshold
   crossing


Event 2 is active, owned by config
Description:
Event firing causes: log, last fired at 00:00:00
Event 5 is active, owned by config
Description:
Event firing causes: trap, last fired at 00:00:00
Event 6 is active, owned by config
Description:
Event firing causes: nothing, last fired at 00:00:00
Notes:
The example has 4 rmon events, respectively identified by 1, 2, 5
and 6.
Event 1 triggers the log and the SNMP alarm.  The relative log table
can display the log index, the time the event happened and a simple
description of events.  (The last Event 1 happened after the system
had been active for 25 minutes and 17 seconds.)
Event 2 and 5 triggers the event log and SNMP alarm respectively.
(In the example, these things haven't been triggered.)
```

```
Event 6 triggers nothing.
To display data about the set rmon alarm, input router# show rmon
alarm
Output:
Alarm 1 is active, owned by config
Monitoring variable: ifEntry.10.1, Sample interval: 10 second(s)
Taking samples type: delta, last value was 6510
Rising threshold: 50, assigned to event: 1
Falling threshold: 40, assigned to event: 1

Alarm 2 is active, owned by config
Monitoring variable: ifEntry.15.1, Sample interval: 50 second(s)
Taking samples type: delta, last value was 156
Rising threshold: 1500, assigned to event: 2
Falling threshold: 500, assigned to event: 5



    Alarm 4 is active, owned by config

    Monitoring variable: ifEntry.16.2, Sample interval: 30 second(s)
Taking samples type: delta, last value was 0
Rising threshold: 300, assigned to event: 6
Falling threshold: 200, assigned to event: 1
```

Notes:
The preceding example has configured 3 rmon alarms, respectively identified by 1, 2 and 4.
Alarm 1 monitors the 10th object whose interface table index is 1 (ie. the total amount of bytes received by the Ethernet interface, including the delimiter). The sampling interval is 10 seconds and sampling type is delta. The last sample value of the monitored object is 6,510. When the sample rises above 50 or falls below 40, event 1 will be triggered (ie. the configuration of the RMON event).
Alarm 2 and Alarm 4 monitors interfaces 15 and 16, whose interface index is respectively 1 and 2. Related sampling interval is respectively 50 seconds and 30 seconds. Related triggered events are: Alarm 2 (ie. the rising event is Event 2 and the falling event is Event 5) and Alarm 4 (ie. the rising event is Event 6 and falling event is Event 1.)
To examine the OID alias data of the monitored objects supported by rmon, input:
show rmon alarm supportVariable

Output:

ly support MIB object: (**NOTE**: be sure to add the index after OID)

ifEntry.[10-21] MIB-II interface table entry

Note: Rmon is only set up to monitor the 10th to 21st objects in the standard MIB interface table. The ifEntry interface table object alias will generate automatically in the OID table when the system restarts.

RMON Configuration example:

Command	Description
router#configure terminal	
router(config)#rmon	Enable RMON
router(config)#rmon alarm 1 1.3.6.1.2.1.2.2.1.10.1 5 absolute risingthreshold 5000 1 fallingthreshold 5000 1	Configure alarm example
router(config)#rmon event 1 description 对接口 f0 的接收字节数进行监控 log 100 trap public	Configure triggering event

IPsec VPN Configuration

IPsec is designed to provide cyptographically-based security for IP. The set of security services offered includes access control, connectionless integrity, data origin authentication, protection against replays (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality. These services are provided at the IP layer, offering protection for IP and/or upper layer protocols.

IPsec VPN is to construct secure information transmission channel of communication parties on public network via IPsec technology. IPsec communication parties authenticate themselves via encryption key management protocol, and negotiate information encryption or other parameters, to construct secure encryption information transmission channel.

Signamax secure router follows IPsec protocol. It realizes the main function, which constructs kinds of VPN, such as Site-to-Site VPN, Dailup VPN, and integrated manages Hub-and-Spoke VPN, to satisfy complex actual application environment requirement.

In the configuration, the system uses default configuration or the user can configures according to the command.

Overview

IPsec Supported Protocol Standard & Secure Service

IPsec provides two kinds of protocol standards to protect IP layer communication, AH(Authenticaion Header) and ESP(Encapsulation Security Payload) .

AH(Authentication Header) provides connectionless integrity, data origin authentication, and an optional anti-replay service. AH

doesn't encrypt the protected data packet.
ESP may provide confidentiality (encryption), and limited traffic flow confidentiality. It also may provide connectionless integrity, data origin authentication, and an anti-replay service. We usually use ESP protocol.

Both AH and ESP are vehicles for access control, based on the distribution of cryptographic keys and the management of traffic flows relative to these security protocols.

IPsec protocol protects a whole IP data packet and some IP packet upper protocol payload.

Security Association,SA

A Security Association (SA) is a simplex "connection" that affords security services to the traffic carried by it. Security services are afforded to an SA by the use of AH, or ESP, but not both. If both AH and ESP protection is applied to a traffic stream, then two (or more) SAs are created to afford protection to the traffic stream. To secure typical, bi-directional communication between two hosts, or between two security gateways, two Security Associations (one in each direction) are required.

A security association is uniquely identified by a triple consisting of a Security Parameter Index (SPI), an IP Destination Address, and a security protocol (AH or ESP) identifier.

Two types of SAs are defined: transport mode and tunnel mode. A transport mode SA is a security association between two hosts. A tunnel mode SA is essentially an SA applied to an IP tunnel. Whenever either end of a security association is a security gateway, the SA MUST be tunnel mode.

The Internet Key Exchange (IKE)

IPsec SA setup has two methods: manual and automated SA management.

Manual management of IPsec SA is complex and cannot support some senior features such as anti-replay. This configuration method is applied to small and static network, but in actual environment, we don't suggest using this method.

IKE is used for automated SA management. It provides smart and convenient configuration, and much higher security.

Setting up IPsec channel via IKE needs two phases of negotiation: first, set security channel used for protecting IPsec SA negotiation; second negotiate IPsec SA used for protecting user data.

Phase one negotiation has two modes: Main Mode and Aggressive Mode.

Diffie-Hellman exchange

Diffie-Hellman exchange permits the participator creating a share secret value. The advantage of this technology is that the participator can set secret information on insecure network, and that information will not transmit via network.

There are five Diffie-Hellman groups defined in IKE and Signamax VPN product support the flowing three:

DH Group 1: 768 bits
DH Group 2: 1024 bits
DH Group 5: 1536 bits

The number is larger, the encryption key is more secure; but the process of creating the encryption key is much longer. Signamax VPN product provides much higher security by supporting the following groups:

DH Group 14: 2048 bits

DH Group 15: 3072 bits
DH Group 16: 4096 bits
DH Group 17: 6144 bits
DH Group 18: 8192 bits

Digital Certificate & Public Key Infrastructure

Public Key Infrastructure, PKI is a mature Internet security solution. It binds the id information of users (or equipment) and the public key together, to guarantee the confidentiality of the communication parties by using this non-symmetry encryption key. We usually call it digital identification.

Digital certificate application in IPsec VPN management solves the encryption key distribution, management difficulties in IPsec VPN application environment, and improves the system security.

IPsec Commands

Command	Description	Config mode
crypto ike key key_string {address ip_address | identity id_string | any} [seed]	*configure peer user encryption key.	config
crypto ike-proposal name_str	*define IKE proposal	config
encryption {3des | des | aes128 | aes192 | aes256 | blowfish | cast }	*configure encryption arithmetic during IKE negotiation process.	config-ike-prop
integrity {md5 | sha1 | sha2-256 | sha2-512 }	*configure IKE arithmetic	config-ike-prop
group {group1 | group2 | group5 | group14 | group15 | group16 | group17 | group18}	*configure IKE Diffie-Hellman groups	config-ike-prop
lifetime time	*configure IKE SA life time	config-ike-prop
crypto IPsec-proposal name_str	*define IPsec proposal	config
esp {3des | des | aes128 | aes196 | aes256 | blowfish | cast | serpent | twofish | ssp02 | null} [md5 | sha1 | sha2-256 | sha2-512 |	*configure ESP protocol encryption and authentication arithmetic.	config-IPsec-prop

rmd160 | aes-mac]		
ah {md5 | sha1 | sha2-256 | sha2-512}	*designate AH authentication arithmetic	config-IPsec-prop
compression {lzs | deflate}	*designate IPComp compression arithmetic	config-IPsec-prop
mode {transport | tunnel}	*designate security protocol encapsulation mode	config-IPsec-prop
pfs {group1 | group2 | group5 | group14 | group15 | group16 | group17 | group18}	*choose using Diffie-Hellman group when enabling PFS features.	config-IPsec-prop
lifetime {secondst_number | kbytes k_number }	*decide IPsec SA renegotiation time according to data or time.	config-IPsec-prop
crypto sec-level custom {basic | medium | high}	*define security level.	config
ike-proposal name_str [nam_str / name_str / name_str]	*designate security level used IKE proposal	config-sec-level
IPsec-proposal name_str {nam_str / name_str / name_str}	*designate IPsec proposal of security level.	config-sec-level
crypto tunnel name_str	*define designated name channel.	Config
peer {address ip_addr | hostname host_name | any}	*designate remote VPN equipment IP address or domain, for initiating channel negotiation.	config-tunnel
local {address ip_addr | interface int_name}	*designate local VPN IP address or external interface	config-tunnel
set peer-id id-str	*designate peer id, for identification during IKE negotiation.	config-tunnel
set local-id id-str	*designate local identification during IKE negotiation.	config-tunnel
set authentication { preshare | rsa-sig }	*configure IKE authentication mode	config-tunnel
set virtual-domain-id id_string	*designate channel virtual domain id.	config-tunnel
set mode {aggressive | main}	*designate local IKE switching mode	config-tunnel
set dpd delay-time retry-number	*designate DPD message retry time and times	config-tunnel
set sec-level {basic | standard | high}	*designate IPsec channel security level	config-tunnel
set ike-proposal name_str1 [name_str2 / name_str3 / name_str4]	*designate IKE negotiation proposal.	config-tunnel
set IPsec-proposal name_str1 [name_str2 / name_str3 / name_str4]	*designate IPsec proposal for channel	config-tunnel
set nat-traversal	*configure sending keepalive packet	config-tunnel

keepalive_time time_num	time interval after NAT.	
set auto-up	*configure whether the designated channel initiates negotiation	config-tunnel
set dhcp-over-IPsec	*configure whether designated channel is used for DHCP over IPsec function.	config-tunnel
set share-limit number	*when the channel peer is configured as any, designate the negotiated channel number.	config-tunnel
set idletime number	*designate the idle time. The channel will be deleted if it is not used during the time.	config-tunnel
crypto tunnel name_str manual	*define manual channel.	config
peer ip_addr	*designate remote VPN IP address	config-manual-tunnel
local {interface int_name | address addr}	*designate local VPN outbound interface	config-manual-tunnel
set IPsec-proposal name_str	*designate IPsec proposal for channel	config-manual-tunnel
set inbound {esp spi {encryption key_str | authentication key_str} | ah spi key_str | compression cpi}	*designate inbound IPsec SA attribute for channel.	config-manual-tunnel
set outbound {esp spi {encryption key_str | authentication key_str} | ah spi key_str | compression cpi}	*designate outbound IPsec SA attribute for channel	config-manual-tunnel
crypto policy name_str	*define name policy	config
flow {src_addr src_mask | any | host src_addr} {dst_addr dst_mask | any | host dst_addr} protocol [s_port d_port] {permit |deny |tunnel name_str name_str name_str name_str [bypass]}	*define policy data flow information	config-policy
set payload-balance	*designate payload balance function.	config-policy
set backup int_name	*designate IPsec link backup	config-policy
set IPsec-proposal name_str1 [name_str2 / name_str3 / name_str4]	*designate IPsec proposal for channel	config-policy
insert name_str1 {before | after} name_str2	*change policy location	config
crypto IPsec enable	*control IPsec command	config

crypto IPsec config-bynet enable	*whether permitting user remote configuration to IPsec module via Telnet.	config
crypto IPsec checked-replay enable	*set check replay	config
crypto IPsec df-bit {clear | copy | set}	*in channel mode, set DF bit dealt mode of original IP top.	config
crypto IPsec inspected-policy enable	*set whether enabling policy check.	config
crypto IPsec fast-forward enable	*set whether open IPsec high speed forwarding	config
crypto IPsec pre-fragment enable	*configure whether enabling pre-fragment function.	config
show crypto ike version	*display IKE module version information	Privileged configuration mode
clear crypto sa {policy po_name | tunnel tun_name} [unrebuild]	*delete and reset IPsec SA	Privileged configuration mode
show crypto ike sa {tunnel tun_name | policy po_name} [detail]	*examine IKE security association information	Privileged configuration mode
show crypto IPsec sa {policy po_name | tunnel tun_name}	*examine IPsec security association information	Privileged configuration mode
show crypto IPsec spd	*examine IPsec security strategy information	Privileged configuration mode
show ip {ahstate| espstate| compstate | IPsecstate| ipipstate}	*display protocol statistics information	Privileged configuration mode
clear ip {ahstate| espstate| compstate | IPsecstate| ipipstate}	*delete statistics information	Privileged configuration mode
show crypto ike logging	*display IKE logging information	Privileged configuration mode
clear crypto ike logging	*delete logging information	Privileged configuration mode
debug crypto ike {all | crypt | dns | emitting | event | kernel | lifecycle | natt | normal | parsing | private | raw}	*display IKE debugging information	Privileged configuration mode
debug crypto IPsec {all | address [tx|rx] | packet [tx|rx] |fragment}	*display IPsec debugging information	Privileged configuration mode
crypto ca identity ca_name	*configure CA identity	config
enrollment {address ip_addr | url name_string}	*configure CA server IP address or URL address	ca-identity
ca type {mpcms | ctca | windows}	*configure CA server type	ca-identity

crl autorenew period num	*configure CRL auto updating strategy	ca-identity
revoke check { off | on }	*configure certificate canceling check strategy	ca-identity
time check { off | on }	*configure certificate effective time check strategy.	ca-identity
crypto ca authenticate ca_name	*get and authenticate CA server certificate.	config
crypto ca enroll ca_name key_len user_name	*online certificate application	config
crypto ca retrive ca_name	*get certificate	config
crypto ca pkcs10-enrollca_name key_len user_name	*offline certificate application	config
crypto ca import certificate [to ca_name]	*import CA certificate	config
crypto ca import crl [to ca_name]	*import CRL	config
crypto ca crl request ca_name	*get certificate revocation list	config
crypto ca certificate {trust | autotrust | untrust} ca_name {name cert_name| sn cert_sn}	*set certificate trust status	config
no crypto ca certificate ca_name {name cert_name | sn cert_sn | type cert_type}	*delete local saved certificate.	config
show crypto ca identity	*display CA information	Privileged configuration mode
show crypto ca certificate { pem | der | general}	*display certificate	Privileged configuration mode
show crypto ca crl { pem | der | general}	*display certificate revocation list.	Privileged configuration mode

Note: 1, "*" before command means it has configuration example description.

2, configuration mode is: config, config-if-××(interface name) config-××(protocol name) .

IPsec Configuration

Via IKE negotiation to set IPsec channel, the configuration content is: pre-share encryption key configuration, IKE proposal, IPsec proposal, security level configuration, tunnel configuration, strategy configuration, global configuration, digital certificate configuration.

Configure Pre-share Encryption Key

When the phase one negotiation of IKE adopts pre-share key authentication, we need to configure pre-share key for both parties of IPsec communication.

crypto ike key…

Configure peer user pre-share key.
Command no is used to delete designated pre-share key.

```
vpn(config)# crypto ike key key_string {address ip_address |
identity id_string | any} [seed]
```

Parameter	Description
key key_string	Designate pre-share encryption key.
address ip_address	Designate ip address
Identity id_string	Designate id string
Any	Designate encryption key address and id.
seed	Designate encryption key as seed key.

(Configuration mode) global configuration mode

cry ike generate-key identity …

User can configure the key of a ID group with "*" as seed key and then generate the specific key for specific ID of this group.

vpn(config)#cry ike generate-key identity id-string [any|group-id]

Paramete r	Description
id-string	Remote ID content
any	Use common pre-share encryption key as seed key.
group-id	Configure this group ID pre-share encryption key as seed key.

The use method of seed key refers to configuration case.

Configur IKE Proposal

This part is optional configuration.

System pre-sets 8 IKE proposals, and the user chooses using some IKE proposals when configuring tunnel or security level, or defines IKE proposal via the following commands.

(pre-configured value)
System defines 8 IKE proposals by default, and their name rule is identified by group id-encryption algorithm-hash algorithm:

Name	Encryption arithmetic	Authentication arithmetic	Diffie-Hellman group	Lifetime (second)
g1-des-sha1	DES	SHA1	1(768 bit)	86400
g1-des-md5	DES	MD5	1(768 bit)	86400
g2-3des-sha1	3DES	SHA1	2(1024 bit)	86400
g2-3des-md5	3DES	MD5	2(1024 bit)	86400
g2-aes128-sha1	AES128	SHA1	2(1024 bit)	86400
g2-aes128-md5	AES128	MD5	2(1024 bit)	86400
g5-3des-sha256	3DES	SHA2-256	5 (1536 bit)	86400
g5-aes256-sha256	AES256	SHA2-256	5 (1536 bit)	86400

Define IKE proposal

crypto ike-proposal …

Define IKE proposal
Enter IKE proposal configuration mode
Command no is used to delete IKE proposal, command show is used to display designated or all IKE proposals.

```
vpn(config)# crypto ike-proposal name_str
vpn(config)# no crypto ike-proposal name_str
vpn# show crypto ike-proposal [name_str]
```

Parameter	Description
name_str	Designate IKE proposal name

(Configuration mode) global configuration mode

Configure IKE encryption algorithm

encryption …

```
Configure encryption arithmetic during IKE negotiation process.
Command no means using default DES.

vpn(config-ike-prop)#encryption {3des | des | aes128 | aes192 | aes256 | blowfish | cast }
vpn(config-ike-prop)#no encryption
```

Parameter	Description
des	IKE uses des encryption arithmetic
3des	IKE uses 3des encryption arithmetic
Aes128	IKE uses aes128 encryption arithmetic (key length is 128 Bit)
Aes192	IKE uses aes192 encryption arithmetic (key length is 192 Bit)
Aes256	IKE uses aes256 encryption arithmetic (key length is 256 Bit)
blowfish	IKE uses blowfish encryption arithmetic
cast	IKE uses cast encryption arithmetic

(Configuration mode) IKE proposal editing sub-mode.

(default configuration) des

Configure IKE hash algorithm

integrity …

Configure IKE hash algorithm
Command no is used to use SHA1

vpn(config-ike-prop)# integrity {md5 | sha1 | sha2-256 | sha2-512 }
vpn(config-ike-prop)#no integrity

Parameter	Description
sha1	Designate using sha1
md5	Designate using md5
sha2-256	Designate using sha2-256
sha2-512	Designate using sha2-512

(Configuration mode) IKE proposal editing sub-mode
(default configuration)sha1

Configure IKE Diffie-Hellman group

- **group …**

Configure IKE Diffie-Hellman arithmetic group.
Command no is used to use default group 1.

vpn(config-ike-prop)#group {group1 | group2 | group5 | group14 | group15 | group16 | group17 | group18}
vpn(config-ike-prop)#no group

Parameter	Description
group1	DH arithmetic uses 768 bit
group2	DH arithmetic uses 1024 bit
group5	DH arithmetic uses 1536 bit
group14	DH arithmetic uses 2048 bit
group15	DH arithmetic uses 3072 bit
group16	DH arithmetic uses 4096 bit
group17	DH arithmetic uses 6144 bit

group18	DH arithmetic uses 8192 bit

(Configuration mode) IKE proposal edits sub mode.
(default configuration) group 1,768 bit.

Configure IKE SA lifetime

lifetime …

Configure IKE setting SA lifetime.
Command no is used to use default IKE SA lifetime(86400 seconds)

vpn(config-ike-prop)#lifetime time
vpn(config-ike-prop)#no lifetime

Parameter	Description
Time	SA existing time(unit: second)

(Configuration mode) IKE proposal editing sub mode.
(default configuration)86400 seconds.

Configure IPsec proposal

This item is optional configuration.
According to different security level and arithmetic, the system pre-configures 8 IPsec proposals. The user can use it in tunnel configuration or security level configuration, or define IPsec proposal according to the following commands.

(pre-configured value)
8 pre-configured IPsec proposals are as following, and all proposals adopt ESP protocol and tunnel mode for encapsulation.

Name	PFS	Encryption arithmetic (ESP)	Authentication arithmetic (ESP)
esp-nopfs-des-sha1	N/A	des	sha1
esp-nopfs-des-md5	N/A	des	md5
esp-g2-3des-sha1	group2	3des	sha1
esp-g2-3des-md5	group2	3des	md5
esp-g2-aes128-sha1	group2	aes128	sha1
esp-g2-aes128-md5	group2	aes128	md5
esp-g5-3des-sha256	group5	3des	sha2-256
esp-g5-aes256-sha256	group5	aes256	sha2-256

Define/Delete IPsec Proposal

crypto IPsec-proposal …

Define IPsec proposal
Execute the command to enter IPsec proposal configuration mode.
Command no is used to delete IPsec proposal.

```
vpn(config)# crypto IPsec-proposal name_str
vpn(config)# no crypto IPsec-proposal name_str
vpn(config)# show crypto IPsec-proposal [name_str]
```

Parameter	Description
name_str	Designate IKE proposal name

(Configuration mode) global configuration mode

Configure ESP Encryption & Authentication Algorithm

```
esp …
```

Configure ESP protocol encryption and authentication arithmetic.
Command no means not using ESP protocol.

```
vpn(config-IPsec-prop)# esp {3des | des | aes128 | aes196 |
aes256 | blowfish | cast | serpent | twofish | ssp02 | null}
[md5 | sha1 | sha2-256 | sha2-512 | rmd160 | aes-mac ]
vpn(config-IPsec-prop)# no esp
```

Parameter	Description
des	Use DES encryption arithmetic
3des	Use 3DES encryption arithmetic
aes128	Use AES encryption arithmetic(key length: 128 bit)
aes196	Use AES encryption arithmetic(key length: 192 bit)
aes256	Use AES encryption arithmetic(key length: 256 bit)
blowfish	Use blowfish encryption arithmetic
cast	Use cast encryption arithmetic
serpent	Use serpent encryption arithmetic
twofish	Use twofish encryption arithmetic

ssp02	Use ssp02 encryption arithmetic(Note: this arithmetic needs special encryption chip)
null	Not use encryption arithmetic
md5	Use md5 authentication arithmetic
sha1	Use sha1 authentication arithmetic
sha2-256	Use sha2-256 authentication arithmetic
sha2-512	Use sha2-512 authentication arithmetic
rmd160	Use rmd160 authentication arithmetic
aes-mac	Use aes-mac authentication arithmetic

(Configuration mode) IPsec proposal configuration mode

ESP authentication arithmetic cannot use singly, and it should be used together with ESP encryption arithmetic; ESP encryption arithmetic can use singly, but if choosing esp-null encryption arithmetic, ESP authentication arithmetic must be configured.

Configure AH authentication arithmetic

ah …

Designate AH protocol authentication arithmetic
Command no means not to use AH protocol.

```
vpn(config-IPsec-prop)# ah {md5 | sha1 | sha2-256 | sha2-512}
vpn(config-IPsec-prop)#no ah
```

Parameter	Description
sha1	Use sha1 authentication arithmetic
md5	Use md5 authentication arithmetic
sha2-256	Use sha2-256 authentication arithmetic
sha2-512	Use sha2-512 authentication arithmetic

(Configuration mode) IPsec proposal configuration mode

Configure IPComp compression algorithm

compression …

Designate IPComp protocol compression arithmetic
Command no means not to use IPComp protocol.

```
vpn(config-IPsec-prop)# compression {lzs | deflate}
vpn(config-IPsec-prop)#no compression
```

Parameter	Description
lzs	Use LZS compression arithmetic
deflate	Use DEFLATE compression arithmetic

(Configuration mode) IPsec proposal configuration mode

Configure Encapsulation Mode

mode …

Designate security protocol encapsulation mode.
Command no is used for default mode (tunnel mode).

```
vpn(config-IPsec-prop)# mode {transport | tunnel}
vpn(config-IPsec-prop)#no mode
```

Parameter	Description
tunnel	Tunnel mode, used for protecting data transmission of gateway or host.
transport	Transport mode, used for protecting the data transmission of host.

(Configuration mode) proposal configuration mode
(default configuration)tunnel,tunnel mode.

The gateway usually uses tunnel mode. IPsec transport mode is for end-to-end security protection.

Configure Perfect Forward Secrecy (PFS)

PFS (Perfect Forward Secrecy) is the leakage of an encryption key only causes the invalid access of the data protected by this encryption key, but the data protected by other encryption keys are keeping original security.

For IKE, with an additional Diffie-Hellman exchange for phase two IPsec SA, a new encryption key for data communication protection created, and the IPsec SA encryption key has the features of PFS.

pfs …

Use Diffie-Hellman group when enabling PFS features.
Command no doesn't provide PFS.

```
vpn(config-IPsec-prop)# pfs {group1 | group2 | group5 | group14 | group15 | group16 | group17 | group18}
```

Parameter	Description
group1	DH uses 768 bits group.
group2	DH uses 1024 bits group.
group5	DH uses 1536 bits group.
group14	DH uses 2048 bits group.
group15	DH uses 3072 bits group.
group16	DH uses 4096 bits group.
group17	DH uses 6144 bits group.
group18	DH uses 8192 bits group.

(Configuration mode) IPsec proposal configuration mode.
(default configuration)group1

Configure IPsec SA Lifetime

lifetime …

Decide IPsec SA renegotiation time according to data flow or time. Command no is used to renew default time and data flow.(3600 seconds, 4608000Kbytes) .

```
vpn(config-IPsec-prop)# lifetime {secondst_number | kbytes
k_number }
vpn(config-IPsec-prop)#no set lifetime [seconds | kbytes]
```

Parameter	Description
t_number	Designate SA lifetime, and the unit is second.
k_number	Designate SA lifetime, and the unit is byte.

(Configuration mode) IPsec proposal configuration mode.
(default configuration)3600 seconds/4608000 kilobytes

Configure security level

This item is optional configuration.

According to different security level and arithmetic, the system configures three security level, and they have pre-configured value. The user uses it in tunnel configuration. And meanwhile, the security level can be configured different IKE proposal and IPsec proposal.

In order to provide convenient configuration and smart management, Signamax VPN provides security level management mode, and security level comprises IKE proposal and IPsec proposal: base, medium, high. Users need only to select security level according to actual communication security requirement

Define Security Level

crypto sec-level …

Define security level.

Command no is for using default mode (tunnel mode), show is to display security level configuration.

```
vpn(config)# crypto sec-level custom {basic | medium | high}
vpn(config)# no crypto sec-level custom [basic | medium | high]
vpn(config)# show crypto sec-level
```

Parameter	Description
basic	Basic security level
medium	Medium security level
high	High security level

(Configuration mode) global configuration mode

Configure IKE Proposal

ike-proposal …

Designate security level IKE proposal.
Command no is for using default IKE proposal.

```
vpn(config-sec-level)# ike-proposal name_str [nam_str/ name_str/ name_str]
vpn(config-sec-level)# no ike-proposal
```

Parameter	Description
name_str	The name of IKE proposal, range is from 1-4.

(Configuration mode) global configuration mode

For base security level, the default IKE proposal is: g1-des-sha1, g1-des-md5; medium security level is: g2-3des-sha1, g2-3des-md5, g2-aes128-sha1, g2-aes128-md5; high security level is:

g5-3des-sha256、g5-aes256-sha256.

Configure IPsec Proposal

IPsec-proposal …

Designate security level IPsec proposal.
Command no is used for default IPsec proposal.

```
vpn(config-sec-level)# IPsec-proposal name_str {nam_str / name_str/ name_str}
vpn(config-sec-level)# no IPsec-proposal
```

Parameter	Description
name_str	The name of IPsec proposal, and range is from 1 to 4.

(Configuration mode) global configuration mode

For base security level, the default IPsec proposal is: esp-nopfs-des-sha1, esp-nopfs-des-md5; medium security level default IPsec proposal is: esp-g2-3des-sha1, esp-g2-3des-md5, esp-g2-aes128-sha1, esp-g2-aes128-md5; high security level default IPsec proposal is: esp-g5-3des-sha256, esp-g5-aes256-sha256.

Configure VPN Tunnel

The basis of configuring IPsec tunnel is: configure local address or interface, peer address or DNS name. Use the default values for other configuration items usually and enabled or modified them according to the requirement.

The peer address or name may not be configured when IPsec communication peer address cannot be confirmed. That means local end can response to peer negotiation request but not initiate negotiation.

Define Tunnel

crypto tunnel …

Define the tunnel, and execute the command to enter the configuration mode.

Command no is used to delete the tunnel, show is used to display tunnel configuration information.

```
vpn(config)# crypto tunnel name_str
vpn(config)# no crypto tunnel name_str
vpn# show crypto tunnel [name_str]
```

Parameter	Description
Name_str	Tunnel name

(Configuration mode) global configuration mode, privileged configuration mode.

Tunnel name cannot be the same with the manual tunnel name.

Configure Peer Address

peer …

Designate remote VPN IP address or domain, for initiating tunnel negotiation, and if not configure the parameter, the tunnel is only used as response end for peer negotiation.

Command no is used to designate peer as default value (any).

```
vpn(config-tunnel)# peer {address ip_addr | hostname
host_name | any}
vpn(config-tunnel)# no peer
```

Parameter	Description
address ip_addr	Peer VPN IP address
hostname host_name	Peer VPN domain name
any	Any peer

(Configuration mode) tunnel configuration mode
(default configuration)any

Configure Local Address

local …

Designate local VPN IP address or outbound interface, if local id not configured, local address will be used as local id. Command no is used to delete local address or outbound interface.

```
vpn(config-tunnel)# local {address ip_addr | interface int_name}
vpn(config-tunnel)# no local
```

Parameter	Description
address ip_addr	Tunnel uses local VPN IP address
interface int_name	Tunnel uses local VPN interface

(Configuration mode) tunnel configuration mode

Configure Peer ID

In IKE negotiation, if adopting pre-share main mode negotiation, IP address is used as identification, but because IP address is always changing, we need to use other information as identification, such as domain name, email address etc.

Therefore, when using the certificate for authentication or using aggressive mode negotiation, the limitation to remote VPN id can enhance security and management, to realize user authority division.

Designate the remote user id for this tunnel. We can use "*", for example, when configuring *.signamax.com, accept ID as server.signamax.com, but not ID as server.sec.com. in this way, the peer user should have pre-share encryption or certificate to complete the tunnel negotiation.

Command no is used to delete peer id.

```
vpn(config-tunnel)#set peer-id id-str
vpn(config-tunnel)#no set peer-id
```

Parameter	Description
id-str	Peer ID content, and it can be IP address, domain name or other characters list.

(Configuration mode) tunnel configuration mode
(example)
Configure peer ID a.sec.com for single peer user.

```
VPN(config-tunnel)#set peer-id a.sec.com
Configure peer ID *.sec.com for the group.
VPN(config-tunnel)#set peer-id *.sec.com
```

Configure Local ID

set local-id …

Designate local id, for id authentication of IKE negotiation process. When local id is not designated, use local IP address as local id for pre-shared key authentication; auto choose a valid local certificate for digital signature authentication mode.

If the local ID is not IP address, we suggest using active negotiation mode. The command no is used for deleting local id.

```
vpn(config-tunnel)#set local-id id-str
vpn(config-tunnel)#no set local-id
```

Parameter	Description
id-str	Local ID content, and it can be IP address, domain name or other characters list.

(Configuration mode) tunnel configuration mode

When using certificate for authentication, the default valid host name as local ID, therefore, the local ID is not configured. But you can configure it when there are many valid certificates in different tunnels.

Configure IKE Authentication Mode

set authentication …

Configure IKE authentication mode, including pre-share encryption key and RSA signature authentication. Command no is used to adopt default authentication mode(preshare) .

```
vpn(config-ike-prop)#set authentication { preshare | rsa-sig }
vpn(config-ike-prop)#no set authentication
```

Parameter	Description
preshare	Use pre-share encryption authentication mode.
rsa-sig	Use RSA digital signature authentication mode.

(Configuration mode) tunnel configuration mode
(default configuration)preshare

Configure Virtual Security Domain

Virtual security domain technology is used for solving VPN isolation and enterprise VPN internal network address multiplexing according to the isolation of IPsec tunnel. And the gateway with this function uses as core access equipment, the same VPN equipment provides to different enterprises (or department).

set virtual-domain-id …

Designate tunnel virtual security domain identity. It uses on core equipment, connecting different subnets via VPN tunnel. And the subnets belonging to the same domain can be accessed.

Command no is used to clear the virtual domain of the tunnel.

```
vpn(config-tunnel)# set virtual-domain-id id_string

vpn(config-tunnel)#no set virtual-domain-id
```

Parameter	Description
id_string	Virtual security domain name

(Configuration mode) tunnel configuration mode

Configure IKE Negotiation Mode

IKE negotiation has two modes: main mode and aggressive mode, and we usually adopt main mode. According to actual environment requirement, if adopting pre-share encryption key authentication mode, and local ID is not IP address or local IP address is changeable, we suggest using aggressive mode.

set mode …

Execute the switching mode.
Command no is used to adopt default mode (main mode).

```
vpn(config-tunnel)# set mode {aggressive | main}
vpn(config-tunnel)#no set mode
(Configuration mode) tunnel configuration mode
```

Parameter	Description
main	Main mode
aggressive	Aggressive mode

(default configuration)main mode

This command has main mode or aggressive mode.

Configure Dead Peer Detection (DPD)

DPD(Dead Peer Detection) means when not receive IPsec packet from the peer, send the packet according to the time and time interval, to detect whether the peer is alive. And that is to examine whether it has IKE status information. This will guarantee IPsec communication.

set dpd …

Designate DPD message retrying time interval and number.
Command no is not enabling DPD.

```
vpn(config-tunnel)# set dpd delay-time retry-number
vpn(config-tunnel)# no set dpd
```

Parameter	Description
delay-time	Sending DPD packet time interval, and the unit is second, default value is 30 seconds.
retry-number	The retry number of no response, and the default value is 2.

(Configuration mode) tunnel configuration mode
(default configuration)

Enable DPD, and its attributes is as: sending DPD packet every 30 seconds, retrying 2 times, and if the peer is down, only clear IKE status information and IPsec SA.

Whether DPD is effective, it needs to confirm whether peer equipment supports this function via IKE negotiation.

Choose Security Level

```
set sec-level …
```

Designate IPsec tunnel security level.
Command no is used to renew default security level(standard) .

```
vpn(config-tunnel)# set sec-level {basic | standard | high}
vpn(config-tunnel)# no set sec-level
```

Parameter	Description
basic	Basic security level
standard	Standard security level
high	High security level

(Configuration mode) tunnel configuration mode
(default configuration)standard

Security level is effective when the tunnel doesn't have special designation of IKE proposal and IPsec proposal. When user chooses special IKE proposal, IKE negotiation will adopt that IKE proposal, and similarly, when user chooses special IPsec proposal, the IPsec proposal of security level will not join into negotiation.

Choose IKE Proposal

set ike-proposal …

Designate IKE proposal.
Command no is used to delete special proposal.

```
vpn(config-tunnel)# set ike-proposal name_str1 [name_str2 / name_str3 / name_str4]
vpn(config-tunnel)# no set ike-proposal
```

Parameter	Description
Name_str1	IKE proposal name

(Configuration mode) tunnel configuration mode

Choose IPsec Proposal

set IPsec-proposal …

Designate IPsec proposal for tunnel.
Command no is used to delete IPsec proposal.

```
vpn(config-tunnel)# set IPsec-proposal name_str1 [name_str2 /
name_str3 /  name_str4]
vpn(config-tunnel)# no set IPsec-proposal
```

Parameter	Description
Name_str1	IPsec proposal name

(Configuration mode) tunnel configuration mode

Configure NAT Traversing Keepalive Packet Time Interval

set nat-traversal …

Set sending keepalive packet time interval for NAT.
Command no is used to renew default time interval (20 seconds).

```
vpn(config-tunnel)# set nat-traversal keepalive_time time_num
vpn(config-tunnel)# no set  nat-traversal
```

Parameter	Description
time_num	Time interval seconds

(Configuration mode) tunnel configuration mode
(default configuration)20 seconds

Configure Auto Negotiation

set auto-up …

Set whether the designated tunnel has initiated negotiation.
Command no is used to close auto negotiation function.

```
vpn(config-tunnel)# set auto-up
vpn(config-tunnel)# no set auto-up
```

(Configuration mode) tunnel configuration mode
(default configuration)close auto negotiation

Auto negotiation function is applied to peer confirmation, which is to say, it is peer but not any.

Configure DHCP over IPsec

```
set dhcp-over-IPsec
```

Set whether the designated tunnel is applied for DHCP over IPsec.
Command no is used to close DHCP over IPsec.

```
vpn(config-tunnel)# set dhcp-over-IPsec
vpn(config-tunnel)# no set dhcp-over-IPsec
(Configuration mode) tunnel configuration mode
(default configuration)close DHCP over IPsec
```

The DHCP command of DHCP over IPsec refers to chapter 21 DHCP configuration.

Configure Permitted Negotiation Tunnel Number

```
set share-limit …
```

When the tunnel peer is configured as any, designate the negotiated tunnel number.

Command no means there is no limitation.

```
vpn(config-tunnel)# set share-limit number
vpn(config-tunnel)# no set share-limit
```

Parameter	Description
number	Permitted tunnel number

(Configuration mode) tunnel configuration mode
(default configuration)no limitation

Configure Permitted Idle Time

set idletime …

Designate tunnel permitted idle time, and the tunnel will be deleted if it is not used during the designated time.

Command no is for no limitation.

```
vpn(config-tunnel)# set idletime number
vpn(config-tunnel)# no set idletime
```

Parameter	Description
number	Permitted idle time

```
(Configuration mode) tunnel configuration mode
(default configuration)no limitation
```

Configure Manual Tunnel

Manual tunnel sets another IPsec SA mode, and it gets the IPsec SA information according to outband mode, and then completes all the configuration in local. IPsec SA establishment cannot be completed via IKE.

Because the manual IPsec tunnel cannot applied to complex network environment, the function is limited, such as: don't support IPsec SA life limitation, don't support resisting replying function and it cannot manage IPsec session encryption key, we don't suggest user adopting manual tunnel to protect data communication.

There are some steps to set manual IPsec tunnel:

Configure peer address and local outbound interface;

Configure IPsec proposal, to get encryption arithmetic or authentication arithmetic;

Configure inbound and outbound IPsec SA security protocols, SPI and encryption key information.

Same as normal tunnel, manual tunnel also needs a strategy to set up IPsec SA.

Define Manual Tunnel

```
crypto tunnel …
```

Define designated name manual tunnel, and enter into manual tunnel configuration mode.

Command no is used to delete designated manual tunnel, command show is used to display manual tunnel configuration information.

```
vpn(config)# crypto tunnel name_str manual
vpn(config)# no crypto tunnel name_str
vpn# show crypto tunnel [name_str]
```

Parameter	Description
name_str	Manual tunnel name

(Configuration mode) global configuration mode, privileged configuration mode.

Manual tunnel name should not be the same as tunnel name.

Configure Peer Address

```
peer …
```

Designate peer VPN IP address.
Command no is used to delete peer address.

```
vpn(config-manual-tunnel)# peer ip_addr
vpn(config-manual-tunnel)# no peer
```

Param eter	Description
ip_addr	Peer VPN IP address

(Configuration mode) manual tunnel configuration mode

Configuration Local Address

local …

Designate local VPN equipment outbound interface.
Command no is used to delete local outbound interface.

```
vpn(config-manual-tunnel)# local {interface int_name | address addr}
vpn(config-manual-tunnel)# no local
```

Parameter	Description
address addr	Local address
interface int_name	Local VPN interface

(Configuration mode) manual tunnel configuration mode

Choose IPsec Proposal

set IPsec-proposal …

Designate IPsec proposal.
Command no is used to delete IPsec proposal.

```
vpn(config-manual-tunnel)# set IPsec-proposal name_str
vpn(config-manual-tunnel)# no set IPsec-proposal
```

Parameter	Description
name_str	The defined IPsec proposal name

(Configuration mode) manual tunnel configuration mode

Configure Inbound IPsec SA Attributes

set inbound …

Designate inbound IPsec SA attributes.
Command no is used to delete the attributes.

```
vpn(config-manual-tunnel)# set inbound {esp spi {encryption
key_str | authentication key_str} | ah spi key_str |
compression cpi}
vpn(config-manual-tunnel)# no set inbound
```

Parameter	Description
esp spi [encryption key_str | authentication key_str	When IPsec proposal designates ESP proposal, designate SPI(security parameter index) value and encryption key and authentication encryption key.
ah spi key_str	When IPsec proposal designates AH protocol, designated SPI(security parameter index) value and encryption key.
compression cpi	When IPsec proposal designates IPComp protocol, designate CPI value.

(Configuration mode) manual tunnel configuration mode

Configure Outbound IPsec SA Attributes

set outbound …

```
Designate outbound IPsec SA attributes.
Command no is used to delete  attributes.

vpn(config-manual-tunnel)# set outbound {esp spi {encryption
key_str  |  authentication  key_str}  |  ah  spi  key_str  |
compression cpi}
vpn(config-manual-tunnel)# no set outbound
```

Parameter	Description
esp spi [encryption key_str | authentication key_str	When IPsec proposal designates ESP proposal, designate SPI(security parameter index) value and encryption key and authentication encryption key.
ah spi key_str	When IPsec proposal designates AH protocol, designated SPI(security parameter index) value and encryption key.
compression cpi	When IPsec proposal designates IPComp protocol, designate CPI value.

(Configuration mode) manual tunnel configuration mode

Configure Policy

Policy is to designate special data flow to special action, which is: permit, deny and apply IPsec tunnel. permit means the data flow is not directly forwarded by IPsec; deny means to via away the data flow, but not to forward it; and application means the data flow needs IPsec tunnel dealt when forwarding.

Define Policy

```
crypto policy …
```

Define policy and enter policy configuration mode.
Command no is used to delete the policy, and command show is used to display policy configuration information.

```
vpn(config)# crypto policy name_str
vpn(config)# no crypto policy name_str
vpn# show crypto policy [name_str]
```

Parameter	Description
name_str	Policy name

(Configuration mode) global configuration mode and privileged configuration mode

Configure Data Flow

```
flow …
```

Define policy data flow information.

```
vpn(config-policy)# flow {src_addr src_mask | any | host src_addr} {dst_addr dst_mask | any | host dst_addr} protocol [s_port d_port] {permit |deny |tunnel name_str name_str name_str name_str [bypass]}
```

Parameter	Description
src_addr src_mask | any | host *src_addr*	Source address and source address mask, use the key word any when matching the source address, and use key word host and the address when matching special host.
dst_addr dst_mask | any | host *dst_addr*	Destination address and destination address mask, which is the same as designated mode. use the key word any when matching the source address, and use key word host and the address when matching special host.
protocol	Designate protocol
s_port	Source port, and its range can be designated.
d_port	Destination port, and its range can be designated.
permit	Permit data flow
deny	Deny forwarding the data flow
tunnel *name_str*	IPsec SA of data flow, and this IPsec SA is from tunnel *name_str.* For one data flow, it has 1-4 tunnels, and when the tunnel is more than one, the extended tunnel is used as tunnel backup or load balance.
bypass	Configure Bypass attributes

(Configuration mode) policy configuration mode

When policy applies to many tunnels, if many are used as backup, there is a priority order, which is to say the first configured tunnel should be used first, such as the following configuration tun1 and tun2:

```
flow 1.1.1.0 255.255.255.0 2.2.2.0 255.255.255.0 ip tunnel tun1 tun2
```

Tun1 has the priority of tun2, when tun1 negotiated IPsec SA exists, tun2 negotiated IPsec SA will not be used. When tun1 is down, tun2 will be used automatically, and when tun1 renews, it will auto switches to tun1.

Designate Load Balance

When data flow applies to many tunnels, these tunnels may use for load balance.

set payload-balance

Designate load balance function of data flow tunnels.
Command no is used to cancel load balance.

```
vpn(config-policy)# set payload-balance
vpn(config-policy)# no set payload-balance
```

Parameter	Description
payload-balance	Load balance key word

(Configuration mode) policy configuration mode

Designate IPsec Link Backup Function

Designate IPsec tunnel for link backup. For example, for one data flow, the user has two links: one is DDN leased line without IPsec encryption, and another is a tunnel with IPsec encryption, DDN is main link and IPsec tunnel is secondary link. When DDN leased line appears malfunction, IPsec tunnel is used. And now we designated link backup to satisfy the function.

For above example, the condition of IPsec tunnel forwarding is that: there is no routing list item on DDN leased line interface.

```
set backup …
```

Designate IPsec link backup function. When data flow is not via this interface, use IPsec for forwarding.

Command no is used to cancel link backup function.

```
vpn(config-policy)# set backup int_name
vpn(config-policy)# no set backup
```

Parameter	Description
int_name	Interface name

(Configuration mode) policy configuration mode

Choose IPsec Proposal

Designate IPsec proposal in policy, only when policy applies to tunnel, it make effective. Policy applies to tunnel (many policies apply to the same tunnel), and tunnel applies security level (many tunnels may use one security level).

set IPsec-proposal …

Designate IPsec proposal.
Command no is used to delete the proposal.

```
vpn(config-policy)# set IPsec-proposal name_str1 [name_str2 /
name_str3 / name_str4]
vpn(config-policy)# no set IPsec-proposal
```

Parameter	Description
name_str1	IPsec proposal name

(Configuration mode) policy configuration mode

Change Policy Location

Policy is in order, for example,

```
P1:flow 192.168.0.0 255.255.0.0 10.0.0.0 255.255.255.0 ip
tunnel tun1

P2:flow 192.168.1.0 255.255.255.0 10.0.1.0 255.255.255.0 ip
tunnel tun2

Suppose user defines P1 first, then, the packet, which source
address fall in subnet 192.168.1.0 255.255.255.0 and the
destination address fall in subnet 10.0.1.0 255.255.255.0,
cannot get the protection of tun2, tun1 protect it in first.
In order to solve this situation, we can change the order via
changing the policy position.
```

insert …

Change policy location.

```
vpn# insert name_str1 {before | after} name_str2
```

Parameter	Description
bef ore	Put policy name_str1 before name_str2.
after	Put policy name_str1 after name_str2.
name_str1	The policy name o f changing location.
name_str2	The policy name used as coordinate

(Configuration mode) privileged configuration mode

Configure Global Parameter

The following parameters have the default value, and so there is no need to configure and modify it.

Configure IPsec Command

crypto IPsec enable

```
Whether IPsec  command can be used.
Command no is used to close IPsec  command.

vpn(config)#crypto IPsec enable
vpn(config)#no crypto IPsec enable
(Configuration mode) global configuration mode
(default configuration)IPsec enable
```

Configure IPsec Permitting Network Configuration

crypto IPsec config-bynet enable

Whether configuring IPsec module via net, such as telnet etc. and the default is permitted.
Command no is used to disable remote configuration.

```
vpn(config)#crypto IPsec config-bynet enable
vpn(config)#no crypto IPsec config-bynet enable
(Configuration mode) global configuration mode
(default configuration)permit remote configuration
```

Configure Replay Check

crypto IPsec checked-replay …

Set checked replay.
Command no is used to close this function.

```
vpn(config)#crypto IPsec checked-replay enable
vpn(config)#no crypto IPsec checked-replay enable
(Configuration mode) global configuration mode
(default configuration)enable checked replay
```

Configure IPsec DF-bit

crypto IPsec df-bit …

In tunnel mode, configure DF-bit in IP header:
clear:clear DF-bit;
copy:copy DF-bit to new IP header;
set:set DF-bit.

```
vpn(config)#crypto IPsec df-bit {clear | copy | set}
(Configuration mode) global configuration mode
(default configuration)clear
```

Configure Inbound Policy Check

crypto IPsec inspected-policy …

```
vpn(config)# crypto IPsec inspected-policy enable
vpn(config)# no crypto IPsec inspected-policy enable
(Configuration mode) global configuration mode
(default configuration)disable the check
```

Configure IPsec High-speed Forwarding

crypto IPsec fast-forward …

Enable IPsec high speed forwarding, to speed IPsec.
Command no is used to disable IPsec high speed forwarding.

```
vpn(config)# crypto IPsec fast-forward enable
vpn(config)# no crypto IPsec fast-forward enable
vpn(config)# show crypto IPsec fast-forward [detail | list]
```

Parameter	Description
detail	Display IPsec high speed forwarding list detailed information.
list	Display IPsec high speed forwarding information.

```
(Configuration mode) global configuration mode
(default configuration)disable high speed forwarding
```

Configure IPsec Pre-fragment Function

crypto IPsec pre-fragment …

Enable pre-fragment function, to speed the forwarding.
Command no is used to disable IPsec pre-fragment function.

```
vpn(config)# crypto IPsec pre-fragment enable
vpn(config)# no crypto IPsec pre-fragment enable
(Configuration mode) global configuration mode
(default configuration)disable pre-fragment function.
```

IPsec/IKE Monitoring & Debugging

All the commands to debugging and monitoring are in privileged user mode.

Monitoring Management

Display Version Information

show crypto ike version

Display IKE module version information

```
vpn#show crypto ike version
```

show crypto IPsec version

Display IPsec module version information

```
vpn#show crypto IPsec version
```

Delete & Reset IPsec SA

clear crypto sa …

Use this kind of command to delete and reset IPsec SA.

```
vpn#clear crypto sa {policy po_name | tunnel tun_name}
[unrebuild]
```

Parameter	Description
unrebuild	If choosing parameter unrebuild,it will not re-negotiate.
policy po_name	Delete designated policy IPsec SA
tunnel tun_name	Delete designated tunnel IPsec SA

(default configuration)re-negotiate IPsec SA

Display IKE Negotiating SA Status

show crypto ike sa…

Examine IKE SA information

```
vpn#show crypto ike sa {tunnel tun_name | policy po_name}
[detail]
```

Parameter	Description
tunnel tun_name	Display tunnel negotiation status
policy po_name	Display policy negotiation status
detail	Display IKE negotiation SA detailed information

(Configuration mode) privileged user mode

Display IPsec SA Status

```
show crypto IPsec sa…
```

Examine IPsec SA information

```
vpn#show crypto IPsec sa {policy po_name | tunnel tun_name}
```

Parameter	Description
policy po_name	Display policy IPsec SA
tunnel tun_name	Display tunnel IPsec SA

Display IPsec Security Policy Information

show crypto IPsec spd

Examine IPsec security policy database information

```
vpn#show crypto IPsec spd
```

Display IPsec Statistics Information

show ip …

Display protocol statistics information
Command clear is used to delete statistics information.

```
vpn#show ip {ahstate| espstate| compstate | IPsecstate|
ipipstate}
vpn#clear ip {ahstate| espstate| compstate | IPsecstate|
ipipstate}
```

Parameter	Description
ahstate	Display AH packet statistics information
espstate	Display ESP packet statistics information
compstate	Display IPComp packet statistics information
IPsecstate	Display IPsec packet statistics information
ipipstate	Display IPinIP packet statistics information

Display IKE log Information

show crypto ike logging

```
Display IKE log information
Command clear is used to delete log information.

vpn#show crypto ike logging
vpn#clear crypto ike logging
```

Debugging Command

IKE Debugging Command

```
debug crypto ike normal

Enable IKE debugging switch

vpn#debug crypto ike {all | crypt | dns | emitting | event |
kernel | lifecycle | natt | normal | parsing | private | raw}
vpn#no debug crypto ike [all | crypt | dns | emitting | event
| kernel | lifecycle | natt | normal | parsing | private |
raw]
```

Parameter	Description
all	Enable all IKE debugging information
crypt	Enable IKE debugging information.
dns	Enable IKE negotiation DNS debugging information.
emitting	Enable IKE negotiation packet detailed content.
event	Enable IKE clock event debugging information.
kernel	Enable debugging information between IKE and kernel.
lifecycle	Enable IKE negotiation lifecycle debugging information
natt	Enable IKE negotiation NAT traversing debugging information.
normal	Enable IKE negotiation normal debugging information.
parsing	Enable IKE negotiation received packet debugging information
raw	Enable IKE negotiation packet original content debugging information.

IPsec Debugging Command

debug crypto IPsec …

```
Display IPsec debugging information

vpn#debug crypto IPsec {all | address [tx|rx] | packet [tx|rx]
|fragment}
vpn#no debug crypto IPsec
```

Parameter	Description
all	Enable all IPsec debugging information
address [tx|rx]	Enable IP packet address debugging information, tx: display outbound packet address information, rx:display inbound packet address information.
packet [tx|rx]	Enable IP packet content debugging information, tx: display outbound packet content information, rx:display inbound packet content information.
fragment	Enable IP packet fragment information.

(Configuration mode) privileged user mode

Digital Certificate Application & Configuration

Signamax VPN product combining with MPSec CMS,Win2000 CA,China Telecom CA, to realize high strength id authentication via digital certificate. Based on the features of VPN, it is applied to construct large-scale VPN network.

Configure CA Server Information & Authentication Policy

Enter CA Identity Configuration

crypto ca identity …

One CA identity is to one CA, including more than one CA certificates. The CA trust are configuration parameter comprises server IP address and certificate authentication policy etc. The system supports defining more than one CA trust areas.

Enter CA trust area, and system prompt is: VPN(ca-identity)#
Command no is used to delete the CA identity.

```
vpn(config)#crypto ca identity ca_name
```

Parameter	Description
ca_name	Configure CA trust area name

(Configuration mode) global configuration mode

Define a CA identity named myca, and this name is only for local id.

```
VPN(config)#crypto ca identity myca
```

Configure CA Server Address

```
enrollment url …
```

Use this command to configure CA server IP address or URL address.

```
vpn(ca-identity)#enrollment {address ip_addr | url name_string}
```

Parameter	Description
name_string	CA server URL
ip_addr	CA server IP address

(Configuration mode) CA identity configuration mode

```
VPN(ca-identity)#enrollment address 128.255.1.10
```

Configure CA Server Type

```
ca type …
```

If using online certificate application for updating function, the system adopts different protocol standard for communication according to CA server type, therefore, CA server type needs to be configured.

If using offline certificate application mode, no need to configure it. System supporting online certificate application CA server type comprises: MPSec-CMS, CTCA,Windows server 2000/2003.

```
vpn(ca-identity)#ca type {mpcms | ctca | windows}
```

Parameter	Description
Mpcms	Signamax certificate server
Ctca	China Telecom CA
Windows	Windows 2000, 2003 CA server

(Configuration mode) CA identity configuration mode
(default configuration)CA type is mpcms

```
VPN(ca-identity)#ca type mpcms
```

Configure CRL(Certificate Revocation List) Auto Update Policy

```
crl autorenew …
```

System supports auto CRL update, and auto update frequency is decided by two factors: CRL next released time and local configuration update period.

```
vpn(ca-identity)#crl autorenew period num
```

Parameter	Description
Num	Update period (minute)

(Configuration mode) CA identity configuration mode
(default configuration)0,no auto update

```
Configure CRL auto update period as 1 hour.
VPN(ca-identity)#crl autorenew peroid 60
```

Configure Certificate Revocation Check Policy

```
revoke check …
```

Certificate validity comprises: CA signature, whether certificate is canceling and whether it is during valid period.

```
vpn(ca-identity)# revoke check { off | on }
```

Parameter	Description
Off	Check only there is CRL.
On	Check certificate canceling, if there is no CRL, it is considered the authentication is failed, to guarantee the security.

```
(Configuration mode) CA identity configuration mode
(default configuration)off,no strict check
```

Configure Certificate Validity Check Policy

time check …

Certificate validity comprises: CA signature, whether certificate is canceling and whether it is during valid period.

```
vpn(ca-identity)# time check { off | on }
```

Parameter	Description
Off	Ignore certificate validity check, to guarantee network usability.
On	Check certificate validity, to guarantee security.

(Configuration mode) CA identity configuration mode
(default configuration)off,ignore validity check.

If check certificate validity, configure system and CA server time.

Retrieve & Authenticate CA Server Certificate

```
crypto ca authenticate …
```

Auto retrieve CA certificate, to authenticate its validity.

```
vpn(config)#crypto ca authenticate ca_name
```

Parameter	Description
ca_name	CA trust area name

(Configuration mode) global configuration mode
(default configuration)off,no strict check

(for example)
Such as following, after executing the command, system will print CA information and finger mark for authentication.

```
VPN(config)#crypto ca authenticate mpca

% The Root CA Certificate has the following attributes:
       Serial Number: 25A56A1B3E851D804BDD7CD3C1228FA2
       Subject: C=CN, CN=WIN2003 2003-10-27
       Issuer : C=CN, CN=WIN2003 2003-10-27
       Validity
       Start date: 2003-10-27 07:19:18
       End   date: 2005-10-27 07:28:54
       Usage: Sign
       Fingerprint(md5) :4077c8a7 79f0d875 e9e81567 0f159aad
       Fingerprint(sha1):b0428783  3dcc2c3c  83ef044a  cacf091d
09b9aabc

% Do you accept this certificate?[yes]/[no]:y
% PKI: Get CA certificate success.
```

Online Certificate Application

crypto ca enroll …

Initiate certificate requirement to CA via online application mode.

```
vpn(config)#crypto ca enroll ca_name key_len user_name
```

Parameter	Description
ca_name	CA trust area name
Key_len	Certificate encryption key length, 512,1024,2048 bit.
User_name	Certificate user name

(Configuration mode) global configuration mode

(Example 1)CA server passes certificate requirement

Command	Description
VPN(config)#crypto ca enroll mpca 1024 zhouq.signamax.com % The Certificate DN will be: CN=zhouq.signamax.com % Waiting,Generate private key now,Key length 1024! % Generating .. Done. % PKI: Certificate enroll success.	Execute the command New certificate host name Encryption key generating process Application success

(Example 2)certificate requirement should be checked by CA administrator:

Command	Description
% Need to retrive the certificate after it's issued. …… VPN(config)#crypto ca retrive mpca % Auto retrive certificate: CN=vpn1.signamax.com % PKI: Cert-retrive success.	After passing the application via administrator, get the certificate via this command.(retrive details refer to next section.)

Some CA get user certificate after registering, such as mpcms, but others like CTCA,Windows CA should be according to CA configuration. If CA needs the check of administrator, the following command can be used.

Retrieve Certificate

This configuration is used for applying certificate from Windows CA or CTCA. CA administrator needs to check the requirement.

crypto ca retrive …

Download certificate from CA server.

```
vpn(config)#crypto ca retrive ca_name
```

Parameter	Description
Ca_name	CA trust area name

(Configuration mode) global configuration mode

Offline Certificate Application and Import

```
crypto ca pkcs10-enroll …
```

Via PKCS10 offline certificate application, system supports any third party CA.

```
vpn(config)# crypto ca pkcs10-enrollca_name key_len user_name
```

Parameter	Description
Ca_name	CA trust area name
Key_len	Encryption length, 512,1024,2048 bit
User_name	Certificate user name

(Configuration mode) global configuration mode

(**Example**)

Command	Description
VPN(config)#crypto ca pkcs10-enroll mpca 1024 vpn2.signamax.com % The Certificate DN will be: CN=vpn2.signamax.com % Waiting,Generate private key now,Key length 1024! % Generating .. Done. Generate PKCS10 request success,send it to ca. After CA issue the certificate,import it by commond 'crypto ca import certificate'. PKCS10 request is: -----BEGIN CERTIFICATE REQUEST----- MIIBdjCB4AIBADAZMRcwFQYDVQQDEw52cG4yLm1haXB1LmNvbTCBnjANBgkqhkiG 9w0BAQEFAAOBjAAwgYgCgYBKxKHl70rsXJ7VmU0fJGb8TFKaFwrh9Mdr+okg6/F3 UNcvnyCpoby2ilF55hfYuyL9++MQvKZ1v6qdJTB5SL7PXL0dRZWkgNjmsEDcGAal FPb09nBwPsuNJLfmUhNpNTagWcAG9G0y3BbQv+APyEi2e4NvANNBZXd/n/dLx+NW wQIDAQABoB8wHQYJKoZIhvcNAQkOMRAwDjAMBgNVHQ8EBQMDALAAMA0GCSqGSIb3 DQEBBQUAA4GBACNGoIdRVkM78KuY8AvCrzHjf7933JMcdyiFPCvAIz7GTrVTILdm /Ng8WM8VWHJGpFzkk2x2YIc8E0wZYwYPtffhKRb72emy4273wg/ppZ4JyE/FTENl ZasUTFewuqrgFEkJCwojkptaKGfq4JuOEbQ/4Fb/QUe/DtWkOWn1XEWF -----END CERTIFICATE REQUEST-----	PKCS10 certificate application certificate host name encryption key

■ **crypto ca import …**

Import CA certificate, CRL,or user certificate via PKCS10.

```
vpn(config)# crypto ca import certificate [to ca_name]
vpn(config)# crypto ca import crl [to ca_name]
```

Parameter	Description
Ca_name	Designate import some CA trust area
Certificate	Import certificate
Crl	Import CRL

(Configuration mode) global configuration mode

(**Example**)

Command	Description
VPN(config)# crypto ca import certificate to mpca % Input the certificate data,Press <Enter> twice to finish: -----BEGIN CERTIFICATE----- MIIDbzCCAxmgAwIBAgIKA/KQaAAAAAAArTANBgkqhkiG9w0BAQUFADAqMQswCQYD VQQGEwJDTjEbMBkGA1UEAxMSV0lOMjAwMyAyMDAzLTEwLTI3MB4XDTA0MDgwMTA4 NDYyMloXDTA1MDgwMTA4NTYyMlowGTEXMBUGA1UEAxMOdnBuMi5tYWlwdS5jb20w gZ4wDQYJKoZIhvcNAQEBBQADgYwAMIGIAoGASsSh5e9K7Fye1ZlNHyRm/ExSmhcK 4fTHa/qJIOvxd1DXL58gqaG8topReeYX2Lsi/fvjELymdb+qnSUweUi+z1y9HUWV pIDY5rBA3BgGpRT29PZwcD7LjSS35lITaTU2oFnABvRtMtwW0L/gD8hItnuDbwDT QWV3f5/3S8fjVsECAwEAAaOCAe0wggHpMAwGA1UdDwQFAwMAsAAwHQYDVR0OBBYE FAW2FHKN4ZVAfGBPALQndvDP2+skMGEGA1UdIwRaMFiAFJ8251OamBcKFTysP3+N /hFRUj2NoS6kLDAqMQswCQYDVQQGEwJDTjEbMBkGA1UEAxMSV0lOMjAwMyAyMDAz LTEwLTI3ghAlpWobPoUdgEvdfNPBIo+iMIGRBgNVHR8EgYkwgYYwQKA+oDyGOmh0 dHA6Ly96cS04NHlza2l5ZzV5OW8vQ2VydEVucm9sbC9XSU4yMDAzJTIwMjAwMy0x MC0yNy5jcmwwQqBAoD6GPGZpbGU6Ly9cXHpxLTg0eXNraXlnNXk5b1xDZXJ0RW5y	Stick certificate information to system, and then press enter key.

b2xsXFdJTjIwMDMlMjAyMDAzLTEwLTI3LmNybDCBwgYIKwYBBQUHAQEEgbUwgbIwVgYIKwYBBQUHMAKGSmh0dHA6Ly96cS04NHlza2l5ZzV5OW8vQ2VydEVucm9sbC96cS04NHlza2l5ZzV5OW9fV0lOMjAwMyUyMDIwMDMtMTAtMjcuY3J0MFgGCCsGAQUFBzAChkxmaWxlOi8vXFx6cS04NHlza2l5ZzV5OW9cQ2VydEVucm9sbFx6cS04NHlza2l5ZzV5OW9fV0lOMjAwMyUyMDIwMDMtMTAtMjcuY3J0MA0GCSqGSIb3DQEBBQUAA0EARiQ9HdCdIKLk12JcSK/fGDGw0gPQHQbKvjglB/52xcm9GkTYIU5x36nC6GJuc/2Sb9AmXdPIVAv9QZMyMccbNw==

-----END CERTIFICATE-----

% PKI: Import Certificate success.

Obtain certificate revocation list

- **crypto ca crl request …**

Download certificate revocation list from CA server.

```
vpn(config)# crypto ca crl request ca_name
```

Parameter	Description
Ca_name	CA trust area name

```
(Configuration mode) global configuration mode
```

25.5.7 Set certificate trust status

- **crypto ca certificate trust | autotrust | untrust …**

Set certificate status as auto check.

```
vpn(config)# crypto ca certificate trust ca_name {name
cert_name| sn cert_sn}
vpn(config)# crypto ca certificate autotrust ca_name {name
cert_name| sn cert_sn}
vpn(config)# crypto ca certificate untrust ca_name {name
cert_name| sn cert_sn}
```

Parameter	Description
Trust	Trust some certificate.
Autotrust	Auto judge certificate validity according to policy
Untrust	Untrust the certificate
Ca_name	Certificate serial number.
Cert_name	According to certificate name
Cert_sn	According to certificate serial number

(Configuration mode) global configuration mode

1. (**default configuration**)auto judge certificate validity.

Delete local saved certificate

```
no crypto ca certificate …
```

Delete system certificate.

```
vpn(config)# no crypto ca certificate ca_name name cert_name
vpn(config)# no crypto ca certificate ca_name sn cert_sn
vpn(config)# no crypto ca certificate ca_name type cert_type
(parameter descripiton)
```

Parameter	Description
ca_name	CA trust area name
Cert_name	Delete according to certificate name
Cert_sn	Delete according to serial number
Cert_type	Delete some certificate, including all all certificates

crl	CRL
my	my certificate
remote	peer certificate
requesting	requesting certificate
root	root CA certificate

(Configuration mode) global configuration mode

(**Example**)

VPN(config)#no crypto ca certificate mpca name vpn1.signamax.com

Certificate display

■ **show crypto ca identity**

Display CA information.

```
vpn(config)# show crypto ca identity
(Configuration mode)  global configuration mode
```

■ **show crypto ca certificate ◦ ◦ ◦**

Display certificate

```
show crypto ca certificate { pem | der | general}
```

Parameter	Description
Pem	Display certificate in the form of PEM
Der	Display certificate in the form of 16 bit
General	Display certificate in the form of general read

```
(Configuration mode)  global configuration mode
```

(**default configuration**) General

■ **show crypto ca crl …**

Display certificate revocation list

```
show crypto ca crl { pem | der | general}
```

Parameter	Description
Pem	Display CRL in the form of PEM
Der	Display CRL in the form of 16 bit
General	Display CRL in the form of general read

(Configuration mode) global configuration mode
(default configuration) General

Configure solution

(Site-to-Site) VPN

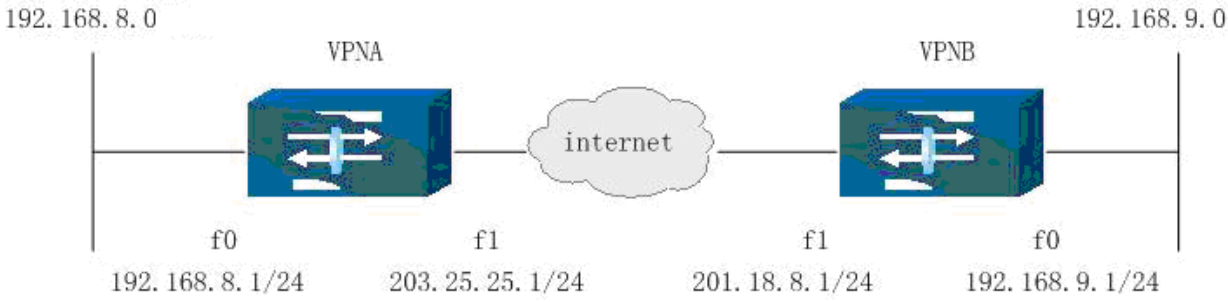


Figure 25-3

🕮 Illustration:

1, security gateway A connects 192.168.8.0/24 via f0, and f0 address is 192.168.8.1/24.
2 security gateway B connects 192.168.9.0/24 via f0, and f0 address is 192.168.9.1/24.
3, VPNA f1 address is 203.25.25.1/24 gateway is 203.25.25.254; VPNB f1 address is 201.18.8.1/24,gateway is 201.18.8.254.

The configuration of security gateway A:

Command	Description
VPNA(config)#crypto ike key key123 address 201.18.8.1	Suppose pre-share encryption is key123,the default peer ID is IP address.
VPNA(config)#crypto tunnel tun1 VPNA(config-tunnel)#peer address 201.18.8.1 VPNA(config-tunnel)#local address 203.25.25.1	Configure VPN tunnel, other configuration such as proposal, lifetime are optional.

VPNA(config-tunnel)#set auto-up VPNA(config-tunnel)#exit	
VPNA(config)#crypto policy p1 VPNA(config-policy)#flow 192.168.8.0 255.255.255.0 192.168.9.0 255.255.255.0 ip tunnel tun1 VPNA(config-policy)#exit	If tun1 configures auto negotiation, VPNA will initiates auto negotiation to VPNB.
VPNA (config)#ip route 0.0.0.0 0.0.0.0 203.25.25.254	Configure routing.
The following is optional:	
VPNA(config)# crypto ca identity mpca VPNA(ca-identity)# enrollment address 203.25.25.2 VPNA(ca-identity)# ca type win VPNA(ca-identity)#exit	If adopting certificate authentication, first complete certificate configuration and application, and use them for VPN tunnel configuration.
VPNA(config)#crypto ca authenticate mpca VPNA(config)#crypto ca enroll mpca 1024 vpna.sec.com	User name is vpna.sec.com, encryption key is 1024 bit certificate.
VPNA(config)#crypto tunnel tun1 VPNA(config-tunnel)#set authentication rsa-sig VPNA(config-tunnel)#exit	Designate digital signature authentication in tunnel.
VPNA(config)#crypto ike-proposal ikep1 VPNA(config-ike-prop)#encryption 3des VPNA(config-ike-prop)#integrity sha2-256 VPNA(config-ike-prop)#exit VPNA(config)#crypto IPsec-proposal secp1 VPNA(config-IPsec-prop)#esp aes192 sha1 VPNA(config-IPsec-prop)#exit	Configure IKE proposal and IPsec proposal, and ue it in the tunnal configuration.
VPNA(config)#crypto tunnel tun1 VPNA(config-tunnel)# set ike-proposal ikep1 VPNA(config-tunnel)# set IPsec-proposal secp1 VPNA(config-tunnel)#exit	

Security gateway B configuration:

Command	Description
VPNB(config)#crypto ike key key123 address 203.25.25.1	Configure pre-share encryption key
VPNB(config)#crypto tun tun1 VPNB(config-tunnel)#peer address 203.25.25.1 VPNB(config-tunnel)#local address 201.18.8.1 VPNB(config-tunnel)#exit	Configure VPN tunnel.
VPNB(config)#crypto policy p1 VPNB(config-policy)#flow 192.168.9.0 255.255.255.0 192.168.8.0 255.255.255.0 ip tunnel tun1 VPNB(config-policy)#exit	Designate policy.
VPNB(config)#ip route 0.0.0.0 0.0.0.0 201.18.8.254	Configure routing.

🕮 **Note**:

The data flow from 192.168.8.0 to 192.168.9.0 uses IPsec tunnel.

Dynamic Dial-up VPN

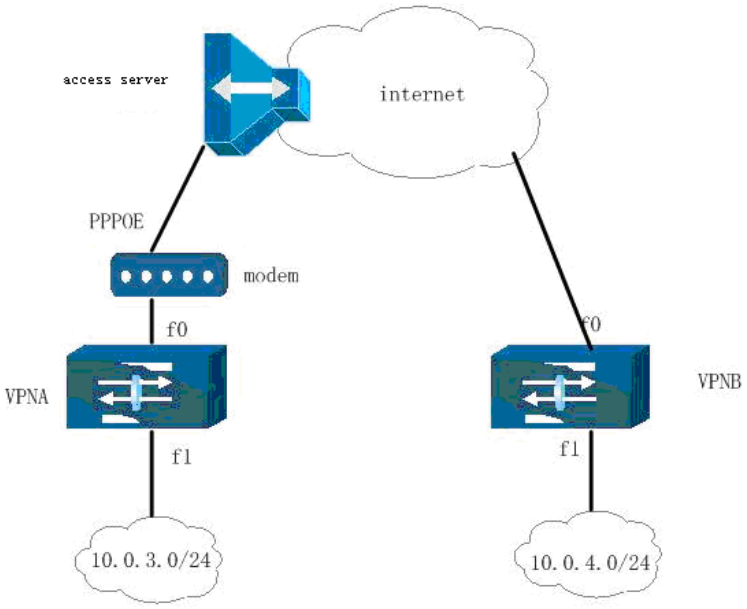


Figure 25-4

🕮 **Illustration**:

1, VPNA connects 10.0.3.0/24 via f1, and f1 address is 10.0.3.1,f0 gets the IP address via ISP access server. And each IP is different.
2, VPNB connects 10.0.4.0/24 via f1, and f1 address is 10.0.4.1,f0 has fixed IP address 128.255.1.1.
3, VPNA sets IPsec tunnel to VPNB, to protect the data flow of 10.0.3.0/24～10.0.4.0/24.
4, 10.0.3.0/24 and 10.0.4.0/24 need nat transform when accessing network.

VPNA configuration:

Command	Description
VPNA(config)# cry ike key key123 identity vpnb.signamax.com	Suppose pre-share encryption key is key123,peer ID is vpnb.signamax.com.
VPNA(config)#crypto tunnel tun1 VPNA(config-tunnel)#peer address 128.255.1.1 VPNA(config-tunnel)#local interface d0 VPNA(config-tunnel)#set local-id vpna.signamax.com VPNA(config-tunnel)#set mode aggressive VPNA(config-tunnel)#exit	Configure VPN tunnel, if adopting pre-share authentication, IP address cannot be used as local ID, and configure local ID as vpna.signamax.com.
VPNA(config)#crypto policy p1	Configure policy

VPNA(config)#flow 10.0.3.0 255.255.255.0 10.0.4.0 255.255.255.0 ip tunnel tun1	
VPNA(config)#exit	
VPNA(config)# dialer-list 1 protocol ip permit	Define dial-up data flow
VPNA(config)# interface dialer0	Define and configure dial-up interface.
VPNA(config-if-dialer0)# ip address negotiated	
VPNA(config-if-dialer0)# dialer in-band	
VPNA(config-if-dialer0)# dialer pool 1	
VPNA(config-if-dialer0)# dialer-group 1	
VPNA(config-if-dialer0)# encapsulation ppp	
VPNA(config-if-dialer0)# ppp pap sent-username 01234@169 password 01234mp	
VPNA(config-if-dialer0)#exit	
VPNA(config)#int f0	Define f0 as PPPOE physical interface.
VPNA(config-if-fastethernet0)#pppoe-client dial-pool-number 1	
VPNA(config-if-fastethernet0)#exit	
VPNA(config)#int f1	Configure f1 interface address.
VPNA(config-if-fastethernet1)#ip address 10.0.3.1 255.255.255.0	
VPNA(config-if-fastethernet1)#exit	
VPNA (config)# ip route 0.0.0.0 0.0.0.0 dialer0	Configure routing.

When 10.0.3.0 access network, it needs nat transform, and nat configuration is as following:

VPNA(config)#access-list 1002 deny ip 10.0.3.0 0.0.0.255 10.0.4.0 0.0.0.255	Set access list 1002,when data flow is from 10.0.3.0 to 10.0.4.0, there is no need for nat transform. But it needs nat transform when 10.0.3.0 0.0.0.255 accesses network.
VPNA(config)#access-list 1002 permit ip 10.0.3.0 0.0.0.255 any	
VPNA(config)#ip nat inside source list 1002 interface f0	List 1002 transforms with f0.
VPNA(config)#interface f1	Designate f1 interface
VPNA(config-if-fastethernet1)#ip nat inside	Mark inside connecting interface.
VPNA(config-if-fastethernet1)#exit	
VPNA(config)#interface d0	Designate d0 interface
VPNA(config-if-dialer0)#ip nat outside	Mark outside connecting interface.
VPNA(config-if-dialer0)#exit	

VPNB configuration is as following:

Command	Description
VPNB(config)# cry ike key key123 identity vpna.signamax.com	Configure pre-share encryption key.
VPNB(config)#crypto tunnel tun1	VPNB uses as response party, no need
VPNB(config-tunnel)#local interface f0	to configure peer address, only
VPNB(config-tunnel)#set local-id vpnb.signamax.com	configure local outbound interface as

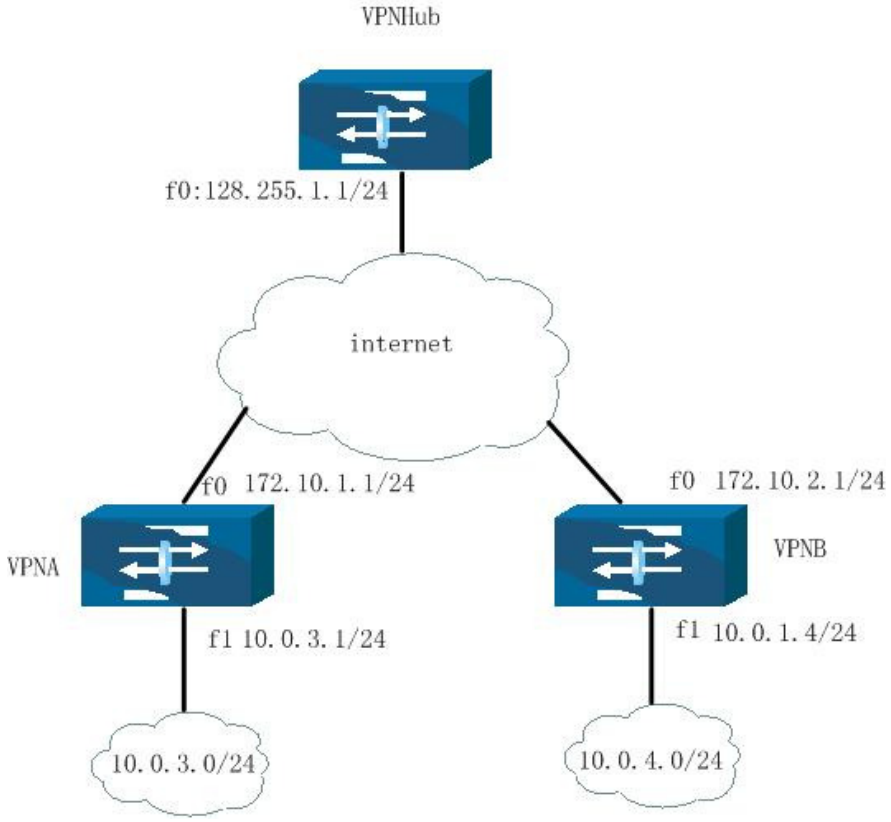
VPNB(config-tunnel)#exit	f0, local ID as vpnb.signamax.com.
VPNB(config)#crypto policy p1	Configure policy.
VPNB(config)#flow 10.0.4.0 255.255.255.0 10.0.3.0 255.255.255.0 ip tunnel tun1	
VPNB(config)#exit	
VPNB(config)#int f0	Configure interface f0 address.
VPNB(config-if-fastethernet0)#ip addr 128.255.1.1 255.255.255.0	
VPNB(config-if-fastethernet0)#exit	
VPNB(config)#int f1	Configure f1 interface address.
VPNB(config-if-fastethernet1)#ip address 10.0.4.1 255.255.255.0	
VPNB(config-if-fastethernet1)#exit	
VPNB (config)# ip route 0.0.0.0 0.0.0.0 128.255.1.254	Configure default routing.

10.0.4.0 accessing network needs nat transform, and nat configuration is as following:

VPNA(config)#access-list 1002 deny ip 10.0.4.0 0.0.0.255 10.0.3.0 0.0.0.255 VPNA(config)#access-list 1002 permit ip 10.0.4.0 0.0.0.255 any	Set access list 1002,there is no nat transform when data flow is from 10.0.4.0 to 10.0.3.0, but it needs when 10.0.4.0 0.0.0.255 accesses network.
VPNA(config)#ip nat inside source list 1 interface f0	List 1002 transforms with f0
VPNA(config)#interface f1	Designate interface f1.
VPNA(config-if-fastethernet1)#ip nat inside	Mark as inside connecting interface.
VPNA(config-if-fastethernet1)#exit	
VPNA(config)#interface f0	Designate interface f0.
VPNA(config-if-fastethernet0)#ip nat outside	Mark as outside connecting interface.
VPNA(config-if-fastethernet0)#exit	

Virtual Security Domain VPN

The topology of VPN is a typical Hub-and-Spoke VPN.



VPNA and VPNB can be considered as the same enterprise security gateway equipment, and connected with Internet; the central VPNHub can be considered as operator VPN integrated machine. VPNA and VPNB set up IPsec tunnel with VPNHub, and the subnet of VPNA and VPNB communication is via these two IPsec tunnel.

VPNA subnet is 10.0.3.0/24; VPNB subnet is 10.0.4.0/24.

VPNC and VPND can be added in above topology figure, and the configuration is the same.

VPNHub configuration:

Command	Description
VPNHub(config)# cry ike key key123 identity *.signamax.com	Configure pre-share encryption key;
VPNHub(config)#crypto tunnel tun1 VPNHub(config)#local interface f0 VPNHub(config-tunnel)# set peer identity *.signamax.com VPNHub(config-tunnel)# set virtual-domain-id signamax VPNHub(config-tunnel)#exit	Configure peer dynamic tunnel, suppose VPNA and VPNB ID satisfy "*.signamax.com",which is to say distributing virtual security area according to ID; configure virtual security area mark as signamax.
VPNHub(config)#crypto policy p1 VPNHub(config-policy)#flow 10.0.3.0 255.255.255.0 10.0.4.0 255.255.255.0 ip tunnel tun1 VPNHub(config-policy)#exit VPNHub(config)#crypto policy p2 VPNHub(config-policy)#flow 10.0.4.0 255.255.255.0 10.0.3.0 255.255.255.0 ip tunnel tun1 VPNHub(config-policy)exit	Configure two policy, and define the data flow information between VPNA and VPNB.
VPNHub(config)#cry ike key key123 identity *.signamax.com seed VPNHub(config)#cry ike generate-key identity vpna.signamax.com *.signamax.com The derived key for ISAKMP ID 'vpna.signamax.com' is: The preshare key is: y3WpsWI9xDMbTyPYI9rtlg== VPNHub(config)#cry ike generate-key identity vpnb.signamax.com *.signamax.com The derived key for ISAKMP ID 'vpnb.signamax.com' is: The preshare key is: 7DHUAPpgixHcVlBISLAuXg==	If adopting pre-share encryption key and accessing control the equipment, configure seed encryption key, and creates VPNA share encryption key according to VPNA ID(vpna.signamax.com) .
VPNHub (config)# ip route 0.0.0.0 0.0.0.0 f0	Configure routing.

VPNA configuration:

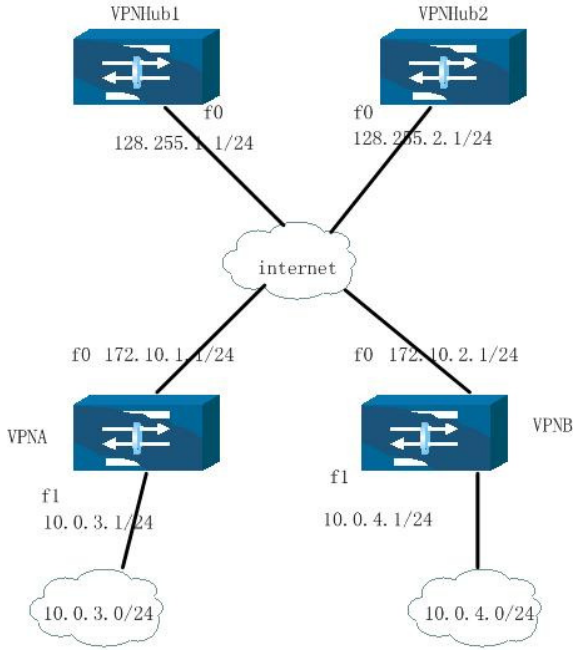
Command	Description
VPNA(config)# cry ike key key123 address 128.255.1.1	If adopting pre-share encryption key authentication policy, configure pre-share encryption key;
VPNA(config)#cry ike key y3WpsWI9xDMbTyPYI9rtlg== address 128.255.1.1	If VPNHub adopts seed encryption key, configure ID pre-share encryption key.
VPNA(config)#crypto tunnel tun1 VPNA(config-tunnel)#peer address 128.255.1.1 VPNA(config-tunnel)#local address 172.10.1.1 VPNA(config-tunnel)#set local-id vpna.signamax.com VPNA(config-tunnel)# set mode aggressive VPNA(config-tunnel)#exit	Configure VPN tunnel, and configure local ID as vpna.signamax.com.
VPNA(config)#crypto policy p1 VPNA(config-policy)#flow 10.0.3.0 255.255.255.0 10.0.4.0 255.255.255.0 ip tun tun1 VPNA(config-policy)#exit	
VPNA (config)# ip route 0.0.0.0 0.0.0.0 128.255.1.254	Configure default routing.

VPNB configuration is similar with above.

Load balance VPN

Load balance uses for above Hub-and-Spoke network. IPsec communication is forwarded via central VPN concentrator. And so we add many VPN concentrators to reach the balance status.

1. network environment:



Configure two VPN concentrators VPNHub1 and VPNHub2 in the center, and their f0 addresses are 128.255.1.1/24 and 128.255.2.1/24.
VPNA and VPNB configuration is similar with 19.4.3 virtual security area VPN. VPNA, VPNHub1 and VPNHUb2 set up IPsec tunnel to data flow 10.0.3.0/24～10.0.4.0/24.

2. Configuration steps:

VPNA configuration is as following and VPNB configuration is similar.

Command	Description
VPNA(config)# cry ike key key123 address 128.255.1.1	Configure pre-share encryption key.
VPNA(config)#cry ike key y3WpsWI9xDMbTyPYI9rtlg== address 128.255.1.1	If VPNHub adopts seed encryption key for access controlling (referring to VPNHub configuration), configure pre-share encryption key.
VPNA(config)#crypto tunnel tun1 VPNA(config-tunnel)#peer address 128.255.1.1 VPNA(config-tunnel)#local address 172.10.1.1 VPNA(config-tunnel)#set local-id vpna.signamax.com VPNA(config-tunnel)# set mode aggressive VPNA(config-tunnel)#exit VPNA(config)#crypto tunnel tun2 VPNA(config-tunnel)#peer address 128.255.2.1 VPNA(config-tunnel)#local address 172.10.1.1 VPNA(config-tunnel)#set local-id vpna.signamax.com VPNA(config-tunnel)# set mode aggressive VPNA(config-tunnel)#exit	Configure two VPN tunnels, and configure its peer address as 128.255.1.1 and 128.255.2.1; configure local ID as vpna.signamax.com.
VPNA(config)#crypto policy p1 VPNA(config-policy)#flow 10.0.3.0 255.255.255.0 10.0.4.0 255.255.255.0 ip tun tun1 tun2 payload-balance VPNA(config-policy)#exit	Configure policy, and the data flow is via tun1 and tun2. payload-balance is the balance.
VPNA (config)# ip route 0.0.0.0 0.0.0.0 172.10.1.254	Configure routing.

VPNHub1 and VPNHub2 configurations are similar with peer dynamic tunnel configuration.

Command	Description
VPNHub1(config)# cry ike key key123 identity *.signamax.com	Configure pre-share encryption key.
VPNHub1(config)#crypto tunnel tun1 VPNHub1(config)#local interface f0 VPNHub1(config-tunnel)# set peer identity	Configure peer dynamic tunnel, and suppose VPNA and VPNB ID satisfy

*.signamax.com VPNHub1(config-tunnel)# set virtual-domain-id signamax VPNHub1(config-tunnel)#exit	"*.signamax.com", Which is to say, distribute all virtual security areas according to ID; configure security mark as signamax.
VPNHub1(config)#crypto policy p1 VPNHub1(config-policy)#flow 10.0.3.0 255.255.255.0 10.0.4.0 255.255.255.0 ip tunnel tun1 VPNHub1(config-policy)#exit VPNHub1(config)#crypto policy p2 VPNHub1(config-policy)#flow 10.0.4.0 255.255.255.0 10.0.3.0 255.255.255.0 ip tunnel tun1 VPNHub(config-policy)exit	Configure two policy, which is via the data information between VPNA and VPNB.
VPNHub1(config)#cry ike key key123 identity *.signamax.com seed VPNHub1(config)#cry ike generate-key identity vpna.signamax.com *.signamax.com The derived key for ISAKMP ID 'vpna.signamax.com' is: The preshare key is: y3WpsWI9xDMbTyPYI9rtlg== VPNHub(config)#cry ike generate-key identity vpnb.signamax.com *.signamax.com The derived key for ISAKMP ID 'vpnb.signamax.com' is: The preshare key is: 7DHUAPpgixHcVlBISLAuXg==	If adopting pre-share encryption key and accessing control the equipment, configure seed encryption key, and creates VPNA share encryption key according to VPNA ID(vpna.signamax.com) .
VPNHub (config)# ip route 0.0.0.0 0.0.0.0 f0	Configure routing

Backup Gateway Configuration Example

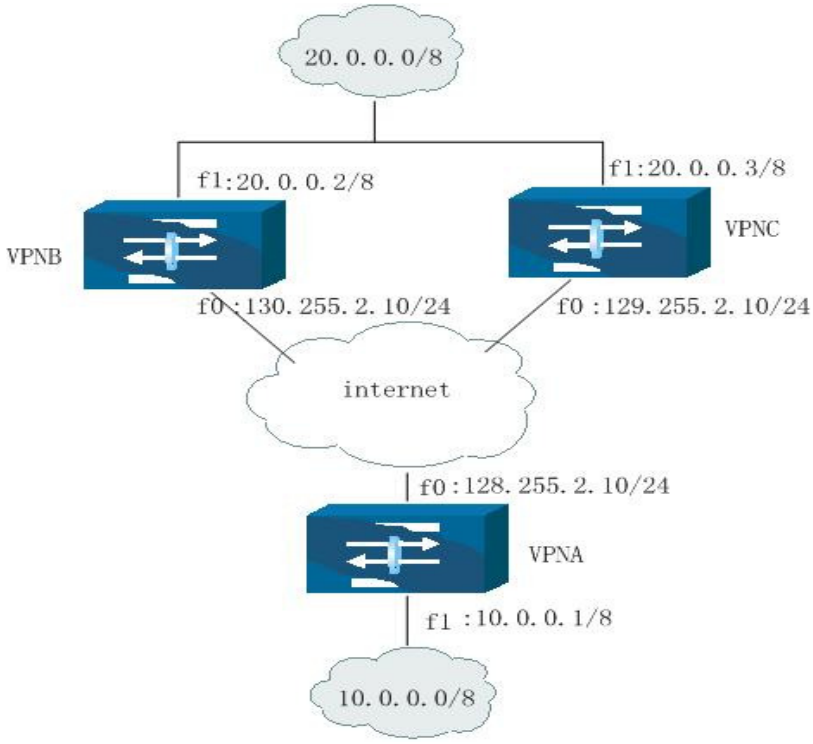


Figure 25-20

PNA f1 connects 10.0.0.0/8; VPNB, VPNC f1 connect 20.0.0.0/8.

VPNA may set tunnel together with VPNB and VPNC

The interface f1 of VPNB and VPNC use the same virtual IP: 20.0.0.5/8,20.0.0.0/8 subnet gateway is configured as this virtual IP. When f1 of VPNB is down, the data flow auto uses the tunnel set up by VPNA and VPNC. VPNA default gateway is 128.255.2.254/24,VPNB default gateway is 130.255.2.254/24 and VPNC default gateway is 129.255.2.254/24.

Security gateway A configuration:

Command	description
VPNA(config)# cry ike key signamax address 130.255.2.10 VPNA(config)# cry ike key signamax address 129.255.2.10	Configure pre-share encryption key;
VPNA(config)#crypto tunnel tun1 VPNA(config-tunnel)#peer address 130.255.2.10 VPNA(config-tunnel)#local address 128.255.2.10 VPNA(config-tunnel)#exit VPNA(config)#crypto tunnel tun2	Configure two VPN tunnels.

VPNA(config-tunnel)#peer address 129.255.2.10 VPNA(config-tunnel)#local address 128.255.2.10 VPNA(config-tunnel)#exit	
VPNA(config)# crypto policy p1 VPNA(config-policy)# flow 10.0.0.0 255.0.0.0 20.0.0.0 255.255.255.0 ip tunnel tun1 tun2 VPNA(config-policy)#exit	Configure policy
VPNA (config)# ip route 0.0.0.0 0.0.0.0 128.255.2.254	Configure default routing.

Security gateway B configuration is:

Command	Description
VPNB (config)# cry ike key key123 address 128.255.2.10	Configure pre-share encryption key;
VPNB(config)#crypto tunnel tun1 VPNB(config-tunnel)# peer address 128.255.2.10 VPNB(config-tunnel)# local address 130.255.2.10 VPNB(config-tunnel)#exit	Configure VPN tunnel.
VPNB(config)# crypto policy p1 VPNB(config-policy)# flow 20.0.0.0 255.255.255.0 10.0.0.0 255.0.0.0 ip tunnel tun1 VPNB(config-policy)#exit	Configure policy
VPNB (config)#int f1 VPNB (config-if-fastethernet1)#ip address20.0.0.2 255.0.0.0 VPNB (config-if-fastethernet1)#standby 1 ip 20.0.0.5 VPNB (config-if-fastethernet1)#standby 1 priority 110 VPNB (config-if-fastethernet1)#standby 1 track f0 10 VPNB (config-if-fastethernet1)#standby 1 preempt delay 10 VPNB (config-if-fastethernet1)#exit	If needed, configure f1 interface address. Configure VBRP group number and virtual ip. Configure VBRP priority level Listen f0, when f0 is down, priority level reduces 10
VPNB (config)# ip route 0.0.0.0 0.0.0.0 130.255.2.254	Configure default routing.
	The following is gateway keepalive configuration.
VPNB (config)#int f0	
VPNB (config-if-fastethernet0)# keepalive 5 gateway 130.255.2.254	f0 checks gateway is down or up every 5 seconds (optional), if gateway is down, f0 is down while gateway is up, f0 is up.
VPNB (config-if-fastethernet0)#exit	

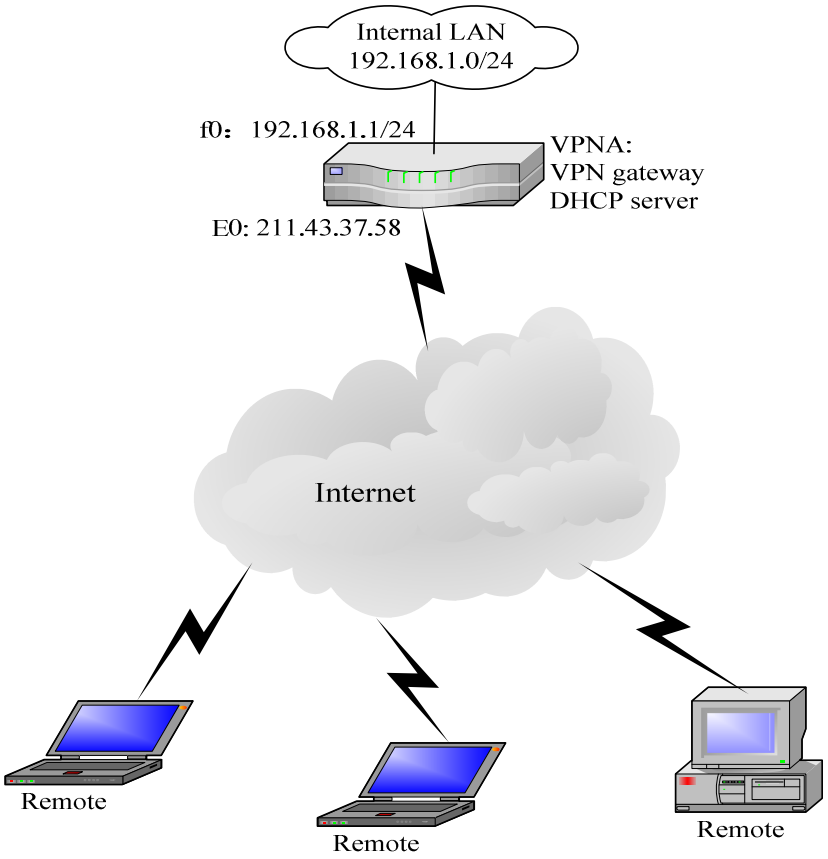
security gateway C configuration is as following:

Command	Description
VPNB (config)# cry ike key key123 address 128.255.2.10	Configure pre-share encryption key.
VPNB(config)#crypto tunnel tun1 VPNB(config-tunnel)# peer address 128.255.2.10 VPNB(config-tunnel)# local address 129.255.2.10 VPNB(config-tunnel)#exit	Configure VPN tunnel.
VPNB(config)# crypto policy p1 VPNB(config-policy)# flow 20.0.0.0 255.255.255.0 10.0.0.0 255.0.0.0 ip tunnel tun1 VPNB(config-policy)#exit	Configure policy
VPNC (config)#int f1	Configure f1 interface address.

VPNC (config-if-fastethernet1)#ip address20.0.0.3 255.0.0.0 VPNC (config-if-fastethernet1)# standby 1 ip 20.0.0.5 VPNC (config-if-fastethernet1)#standby 1 track f0 10 VPNC (config-if-fastethernet1)#standby 1 preempt delay 10 VPNC (config-if-fastethernet1)#exit	Configure VBRP group number and virtual ip. Listen to f0, when f0 is down, the priority level reduces 10. Set preempt mode and delay 10 seconds.
VPNC (config)# ip route 0.0.0.0 0.0.0.0 129.255.2.254	Configure default routing.
	The following is gateway keepalive configuration.
VPNC (config)#int f0	
VPNC (config-if-fastethernet0)# keepalive 5 gateway 129.255.2.254	f0 checks gateway is down or up every 5 seconds (optional), if gateway is down, f0 is down while gateway is up, f0 is up.
VPNC (config-if-fastethernet0)#exit	

The configuration to VBRP refers to VBRP configuration; VPN3020B is going to support gateway keepalive function.

DHCP over IPsec Configuration Example



VPNA uses as VPN gateway and DHCP server. DHCP server administrating address is 192.168.1.10-192.168.1.20;

Remote user uses VRC connecting VPNA, and uses DHCP over IPsec function to get internal address.

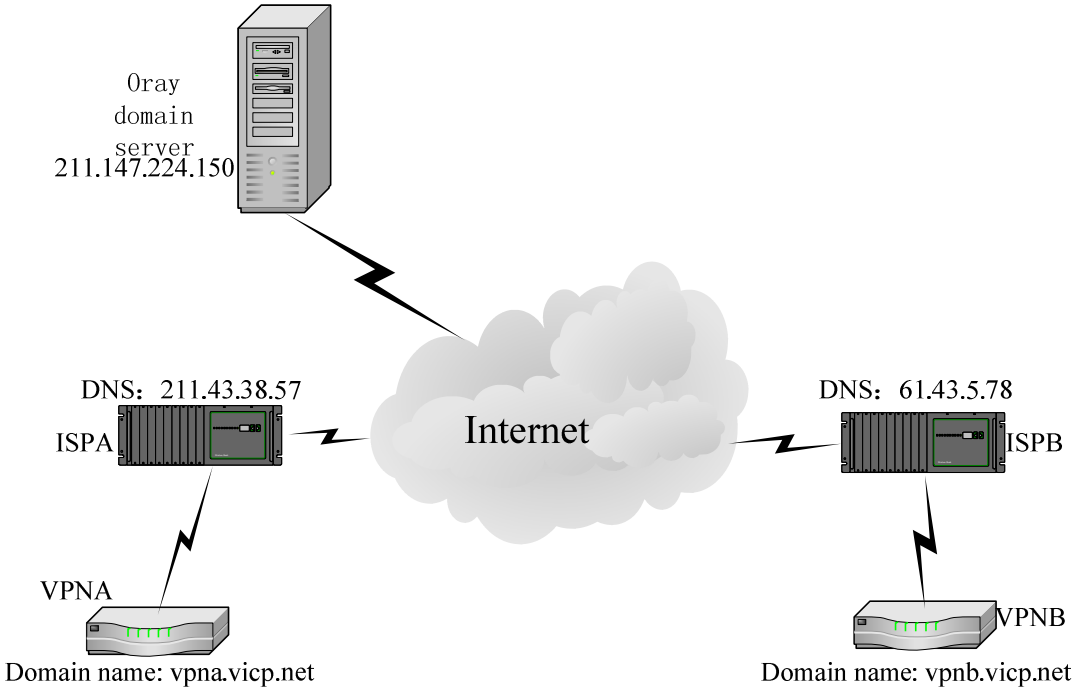
VPNA configuration:

Command	Description
VPNA(config)# ip dhcp pool vrc VPNA(dhcp-config)# range 192.168.1.10 192.168.1.20 VPNA(dhcp-config)# server-identifier interface f0 VPNA(dhcp-config)# default-router 192.168.1.1 VPNA(dhcp-config)# exit	Configure DHCP server Note: server-identifier cannot be dropped.
VPNA(config)# cry ike key signamax any	Configure pre-share encryption key.
VPNA(config)#crypto tunnel tun1 VPNA(config-tunnel)#peer any VPNA(config-tunnel)#local interface e0 VPNA(config-tunnel)#set dhcp-over-IPsec VPNA(config-tunnel)#exit	Configure a tunnel for DHCP over IPsec.
VPNA(config)# crypto policy p1 VPNA(config-policy)# flow 192.168.1.0	Configure policy

255.255.255.0 192.168.1.0 255.255.255.0 ip tunnel tun1 bypass VPNA(config-policy)#exit	

Configuration Example Combining with DHRP

DHRP realizes dynamic domain name registering and updating function. IPsec uses DHRP to complete IKE negotiation function.



VPNA connects Internet via ISP, and its address is ISPA distributed dynamic address, and ISPA provided DNS server address is 211.43.38.57,VPNA registers user name on Oray server: vpna, and password is: vpna-key123,domain name is vpna.vicp.net；

VPNB connects Internet via ISP, and its address is ISPB distributed dynamic address. ISPB provided DNS server address is 61.43.5.78,VPNB registers user name on Oray server: vpnb, password is vpnb-key123,domain name is vpnb.vicp.net；

The data flow between VPNA and VPNB is 192.168.1.0/24-

192.168.2.0/24.

VPNA configuration:

Command	Description
VPNA(config)# ip name-server 211.43.38.57	Designate DNS server
VPNA(config)# oray-ddns register user vpna VPNA(config-oray-ddns)# password vpna-key123 VPNA(config-oray-ddns)# server address 211.147.224.150 VPNA(config-oray-ddns)# domain-name vpna.vicp.net VPNA(config-oray-ddns)# exit	Configure DHRP
VPNA(config)# cry ike key signamax identity vpnb.vicp.net	Configure pre-share encryption key.
VPNA(config)#crypto tunnel tun1 VPNA(config-tunnel)#peer hostname vpnb.vicp.net VPNA(config-tunnel)#local interface f0 VPNA(config-tunnel)#set local-id vpna.vicp.net VPNA(config-tunnel)#set peer-id vpnb.vicp.net VPNA(config-tunnel)#exit	Configure a peer named tunnel.
VPNA(config)# crypto policy p1 VPNA(config-policy)# flow 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0 ip tunnel tun1 VPNA(config-policy)#exit	Configure policy

VPNB configuration:

Command	Description
VPNB(config)# ip name-server 61.43.5.78	Designate DNS server
VPNB(config)# oray-ddns register user vpnb VPNB(config-oray-ddns)# password vpnb-key123 VPNB(config-oray-ddns)# server address 211.147.224.150 VPNB(config-oray-ddns)# domain-name vpnb.vicp.net VPNB(config-oray-ddns)# exit	Configure DHRP
VPNB(config)# cry ike key signamax identity vpna.vicp.net	Configure pre-share encryption key.
VPNB(config)#crypto tunnel tun1 VPNB(config-tunnel)#peer hostname vpna.vicp.net VPNB(config-tunnel)#local interface f0 VPNB(config-tunnel)#set local-id vpnb.vicp.net VPNB(config-tunnel)#set peer-id vpna.vicp.net VPNB(config-tunnel)#exit	Configure a peer named tunnel.
VPNB(config)# crypto policy p1 VPNB(config-policy)# flow 192.168.2.0 255.255.255.0	Configure policy

192.168.1.0 255.255.255.0 ip tunnel tun1 VPNB(config-policy)#exit	

Software Upgrade

The software upgrade of Signamax router comprises two kinds of situations. One is the upgrade of the ROOT program (Namely Monitor or the root program), and its main functions include the management and allocation of the flash space, with the low upgrade-frequency; and the other is the upgrade of the program (IOS) in a router. When functions of the router need be expanded, the program (IOS) need be upgraded.

Upgrade of ROOT

Upgrade Hex File of ROOT Program via Console Interface

The function Hyper Terminal provided by Windows 95/98/NT is used to send the upgrading program to the router. The following will, taking example for the Hyper Terminal application in Windows, describe the upgrade process.

Step 1: Set the Hyper Terminal.

Start the Hyper Terminal application and select related serial port (such as COM 1) and set its attributes: 9600 baud rate, the soft flow control, eight data bits, no parity and one stop bit.

Step 2: Enter the Monitor mode.

If some information similar to "Monitor version 2.02 is Booting (^c enter monitor mode) ..." is displayed on the screen when the router starts up, you can press "CTRL+C" to enter the Monitor mode immediately. The prompt character of the mode is "mpMonitor:>" or "Monitor:>".

If no foregoing information is displayed on the screen when the router starts up, you need set the baud rate of the Hyper Terminal as 115200, restart the router, and then press the key ENTER to enter the Monitor mode.
Step 3:Reconfigure the speed of the Console interface and the Hyper Terminal to upgrade the hex file of the ROOT program.

When the prompt character "mpMonitor:>" or "Monitor:>" appears, the command "mpMonitor:>s 115200" is used to set the speed of the Console interface as 115200bps. At the same time, the speed of the Hyper Terminal is set as 115200bps (attribute-configuration-baud rate).

Stop the connection in the Hyper Terminal and start the connection again. Press "lr <CR>" behind "mpMonitor:>" and select the option 'Send text file' in the menu 'Transmit'. After the ROOT program (hex file) that will be upgraded is selected, its transmission starts. After the upgrade ends, set the attributes of the Hyper Terminal back to the initial setting, and restart it.

You can, according to information "Monitor version xxx is Booting (^c enter monitor mode) ...", judge whether the ROOT program is upgraded successfully.

Different modesof Signamax router may adopt different ROOT program. Before the ROOT program is upgraded, please affirm whether the ROOT program that need be upgraded is suit for the model of Signamax router lest the upgrading mistake make the router unusable.

After the ROOT program of Signamax low-end router is upgraded from

v1.xx to v2.xx or 3.xx, the MAC address of the router may be changed. To keep the MAC address exclusive and avoid the address conflict that may result in the network fault, please notice that one ROOT program can only be upgraded on one router.

To void the MAC address conflict resulting from upgrading ROOT as possible, the MAC address of the Ethernet interface of the router isn't changed after the ROOT program of Signamax low-end router is upgraded from v2.xx to v3.xx. If you want to change the MAC address, please refer to step 3----use the command "lr filename r <CR>" to upgrade the ROOT program. And the filename can be the combination of any letters.

Application IOS Upgrade

Signamax router provides three kinds of methods for the software upgrade. These methods can ceaselessly extend functions of the router. The following is to describe the three methods of the software upgrade.

Upgrade Bin File of Application via TFTP/FTP

Step 1: Run and configure the TFTP/FTP server.

Either Signamax TFTP server, CISCO TFTP or other TFTP/FTP server can be used to upgrade the bin file of application. We take example for Signamax TFTP server to describe the upgrade:

Open cisco TFTP server and click "TFTP server root-browse" to select directory of the IOS firmware.

Step 2: Make the TFTP server at the listening state.

Step 3: Connect the Network

Connect the PC serving as the TFTP server with the router via the Ethernet (or other manners) to assure both can ping each other.

Step 4: Upgrade the application

Enter "sysupdate <the address of the TFTP server> <the name of the file to be upgraded>" in the privilege user mode of the router. We take example for MP2692:

MP2692# sysupdate 128.255.32.10 mp2692.bin <CR>

Here, the router can prompt you: "Do you really update "mp2692.bin" ? (yes|no):". You can either enter "n <CR>" to cancel the operation or enter "y <CR>" to implement the operation to upgrade.

If you enter “y <CR>”, the router will prompt the following information:

```
■        “downloading "IOS" (2688708 Bytes):
##################################################
■        ##########################################################
############################
■          (Omitting the middle information)
■        OK
■        Download " mp2692.bin " (2707672 Bytes) succeeded
■        the flash is TE28F160C3T
■        erase flash ... success.
■        write flash ... success.
■        MP2692#
```

Information above indicates that IOS file is erased and written successfully. Now, you can reset the router.

Upgrade Bin File of Application via Console Interface

Step 1: Set the Hyper Terminal.

Start the Hyper Terminal program and select related serial (such as COM 1) and set its attributes: 9600 baud rate, the soft flow control, eight data bits, no parity and one stop bit.

Step 2: Enter the Monitor mode.

If some information similar to “Monitor version 2.02 is Booting (^c enter monitor mode) ...” is displayed on the screen when the router starts up, you can press “CTRL+C” to enter the Monitor mode immediately. The prompt character of the mode is “mpMonitor:>” or “Monitor:>”.

If no foregoing information is displayed on the screen when the router starts up, you need set the baud rate of the Hyper Terminal as 115200, restart the router, and then press the key ENTER to enter the Monitor mode.

Step 3 Erase the previous IOS.

Under the system prompt, use the commands "mpMonitor:>e p" or "mpMonitor:>e a" to erase the existing the IOS in the flash. The difference of the foregoing two commands is that the former only erases IOS while the latter erases both IOS and the configuration file. But, both don't erase the ROOT program, which can only be upgraded and can't be erased.

Step 4: Reconfigure the speed of the Console interface and the Hyper Terminal to upgrade the hex file of the application.

Use the command "mpMonitor:>s 115200" to set the speed of the Console interface of the router as 115200bps. At the same time, the speed of the Hyper Terminal is set as 115200bps (attribute-configuration-baud rate). Stop the connection in the Hyper Terminal and start the connection again. Press "lx <CR>" behind "mpMonitor:>" and select the option 'Send text file' in the menu 'Transmit'. Select 'xModem protocol' in the pop-up dialog box. After the IOS program (hex file) that will be upgraded is selected, its transmission starts. After the upgrade ends, set the attributes of the Hyper Terminal back to the initial setting, and restart it.

The purpose of setting the baud rate as 115200bps is only to improve the transmission speed and reduce the time of upgrading the application.

Upgrade Hex File of Application via Console Interface

Step 1: Set the Hyper Terminal.

Start the Hyper Terminal program and select related serial (such as COM 1) and set its attributes: 9600 baud rate, the soft flow control, eight data bits, no parity and one stop bit.

Step 2: Enter the Monitor mode.

If some information similar to "Monitor version 2.02 is Booting (^c enter monitor mode) ..." is displayed on the screen when the router starts up, you can press "CTRL+C" to enter the Monitor mode immediately. The prompt character of the mode is "mpMonitor:>" or "Monitor:>".

If no foregoing information is displayed on the screen when the router starts up, you need set the baud rate of the Hyper Terminal as 115200, restart the router, and then press the key ENTER to enter the Monitor mode.

Step 3: Erase the previous IOS.

Under the system prompt, use the commands "mpMonitor:>e p" or "mpMonitor:>e a" to erase the existing the IOS in the flash. The difference of the foregoing two commands is that the former only erases IOS while the latter erases both the IOS and the configuration file. But, both don't erase the ROOT program, which can only be upgraded and can't be erased.

Step 4: Reconfigure the speed of the Console interface and the Hyper

Terminal to upgrade the hex file of the application.

Use the command "mpMonitor:>s 115200" to set the speed of the Console interface of the router as 115200bps. At the same time, the speed of the Hyper Terminal is set as 115200bps (attribute-configuration-baud rate). Stop the connection in the Hyper Terminal and start the connection again. Press "l <CR>" behind "mpMonitor:>" and select the option 'Send text file' in the menu 'Transmit'. After the IOS program (hex file) that will be upgraded is selected, its transmission starts. After the upgrade ends, set the attributes of the Hyper Terminal back to the initial setting, and restart it.

We can, from the aspect of the speed, compare the foregoing three methods of upgrading the ISO program: the first method (upgrading the bin file of an application via TFTP/FTP) is of the fastest speed, while the third method is of the lowest speed. And the speed of the second method (Upgrading bin file of an application via the xModem protocol under the Monitor mode) is between that of the first method and third method. In the factual environment, the selection of the upgrade method should depend on the factual situation.

The first method can also upgrade the mixed program (ROOT+IOS). So, this method can remotely control the upgrade of the router whose ROOT program need be upgraded instead of on-the-spot upgrading it via the console interface, saving upgrade time. But the method has fatalness and its misoperation can result in router being unusable. If you want to

use the method, please request technology service center to provide the special upgrade program and related documents of operation description.

Network Test & Troubleshooting

This chapter explains how to use Signamax router network testing tool, and how to diagnose it when there is malfunction.

Network Test Tools

These four test tools are provided on the router:

Ping: Tests network connectivity

Traceroute: Tests the data packet's route information

Netstat: Examines network interface status and offers detailed statistical data

Show: Examines the system's statistical information

Ping & Groupping

Ping and groupping are used to test network connectivity and test whether the router can access the host address. This tool only supports IP protocol.

Ping and groupping run in common user mode or privileged user mode:

Common User Mode:

Router >ping ?

Option	Task
<hostname ipAddress >	Pings the host name or destination address.

Privileged user mode:

Router #ping ?

Command	Description
<hostname ipAddress <CR>>	Pings the host name or destination address.

You can stop the ping procedure by pressing Ctrl+Shift+6 on the keyboard at the same time. After the ping command has been executed, you will see the following onscreen output:

! shows a successful action, while . shows a failed action.

If ping worked, you will statistical information about the number of sent/received data packets, the percentage of data packets that responded and the minimum, average or maximum response time values.

After you execute the ping <CR> command in privileged user mode, you can input optional parameters. The following two examples explain these parameters and their meanings.

Example 1: Here, the command ping doesn't have any extended options:

router#ping

Option	Task
Target IP address: 192.168.8.1	The destination address.
Repeat count [5]: 20	The ICMP number repeatedly requesting the data packet.
Data packet size [76]: 1000	Appoints the ICMP packet size (1,000 byte).
Timeout in seconds [2]: 1	Permits delay. (The delay is regarded as a lost packet when it receives no acknowledgment of the packet's location.)
Extended commands [no]: n	The extended command.
Sweep range of sizes [no]: n	Whether the ICMP data packet is appointed or not.

Output:

Press key (ctrl + shift + 6) interrupt it.

Sending 20, 1000-byte ICMP Echos to 192.168.8.1 timeout is 1 seconds:

!!!!!!!!!!!!!!!!!!!

Success rate is 100% (20/20). Round-trip min/avg/max = 0/12/16 ms.

Example 2: After you choose the extended command options, you can set such options as source route, record timestamp and display detailed information, etc.:

router#ping

Option	*Task*
Target IP address: 128.255.255.1	
Repeat count [5]: 1930	
Data packet size [76]: 1000	
Timeout in seconds [2]: 1	
Extended commands [no]: **y**	
Source address or interface: 128.255.255.223	
Type of service [0]: 1	
Set DF bit in IP header? [no]: y	Decides whether or not the IP layer will permit an ICMP packet to be segmented.
Validate reply data? [no]: y	Decides whether or not the received ICMP data packet should be examined.
Data pattern [abcd]: asdf	Appoints ICMP data regarding requested data packets.
Loose, Strict, Record, Timestamp, Verbose[none]: L	Appoints loose/strict source route, record route and timestamp.
Source route: 128.255.255.223 128.255.255.1	
Loose, Strict, Record, Timestamp, Verbose[LV]: r	
Number of hops [6]: 3	Appoints the hops number.
Loose, Strict, Record, Timestamp, Verbose[LVR]: t	
Loose, Strict, Record, Timestamp, Verbose[LVRT]:v	
Loose, Strict, Record, Timestamp, Verbose[LRT]:	
Sweep range of sizes [no]: y	Decides whether or not the ICMP size scope requesting the data packet should be appointed.
Sweep min size [74]:	Minimum
Sweep max size [65530]: 2000	Maximum
Sweep interval [1]: 10	Shows the increasing interval between two adjacent ICMP packets

Output:

Press key (ctrl + shift + 6) interrupt it.

Sending 1930, [74..2000]-byte ICMP Echos to 128.255.255.1 timeout is 1 seconds:
Packet has IP options: Total option bytes = 40 .
Loose source route: 128.255.255.223 128.255.255.1
Record route number : 3
Record timestamp number : 2
!!
!!.....

Success rate is 64% (1235/1930). Round-trip min/avg/max = 0/12/1000 ms.

Command	Description	Configuration mode
groupping	*send ICMP request packet testing	"router>" or "router#"

groupping xxxx [-l/-n/-t/-w/-g]

Syntax	Description
xxxx	Groupping peer IP address or host name
—l	Configure sending ICMP request packet length
—n	Configure sending ICMP request packet number
—t	Sending ICMP request packet all the time until press ctrl+shift+6
—w	Configure waiting ICMP packet maximum length time, and the unit is ms
—g	Configure sending groupping number

(Default status)packet length is 76 bytes; 10 group, each group 5 packets; waiting time is 2s
(Example)router#groupping 1.1.1.1 –n 6 –g 8

traceroute

Traceroute: testing the gateway data packet used from source site to destination site, it uses for testing network connectivity and analyzing the malfunction.

Command	Description	Configuration mode
raceroute -----traceroute vrf	Discover gateways from source to destination. Discover gateways from source to destination.	Normal user mode "router>" or privileged user mode "router#" Normal user mode "router>" or privileged user mode "router#"

traceroute xxxx
traceroute vrf vrf-name xxxx

Syntax	Description
xxxx	Destination IP or host name

vrf-name	Destination address vrf name(VPN routing list item)

(Default status)no

1. In the process of traceroute, use Ctrl+Shift+6 to stop.
2. Output including:

Sending out ICMP packet information(TTL value, IP head option etc.)
List the routing information ICMP packet from source to destination
After executing traceroute <CR> or traceroute vrf vrf-name <CR>, the parameter can be input.

(Example)
Don't choose extended command option, only provide basic option parameter.

router#traceroute

Option	Description
Target IP address or hostname: 192.168.8.254	Destination address
Source address or interface: 128.255.255.223	Designate source address/ interface
Timeout in seconds [3]:	Permitted maximum time delay, and the default is 3 seconds.
Probe count [3]:	Send packet number, and the default value is 3
Minimum Time to Live [1]:	Send detecting packet default minimum TTL value, and the default value is 1
Maximum Time to Live [30]:	Send detection packet default maximum TTL value, 30
Port Number [33434]:	Receive detecting packet destination site default UDP port number, and the default is 33434
Loose, Strict, Record, Timestamp, Verbose[none]:	Source routing option

(output)
Type escape sequence to abort.
Tracing the route to 192.168.8.254 min ttl = 1, max ttl = 30 .

1 2.1.1.1 16 ms 33 ms 16 ms
2 192.168.8.254 16 ms 33 ms 16 ms

(Example)

When user chooses extending command, configure source routing, recording time, displaying information. And the format is as following:

router#traceroute

Option	Description
Target IP address or hostname: 192.168.8.254	
Source address or interface: 128.255.255.223	
Timeout in seconds [3]: 1	Configure maximum time delay 1 second, default value is 3
Probe count [3]:	Send the same TTL valued detection packet number, and the default value is 3.
Minimum Time to Live [1]:	Send detection packet default minimum TTL value, and the default value is 1
Maximum Time to Live [30]:	Send detection packet default maximum TTL value, and the default value is 30.
Port Number [33434]:	Receive detection packet destination site default UDP port number, and the default value is 33434
Loose, Strict, Record, Timestamp, Verbose[none]:L	Source routing item.
Source route: 128.255.255.1	Source address
Loose, Strict, Record, Timestamp, Verbose[LV]: v	Don't print detailed information.
Loose, Strict, Record, Timestamp, Verbose[L]: t	
Number of hops [7]: 7	Designate hops of time record.
Loose, Strict, Record, Timestamp, Verbose[LTV]: v	Don't print detailed information
Loose, Strict, Record, Timestamp, Verbose[LT]:	

(output)
Type escape sequence to abort.

Tracing the route to 192.168.8.254 min ttl = 1, max ttl = 30 .
Packet has IP options: Total option bytes = 40.
Loose source route: 128.255.255.1

```
Record timestamp number : 7
1         16 ms    0 ms     16 ms
2         0 ms     0 ms     16 ms
3         !S       !S       !S
```

Note:

·!N——network not reachable

·!H——host not reachable

·!S——source routing failure not reachable

·!A——forbidden access not reachable

·!F——packet fragment not reachable

·?——unknown type packet

netstat

Netstat only runs privileged user mode, for displaying system list, interface status /configuration, protocol statistics and buffer information. And the command parameter is as following:

Netstat parameter

router#netstat ?

Command	Description	Mark
-a	Display system internal ARP list	
-e	Examine status information	
-h	Display system host list	
-i	Display router interface status and configuration information	
-m	Display network stack data buffer info	
-n	Display network stack system buffer area information	
-p	Display special protocol statistics information	Support igmp,icmp,ip,tcp,udp protocols
-r	Display routing list information	
-s	Display all IP protocol statistics information	
<CR>	Display TCP, UDP protocol connection and port information	

show

Show has following types:

- Display system clock command
- Display system equipment and interface command
- Display system statistics information command
- Display system startup parameter command
- Display system task command
- Display system stack command

The protocol and kinds of interface show command refer to chapter. The following is some part of command show:

system show subnet command

router#show ?

Command	Description	Mark
clock	Display system clock	In normal user mode
device	Print system equipment information	
interface	Print system interface information	In normal user mode
version	Print system software and hardware version information	In normal user mode
ip	Examine TCP/IP protocol statistics information	In normal user mode
process	Display system task/ process information	
stack	Display system stack information	

Troubleshooting

Because of many kinds of router interfaces and protocols, there may have some fault.

Troubleshooting of LAN Interface

Signamax router at least provides a LAN interface for connecting LAN, and connects LAN via serial or other interfaces.

Ping from PC to Ethernet interface, if there is no response or the data flow drops, it means the fault is on Ethernet interface. Check the fault on Ethernet interface according to the following steps:

Check whether the connection between PC and router is right.

If using Hub or LAN Switch to connect Ethernet, confirm the light is normal. Usually check

link(some
are 10M/100M/1000M lights) active light(some are rx/tx light) .
When hardware is not correct, it appears: ping router no response.
The process is as following:
(under DOS shell)
c:>**ping** 128.255.255.1

- Pinging 128.255.255.1 with 32 bytes of data
- Request timed out.
- Request timed out.
- Request timed out.

128.255.255.1 is Ethernet interface IP address.
(in normal user mode)

- router>**ping** 128.255.255.2
- Press key (ctrl + shift + 6) interrupt it.
- Sending 5, 76-byte ICMP Echos to 128.255.255.2 timeout is 2 seconds:
- .....
- Success rate is 0% (0/5).

128.255.255.2 is PC Ethernet card IP address.

2. If hardware connection is normal, test software

Check IP address of PC and router Ethernet interface. These two IP addresses should be the same, only the host address is different.

3. According to the following to define the fault

Whether protocol is matching, Ethernet supports IP frame type: Ethernet_II and Ethernet_SNAP. Signamax router can accept these two IP packets at the same time, but only send one type.

Whether Ethernet works normal Signamax router Ethernet interface supports kinds of rate, full-duplex/half-duplex working mode.

Troubleshooting of WAN Interface

Check the fault according to the following steps:

Check whether physical interface is normal connected
Signamax router provides V24, V35 etc. kinds of WAN interface cables, and meanwhile has DTE/DCE working modes.

(1) first, confirm WAN interface type(V24/V35) .

(2) confirm WAN interface working mode.
If interface works in asynchronous mode, check baud rate, the lowest is 1200bps,and highest is 115200bps；

If interface works in synchronous mode, the clock is provided by router. Check whether the clock rate and clock mode are correct; if interface works in DTE mode, the clock is provided by DSU/CSU, referring to DSU/CSU description, to set clock mode.

If the hardware parameter or connection is not correct, the fault is: ping peer router no response, no change of WAN input and output packet number.

If hardware parameter and connection are correct, check whether link layer protocol is normally configured.

Signamax router WAN interface ly supports SLIP, PPP, CSLIP etc kinds of

protocols. They only communicate if both sides configure the same protocols.
If using PPP(Point to Point Protocol), and adopting PAP or CHAP as authentication protocol, please guarantee the password;

If using Modem by asynchronous mode, make sure whether use Modem command on routers;

If link layer configures correctly, but IP layer is not normal, check it according to the following:

If link layer protocol is PPP,and asynchronous dialup mode, make sure the configuration of dialer map is correct: dialer map ip ipAddress telephoneNumber, ipAddress is peer serial IP address, and telephoneNumber is peer serial telephone number.

The WAN IP address should be the same with network address. If not, there will be malfunction of IP packet.

Check routing malfunction. Signamax router ly supports static routing, RIP v1/v2, OSPF, IRMP dynamic routing and dialup on demand. Router forwards packet according to routing information. Router malfunction means the failure of packet forwarding. The solution is:

If adopting statistic routing, no need to add manual routing.

For RIP, OSPF, IRMP dynamic routing, configure RIP, OSPF routing protocol.

Card Hot-swappable

This chapter explains router hot-swappable function and how to do it.

Overview

Hot-swappable function is to inset card to the system without stopping the work. The card can be changed, added or removed but not affect other service.

Hot-swappable Commands

Command	Description	Config. mode
hotswap online *slot*	Hot-swappable online slot	Privileged user mode
hotswap offline *slot*	Hot-swappable offline slot	Privileged user mode
hotswap reset *slot*	Hot-swappable reset slot	Privileged user mode
debug hotswap	Enable hot-swappable debugging	Privileged user mode
no debug hotswap	Disable hot-swappable debugging	Privileged user mode
debug hot-swap-config	Enable hot-swappable configuration debugging	Privileged user mode
no debug hot-swap-config	Enable hot-swappable configuration debugging	Privileged user mode

Manual Hot-swappable

Manual hot-swappable is to manual switch card online or offline.

Manual Hot Inset

The operation is to inset card to system with hot-swappable function, or press the hot-swappable button, and at this time the status light is shinning, which means the system is loading the card till the light is in lighten status.

For manual inset, the following information will be printed on shell, and these information will be written into log file:

Load successful:
00:02:34: %HOTSWAP: Manual hotswap online, slot = 6
00:02:36: %HOTSWAP: Hotswap process success!

Load failed:
00:02:34: %HOTSWAP: Manual hotswap online, slot = 6
00:02:36: %HOTSWAP: Hotswap process fail!

When card loading is failed, inset it into a new system for reloading.
🕮 Note:
According to different types of card, and time is 3-10 seconds.

Manual Hot Pull Out

Operation:

Press hot-swappable button, and at this time, the status light is shining, which means the system is uninstalling the card.

After the uninstall, the status light is off, and then the card can be pull out from the system.

For manual pull out, the following information will be printed out on shell, and these information will be written into the log:

uninstall successful:

```
00:02:59: %HOTSWAP: Manual hotswap offline, slot = 6
00:03:00: %HOTSWAP: Hotswap process success!
```

Uninstall failed:

```
00:02:59: %HOTSWAP: Manual hotswap offline, slot = 6
00:03:00: %HOTSWAP: Hotswap process fail!
```

- When status light is shining, don't pull card out of the system.
- Hot-swappable button is installed inside the panel.
- When card is online, press the button to uninstall the card; when the card is offline, press the button to load card.

Card Command Hot-swappable

Card command hot-swappable is to send hot-swappable command via shell or network interface, to complete card load, uninstall and reset.

Card Command Hot Inset

Upload card to online status.

```
hotswap online slot
```

This command is used in privileged user mode. The status light is shining, and after the load, the light turns lighten.

Application example:

```
router#hotswap online 6
shell has following prompt:
success:
00:04:05: %HOTSWAP: Command hotswap online, slot = 6
00:04:08: %HOTSWAP: Hotswap process success!

    failed:
00:04:05: %HOTSWAP: Command hotswap online, slot = 6
00:04:08: %HOTSWAP: Hotswap process fail!
```

When status light is shining, don't pull card out of the system.

Card Command Hot-swappable

Uninstall to offline status.

```
hotswap offline slot
```

This command is used in privileged user mode, The status light is shining, and after the uninstall, the
light is off.

Application example:

```
router#hotswap offline 6
shell has following prompt:
success:
00:04:58: %HOTSWAP: Command hotswap offline, slot = 6
00:04:59: %HOTSWAP: Hotswap process success!

Failed:
00:04:58: %HOTSWAP: Command hotswap offline, slot = 6
00:04:59: %HOTSWAP: Hotswap process fail!
```

When status light is shining, don't pull card out of the system.

Card Command Reset

Reset the card.

```
hotswap reset slot
```

This command is used in privileged user mode, The status light is shining, and after the reset, the light is on.

Application example:

```
router#hotswap reset 6
shell has following prompt:
Successful:
00:05:49: %HOTSWAP: Command linecard reset, slot = 6
00:05:51: %HOTSWAP: Hotswap process success!

Failed:
00:05:49: %HOTSWAP: Command linecard reset, slot = 6
00:05:51: %HOTSWAP: Hotswap process fail!
```

When status light is shining, don't pull card out of the system.

Hot-swappable Debugging

Enable hot-swappable debugging.

```
debug hotswap
```

Application example:

```
router# debug hotswap
```

The following is information of slot6 insetting and pulling out of 8CE1 card:

```
/* inset debugging information */
router#
00:09:41: %HOTSWAP(sysHotSwapInt): Start
00:09:41: %HOTSWAP(sysHotSwapInt): hsStatOld = 0xff, hsStatNew =
 0xbf
00:09:41: %HOTSWAP(sysHotSwapInt): Hotswap happend, slot = 6
00:09:41: %HOTSWAP(sysHotSwapInt): Hotswap happend, slot = 6, busNo
 = 21, devNo = 3
00:09:41: %HOTSWAP(sysHotSwapInt): VendorId = 0x1172, DeviceId = 0x9,
 Operation = 0x1
00:09:41: %HOTSWAP(sysHotSwapTask): Received a message, slotNo = 6,
 operation = 0x1, vendorId = 0x1172, deviceId = 0x9
00:09:41: %HOTSWAP: Manual hotswap online, slot = 6
00:09:41: %HOTSWAP(sysHotSwapTask): Manual hotswap online
00:09:42: %HOTSWAP(sysHotSwapTask): Hotswap online
00:09:43: %HOTSWAP(sysHotSwapTask): Notify the shell to restore
 configration, slot = 6, cardType = 0x8
00:09:43: %HOTSWAP: Hotswap process success!
router#

/* pull out debugging information */
router#
00:10:10: %HOTSWAP(sysHotSwapInt): Start
00:10:10: %HOTSWAP(sysHotSwapInt): hsStatOld = 0xbf, hsStatNew =
 0xff
00:10:10: %HOTSWAP(sysHotSwapInt): Hotswap happend, slot = 6
00:10:10: %HOTSWAP(sysHotSwapInt): Hotswap happend, slot = 6, busNo
 = 21, devNo = 3
00:10:10: %HOTSWAP(sysHotSwapInt): VendorId = 0x1172, DeviceId = 0x9,
 Operation = 0x2
```

```
00:10:10: %HOTSWAP(sysHotSwapTask): Received a message, slotNo = 6,
 operation = 0x2, vendorId = 0x1172, deviceId = 0x9
00:10:10: %HOTSWAP: Manual hotswap offline, slot = 6
00:10:10: %HOTSWAP(sysHotSwapTask): Manual hotswap offline
00:10:10: %HOTSWAP(sysHotSwapTask): Notify the shell to save
 configration, slot = 6, cardType = 0x8
00:10:11: %HOTSWAP(sysHotSwapTask): Hotswap offline
00:10:11: %HOTSWAP: Hotswap process success!
router#
```

```
disable hot-swappable debugging.
```

Command:

```
router#no debug hotswap
```

Hot-swappable Configuration Debugging

Enable hot-swappable configuration debugging.

```
debug hot-swap-config
```

Application example:

```
router#debug hot-swap-config
```

The following is the configuration debugging information of slot6 insetting and pulling out of 8CE1 card.

```
/* inset debugging information */
router#
00:19:24: %HOTSWAP: Manual hotswap online, slot = 6
00:19:27: %HSC(plugin): start plugin ..........
00:19:27: %HSC: find existed interface script file
 /hsconfig/intf_6_8
00:19:27: %HSC(plugin): Find interface script /hsconfig/intf_6_8
00:19:27: %HSC(plugin): Ready to configure these script
00:19:27: cmd : interface serial6/0
00:19:27: cmd :  encapsulation hdlc
00:19:27: cmd :  bandwidth 2048
00:19:27: cmd :  exit
00:19:27: cmd : interface serial6/1
00:19:27: cmd :  encapsulation hdlc
00:19:27: cmd :  bandwidth 2048
```

```
00:19:27: cmd :  exit
00:19:27: cmd : interface serial6/2
00:19:27: cmd :  encapsulation hdlc
00:19:27: cmd :  bandwidth 2048
00:19:27: cmd :  exit
00:19:27: cmd : interface serial6/3
00:19:27: cmd :  encapsulation hdlc
00:19:27: cmd :  bandwidth 2048
00:19:27: cmd :  exit
00:19:27: cmd : interface serial6/4
00:19:27: cmd :  encapsulation hdlc
00:19:27: cmd :  bandwidth 2048
00:19:27: cmd :  exit
00:19:27: cmd : interface serial6/5
00:19:27: cmd :  encapsulation hdlc
00:19:27: cmd :  bandwidth 2048
00:19:27: cmd :  exit
00:19:27: cmd : interface serial6/6
00:19:27: cmd :  encapsulation hdlc
00:19:27: cmd :  bandwidth 2048
00:19:27: cmd :  exit
00:19:27: cmd : interface serial6/7
00:19:27: cmd :  encapsulation hdlc
00:19:27: cmd :  bandwidth 2048
00:19:27: cmd :  exit
00:19:27: %HSC(plugin): configue ok,remove script file
 /hsconfig/intf_6_8
00:19:27: %HSC(plugin): notify some module after plugining and
 configuring
00:19:27: %HSC: notify other module relation with interface
 serial6/0
00:19:27: %HSC: notify other module relation with interface
 serial6/1
00:19:27: %HSC: notify other module relation with interface
 serial6/2
00:19:27: %HSC: notify other module relation with interface
 serial6/3
00:19:27: %HSC: notify other module relation with interface
 serial6/4
00:19:27: %HSC: notify other module relation with interface
 serial6/5
00:19:27: %HSC: notify other module relation with interface
```

```
 serial6/6
00:19:27: %HSC: notify other module relation with interface
 serial6/7
00:19:27: %HSC(plugin): end plugin ===========
00:19:27: %HOTSWAP: Hotswap process success!
router#

/* pull out debugging information */
router#
00:20:33: %HOTSWAP: Manual hotswap offline, slot = 6
00:20:33: %HSC(unplug): start unplug ..........
00:20:33: %HSC(unplug): find free interface script file location in
 slot 6
00:20:33: %HSC(unplug): create file /hsconfig/intf_6_8 success
00:20:33: %HSC(unplug): the last interface script file
 /hsconfig/intf_6_8 loc = 0
00:20:33: %HSC(unplug): get interface-self script
00:20:33: %HSC(unplug): no interface-self config
00:20:33: %HSC: notify other module relation with interface
 serial6/0 before no interface config
00:20:33: %HSC: notify other module relation with interface
 serial6/1 before no interface config
00:20:33: %HSC: notify other module relation with interface
 serial6/2 before no interface config
00:20:33: %HSC: notify other module relation with interface
 serial6/3 before no interface config
00:20:33: %HSC: notify other module relation with interface
 serial6/4 before no interface config
00:20:33: %HSC: notify other module relation with interface
 serial6/5 before no interface config
00:20:33: %HSC: notify other module relation with interface
 serial6/6 before no interface config
00:20:33: %HSC: notify other module relation with interface
 serial6/7 before no interface config
00:20:33: %HSC: shutdown interface serial6/0
00:20:33: delete dst-if serial6/0 config by src-if serial6/0
00:20:33: <src>serial6/0 :  interface serial6/0
00:20:33: <dst>serial6/0 :  interface serial6/0
00:20:33: <src>serial6/0 :  encapsulation hdlc
00:20:33: <src>serial6/0 :  bandwidth 2048
00:20:33: <src>serial6/0 :  shutdown
00:20:33: <src>serial6/0 :  exit
```

```
00:20:33: <dst>serial6/0 :  no bandwidth
00:20:33: <dst>serial6/0 :  exit
00:20:33: %HSC: shutdown interface serial6/1
00:20:33: delete dst-if serial6/1 config by src-if serial6/1
00:20:33: <src>serial6/1 :  interface serial6/1
00:20:33: <dst>serial6/1 :  interface serial6/1
00:20:33: <src>serial6/1 :  encapsulation hdlc
00:20:33: <src>serial6/1 :  bandwidth 2048
00:20:33: <src>serial6/1 :  shutdown
00:20:33: <src>serial6/1 :  exit
00:20:33: <dst>serial6/1 :  no bandwidth
00:20:33: <dst>serial6/1 :  exit
00:20:33: %HSC: shutdown interface serial6/2
00:20:33: delete dst-if serial6/2 config by src-if serial6/2
00:20:33: <src>serial6/2 :  interface serial6/2
00:20:33: <dst>serial6/2 :  interface serial6/2
00:20:33: <src>serial6/2 :  encapsulation hdlc
00:20:33: <src>serial6/2 :  bandwidth 2048
00:20:33: <src>serial6/2 :  shutdown
00:20:33: <src>serial6/2 :  exit
00:20:33: <dst>serial6/2 :  no bandwidth
00:20:33: <dst>serial6/2 :  exit
00:20:33: %HSC: shutdown interface serial6/3
00:20:33: delete dst-if serial6/3 config by src-if serial6/3
00:20:33: <src>serial6/3 :  interface serial6/3
00:20:33: <dst>serial6/3 :  interface serial6/3
00:20:33: <src>serial6/3 :  encapsulation hdlc
00:20:33: <src>serial6/3 :  bandwidth 2048
00:20:33: <src>serial6/3 :  shutdown
00:20:33: <src>serial6/3 :  exit
00:20:33: <dst>serial6/3 :  no bandwidth
00:20:33: <dst>serial6/3 :  exit
00:20:33: %HSC: shutdown interface serial6/4
00:20:33: delete dst-if serial6/4 config by src-if serial6/4
00:20:33: <src>serial6/4 :  interface serial6/4
00:20:33: <dst>serial6/4 :  interface serial6/4
00:20:33: <src>serial6/4 :  encapsulation hdlc
00:20:33: <src>serial6/4 :  bandwidth 2048
00:20:33: <src>serial6/4 :  shutdown
00:20:33: <src>serial6/4 :  exit
00:20:33: <dst>serial6/4 :  no bandwidth
```

```
00:20:33: <dst>serial6/4 :  exit
00:20:33: %HSC: shutdown interface serial6/5
00:20:33: delete dst-if serial6/5 config by src-if serial6/5
00:20:33: <src>serial6/5 :  interface serial6/5
00:20:33: <dst>serial6/5 :  interface serial6/5
00:20:33: <src>serial6/5 :  encapsulation hdlc
00:20:33: <src>serial6/5 :  bandwidth 2048
00:20:33: <src>serial6/5 :  shutdown
00:20:33: <src>serial6/5 :  exit
00:20:33: <dst>serial6/5 :  no bandwidth
00:20:33: <dst>serial6/5 :  exit
00:20:33: %HSC: shutdown interface serial6/6
00:20:33: delete dst-if serial6/6 config by src-if serial6/6
00:20:33: <src>serial6/6 :  interface serial6/6
00:20:33: <dst>serial6/6 :  interface serial6/6
00:20:33: <src>serial6/6 :  encapsulation hdlc
00:20:33: <src>serial6/6 :  bandwidth 2048
00:20:33: <src>serial6/6 :  shutdown
00:20:33: <src>serial6/6 :  exit
00:20:33: <dst>serial6/6 :  no bandwidth
00:20:33: <dst>serial6/6 :  exit
00:20:33: %HSC: shutdown interface serial6/7
00:20:33: delete dst-if serial6/7 config by src-if serial6/7
00:20:33: <src>serial6/7 :  interface serial6/7
00:20:33: <dst>serial6/7 :  interface serial6/7
00:20:33: <src>serial6/7 :  encapsulation hdlc
00:20:33: <src>serial6/7 :  bandwidth 2048
00:20:33: <src>serial6/7 :  shutdown
00:20:33: <src>serial6/7 :  exit
00:20:33: <dst>serial6/7 :  no bandwidth
00:20:33: <dst>serial6/7 :  exit
00:20:33: %HSC: delete netDevice by interface serial6/0
00:20:33: %HSC(unplug): end unplug ===========
00:20:34: %HOTSWAP: Hotswap process success!
router#
```

Disable hot-swappable configuration debugging.

```
router#no debug hot-swap-config
```

DHRP Configuration

DHRP realizes dynamic domain registering and updating function.

Main contents of this chapter are:

Configuring DHRP commands

Configuring DHRP example

DHRP check and debugging

Overview

DHRP provides binding domain name and dynamic IP address, permitting PC gives its IP address to server, and chooses registered domain record. The server modifies DNS record.

In order to complete dynamic domain register on router, there are two steps:

log in (www.oray.net) ,to register user name and free domain name

According to user name and domain name, configure parameter.

Commands

Command	Description	Config. mode
oray-ddns register user *name_string*	*configure host registering user name	config
server {address *ip_address* / domain-name *name*}	*configure Oray DDNS server address	config-oray-ddns
password *key_string*	*configure password	config-oray-ddns
domain-name *name_string*	*designate registering domain name	config-oray-ddns
show oray-ddns user *[name_str]*	*display Oray-DDNS information	Privileged configuration mode
debug oray-ddns	*display Oray-DDNS debugging information	Privileged configuration mode
clear oray-ddns register	*clear Oray-DDNS registering internal status and re-register.	Privileged configuration mode

DHRP Basic Configuration

oray-ddns …

Configure host registering user name

```
oray-ddns register user name_string
```

Parameter	Description
name_str	Designate the registering usre name in Oray

(Configuration mode) global configuration mode
(default configuration)no

server address …

Configure Oray DDNS server address or domain name

```
server {address ip_address | domain-name name}
```

Parameter	Description
name	Designate Oray DDNS server domain name
ip_address	Designate Oray DDNS server address

(Configuration mode) oray-ddns configuration sub-mode
(default configuration)no

password …

Configure password

```
password key_string
```

Parameter	Description
key_string	Designate password

(Configuration mode) oray-ddns configuration sub-mode.
(default configuration)no

domain-name …

Designate registering domain name: vicp.net, oicp.net, xicp.net and eicp.net. This command supports repeated configuration. Registering domain name number is 6.

```
domain-name name_string
```

Parameter	Description
name_string	Designate registering domain name

(Configuration mode) oray-ddns configuration sub-mode.
(default configuration)no

DHRP Check & Debugging

show oray-ddns user …

Display Oray-DDNS information.

```
show oray-ddns user [name_str]
```

Parameter	Description
name_string	Designate user name

```
(Configuration mode) privileged user mode
```

debug oray-ddns

Display Oray-DDNS debugging information. Command no is used to disable information.

```
debug oray-ddns
no debug oray-ddns
```

(Configuration mode) privileged user mode

clear oray-ddns register

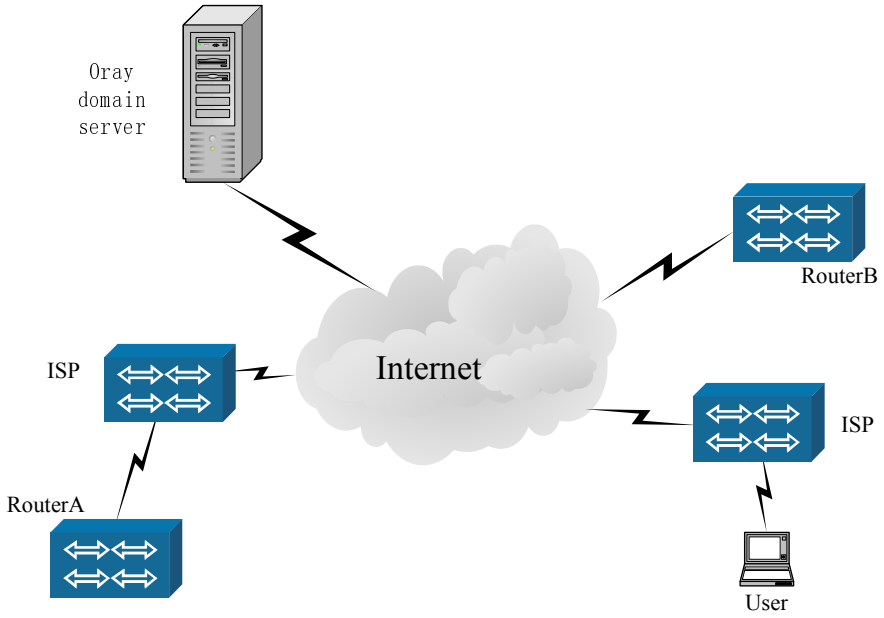
Clear Oray-DDNS registering internal status, and re-registering.

```
clear oray-ddns register
```

(Configuration mode) privileged user mode

DHRP Configuration Example

DHRP application:



The figure displays actual application of DHRP. Router A accesses Internet via ISP, and its address is dynamic distributed by ISP, and so its address is changeable. So we use DHRP. Register an Oray domain name on Router A, and other nodes only use this domain name to access other Router A.

Router A configuration:

Command	Description
RouterA#configure terminal	Enter global configuration mode
RouterA(config)#ip name-server 61.139.2.69	Designate normal DNS server address
RouterA(config)#oray-ddns register user signamax	Use registering user name to enter Oray-DDNS configuration sub-configuration mode.
RouterA(config-oray-ddns)#password signamax123	Input password
RouterA(config-oray-ddns)# server domain-name ph002.oray.net	Designate Oray DDNS server domain name
RouterA(config-oray-ddns)#domain-name signamax-sail.vicp.net	Designate the first domain name
RouterA(config-oray-ddns)#domain-name signamax-research.vicp.net	Designate the following domain names.

Ethernet Switching Module Configuration

The function of Ethernet switching module is similar to normal L2 Ethernet switch. It realizes L2 Ethernet packet wire speed forwarding and supports the following function:

Support 802.1Q, configuring 4k vlan

Support port bandwidth limitation function

Support port broadcast storm restraining

Support port isolation function

Support 10BaseT/100BaseTX adaptive, 10/100Mbps, and full-duplex/half-duplex configuration

Support crossing and direct connecting wire adaptive function

Support port status displaying, data statistics

Support L3 simulating function, mapping from VLAN to IP, support L3 interface mac address changing

Ethernet Switching Module L2 Function Configuration

Main contents of this section: Ethernet switching module L2 function configuration command description.

L2 Commands

Command	Description	Config. mode
vlan [vlan-num]	Enter VLAN configuration mode	config config-vlan
description string	Configure VLAN name	config-vlan
port port-list ----tagged ----untagged	Configure VLAN port status Configure VLAN port list TAG status Configure VLAN port list UNTAG status	config-vlan
no port port-list	Delete VLAN member port	config-vlan
pvid pvid-num	Configure VLAN port default VLAN number	config-port
show vlan [vlan-num]	Display VLAN configuration condition	router config config-vlan
switch-mac aging-time [seconds]	Configure mac address aging time	config
dot1p-map ----[dot1pVal] [priority] ----default	Configure 802.1p value and priority queue mapping 802.1p → priority Default configuration	config
dot1p-scheduler ----sp_wrr ----wrr	Configure priority queue arithmetic Q0 is the highest, other is 3 wrr Q4 are wrr	config
default-dot1p [dot1pVal]	Configure port default dot1p value	config-port
show dot1p-map	Display 802.1p value and priority queue mapping	router config
port port-list	Enter port configuration mode	config config-port
shutdown/no shutdown	Enable/ disable Ethernet port	config-port
duplex ---auto ----full ----half	Configure port duplex status Auto negotiation Full duplex Half duplex	config-port
bandwidth-limit ----receive limit ----transmit limit	Configure port bandwidth limitation Entry bandwidth limitation Exit bandwidth limitation	config-port
speed ----10 ----100 ----auto	Configure port rate 10Mb/s 100Mb/s Auto negotiation	config-port
storm-control disable lowest low high	Configure port storm control Not control Permit 3.3% storm Permit 5% storm Permit 10% storm	config-port

highest	Permit 20% storm	
mdix ----enable ----disable	Manual configure wire transferring function Enable Disable	config-port
isolated-port ---enable ----disable	Configure port isolation Isolation port Not isolating port	config-port
clear port portlist statistics	Clear port statistics value	router
show port port-list ----configuration ----statistics	Display port information *display port configuration information *display port packet statistics information	router config

VLAN Configuration Commands

Enter VLAN configuration mode

Enter VLAN configuration mode.
Configuration command
`vlan [vlan-num]`

Syntax	Description
vlan-num	Enable VLAN command, and enter VLAN configuration mode, and the range is 1~4094

(Configuration mode) global configuration mode, VLAN configuration mode
(Default status)not enable VLAN configuration

Configure VLAN name

Configuration command
`description string`

Syntax	Description
String	VLAN name

(Configuration mode) VLAN configuration mode
(Default status)VLAN+vlan id.

Configure VLAN port status

Configuration command
`port port-list {tagged | untagged}`

Syntax	Description
tagged	Configure VLAN port list TAG status
untagged	Configure VLAN port list UNTAG status

(Configuration mode) VLAN configuration mode

Delete VLAN member port
Configuration command
`no port port-list`

(Configuration mode) VLAN configuration mode

Configure VLAN port default VLAN number
Configuration command

```
pvid pvid-num
```

Syntax	Description
pvid-num	Default VLAN number, and the range is 1～4094.

(Configuration mode) port configuration mode.
(Default status)PVID number is 1.

Display VLAN configuration status
Configuration command

```
show vlan [vlan-num]
```

Syntax	Description
vlan-num	Display designated VLAN,and the range is 1~4094,or directly press enter key.

(Configuration mode) ENABLE mode, global configuration mode and VLAN configuration mode.

Configure mac address aging time
Configuration command

```
switch-mac aging-time [seconds]
```

Syntax	Description
seconds	Configure mac address aging time

(Configuration mode) global configuration mode
(Default status)aging time is 30 seconds.

802.1p Commands

Configure 802.1p value and priority queue mapping
Configuration command

```
dot1p-map {[dot1pVal] [priority]  |  default}
```

Syntax	Description
dot1pVal	802.1p value, and the range is 0-7
priority	Priority queue, and the range is 0-3,highest is 0.
default	Default mapping relation is: 802.1p priority 0-1 0 2-3 1 4-5 2 6-7 3

(Configuration mode) global configuration mode
(Default status)default mapping

Configure priority queue scheduler
Configuration command

```
dot1p-scheduler { sp_wrr  |  wrr}
```

Syntax	Description
sp_wrr	The scheduler is: 0 is the highest
wrr	The scheduler is: 0-3 is wrr sending.

(Configuration mode) global configuration mode
(Default status)wrr scheduler

Configure port default dot1p value
Configuration command

```
default-dot1p [dot1pVal]
```

Syntax	Description
dot1pVal	802.1p value, and the range is 0-7

(Configuration mode) global configuration mode
(Default status)0

Display 802.1p value and priority queue mapping
Configuration command

```
show dot1p-map
```

(Configuration mode) ENABLE mode, global configuration mode.

Port Configuration Commands

Enter port configuration mode
Configuration command

```
port port-list
```

Syntax	Description
port-list	Configured Ethernet port number, it can be different type ports, and the format refers to port-list configuration description.

(Configuration mode) global configuration mode, port configuration mode.

Enable/disable Ethernet port
Configuration command

```
shutdown/no shutdown
```

Syntax	Description
shutdown	Disable Ethernet port. Port is not in working mode.
no shutdown	Enable Ethernet port.

(Configuration mode) port configuration mode.
(Default status)enable Ethernet port

Configure port duplex status
Configuration command

```
duplex {auto|full|half}
```

Syntax	Description
Auto	Set port duplex status as auto negotiation.
Full	Set port full-duplex status
Half	Set port half-duplex status

(Configuration mode) port configuration mode.
(Default status)auto

Configure port bandwidth limitation
Configuration command

```
bandwidth-limit {receive|transmit} bandwidth-limit-index
```

Syntax	Description
Receive	The limitation of port receiving frame bandwidth.
Transmit	Limitation of port sending frame bandwidth
bandwidth-limit-index	Bandwidth limitation index, and the range is below 1792K, granularity is 64K, above 2M, granularity is 1M.

(Configuration mode) port configuration mode.
(Default status)no limitation.

Set port rate
10/100Base-T Ethernet port supports 10Mbit/s, 100Mbit/s.
Configuration command

```
speed {10|100|auto}
```

Syntax	Description
10	Set Ethernet port rate 10Mb/s.
100	Set Ethernet port rate 100Mb/s.
Auto	Set Ethernet port rate as auto negotiation.

(Configuration mode) port configuration mode.
(Default status)auto

Configure storm controlling function
Configuration command

```
storm-control {disable|lowest|low||high|highest}
```

Syntax	Description
Disable	Disable storm control function 100%
Lowest	Set storm control function as lowest level 3.3%
Low	Set storm control function as low level 5%
High	Set storm control function as high level 10%
Highest	Set storm control function as highest level 20%

(Configuration mode) port configuration mode.
(Default status)low

Configure manual wire transfer function

Configuration command

```
mdix {enable | disable}
```

Syntax	Description
enable	Enable manual wire transfer function
disable	Disable manual wire transfer function

(Configuration mode) port configuration mode.
(Default status)disable
This command only uses when port rate and duplex are fixed.

Port renew system default value
Configuration command

```
no { bandwidth-limit | duplex | pvid | shutdown | speed |mdix}
```

Syntax	Description
bandwidth-limit	Not use port bandwidth limitation
duplex	Renew to port default duplex status
Pvid	Renew to port default PVID
shutdown	Enable port
speed	Renew to port default rate
mdix	No crossing /direct connection transfer

(Configuration mode) port configuration mode.

Port isolation command

```
Configuration command
isolated-port {enable | disable}
```

Syntax	Description
enable	Isolate this port
disable	Don’t isolate this port

(Configuration mode) port configuration mode.
(Default status)disable.

Clear port statistics value command
Configuration command

```
clear port portlist  statistics
```

(Configuration mode) ENABLE mode

Examine port information
Configuration command

```
show port port-list [configuration|statistics]
```

Syntax	Description
Port-list	Port list
configuration	Display port configuration information
statistics	Display port statistics information

(Configuration mode) Enable mode, global configuration mode and port configuration mode. For port configuration information, and the segment is as following:

Syntax	Description
Status	Display enabling or disabling the port, referring to front introduction.
Link	Port working status, up or down.
Set Speed	Set port rate mode, referring to front introduction.
Acutal Speed	Port working rate mode, unknown, 10, 100, or illegal;
Set Duplex	Set port duplex mode, referring to front introduction.
Acutal Duplex	Port working duplex mode, unknown, half, full, illegal;
Storm Control	Storm control function configuration, referring to before introduction.
Bandwidth receive limit	Port receiving packet bandwidth limitation.
Bandwidth transmit limit	Port sending packet bandwidth limitation value.
Default Priority	Set port default priority level.
Pvid	Port default VLAN number.

Configuration example

```
Display port 5 configuration information:
Switch#show port 5
port 5 configuration information:
        Status          : Enabled
        Link            : Up
        Set Speed       : Auto
```

```
Act Speed          : 100
Set Duplex         : Auto
Act Duplex         : Full
Storm Control      : Low
Band-in-limit      : 0
Band-out-limit     : 0
Mdix Swap          : Disabled
Isolated Port      : Disabled
Default Dot1p      : 0
Pvid               : 1
```

For port statistics information, it displays:

Syntax	Description
DropEvents	Port dropped packet number.
Octets	Port receiving and sending byte total number.
Pkts	Port receiving and sending packet total number.
Broadcasts	Port receiving and sending broadcast packet total number.
Multicasts	Port receiving and sending multicast packet total number.
CRCAlignErrors	Port receiving CRC check error packet number.
UndersizePkts	Port received packet number less than 64 (if it is VLAN TAG frame, it should be less than 68 bytes).
OversizePkts	Port received and sending packet bigger than 1518 (if it is VLAN TAG frame, it should be bigger than 1522 bytes).
Fragments	Port received and sending error packet number smaller than 64 (if it is VLAN TAG frame, it should be smaller than 68 bytes).
Jabbers	Port received and sending error packet bigger than 1518 (if it is VLAN TAG frame, it should be bigger than 1522 bytes)
Collisions	Collision packet total number.
Pkts64Octets	Port received packet length smaller than 64 (if it is VLAN TAG frame, it should be 68 bytes)
Pkts65to127Octets	Port received packet length between 65 and 127 (if it is VLAN TAG frame, it should be between 69 and 131)
Pkts128to255Octets	Port received packet length between 128 and 255 (if it is VLAN TAG frame, it should be between 132 and 259)
Pkts256to511Octets	Port received packet length between 256 and 511 (if it is VLAN TAG frame, it should be between 260 and 515)
Pkts512to1023Octets	Port received packet length between 512 and 1023 (if it is VLAN TAG frame, it should be between 516 and 1027)
Pkts1024to1518Octets	Port received packet length between 1024 and 1518 (if it is VLAN

	TAG frame, it should be between 1028 and 1522)

Configuration example

Display port 5 statistics information

Switch#show port 5 statistics

port 5 statistics information:

```
    TxOctets              : 598
        TxUnicasts            : 5
        TxMulticasts          : 0
        TxBroadcasts          : 2
        RxDropEvents          : 0
        RxOctets              : 2459753
        RxPkts                : 3791
        RxBroadcasts          : 2427
        RxMulticasts          : 1074
        RxCRCAlignErrors      : 0
        RxUndersizePkts       : 0
        RxOversizePkts        : 0
    RxFragments           : 0
        RxJabbers             : 0
        RxCollisions          : 0
        RxPkt64Octets         : 0
        RxPkts65to127Octets   : 1937
        RxPkts128to255Octets  : 301
        RxPkts256to511Octets  : 97
        RxPkts512to1023Octets : 1
        RxPkts1024to1518Octets: 1455
```

Ethernet Switch Module L3 Simulated Interface Configuration

L3 simulated interface is a logical interface, it binds with VLAN, only receiving this VLAN packet.

sw Interface Command

Command	Description	Configuration mode
int switchethernet [swNum]	Create a switchethernet interface/ enter switchethernet interface configuration mode	configconfig-if-switchethernet
no int switchethernet [swNum]	Delete a switchethernet interface	config
vlan vlanNum	Bind switchethernet interface	config-if-switchethernet
sw-macaddr mac	Modify mac address to switchethernet	config-if-switchethernet

Switchethernet Interface Command

Switchethernet interface most configuration commands are the same to normal Ethernet sub-interface.

Create a switchethernet interface/enter a switchethernet interface configuration mode

Configuration command

```
int switchethernet [swNum]
```

Syntax	Description
swNum	Switchethernet interface unit number, and the range is same with switching port number

(Configuration mode) global configuration mode, interface configuration mode

(Default status)SW0 binding VLAN 1.

Delete a switchethernet interface
Configuration command

```
no int switchethernet [swNum]
```

Syntax	Description
swNum	Switchethernet interface unit number, and the range is the same as switching port number.

(Configuration mode) global configuration mode.

Binding switchethernet interface
Configuration command

```
vlan vlanNum
```

Syntax	Description
vlanNum	Binding vlan to switchethernet interface

(Configuration mode) interface configuration mode
(Default status)switchethernet interface doesn't bind vlan.

Modify mac address to switchethernet interface
Configuration command

```
sw-macaddr mac
```

Syntax	Description
mac	New configured mac address, format is similar as 0001.7a12.3456

(Configuration mode) interface configuration mode
(Default status)switchethernet interface uses flash mac address.